Symantec NetBackup™ Troubleshooting Guide

UNIX, Windows, and Linux

Release 7.6

21317380

Symantec

Symantec NetBackup™ Troubleshooting Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 7.6

PN: 21317380

Legal Notice

Copyright © 2013 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Technical Support 4

Chapter 1 Introduction 13

Troubleshooting a problem 13
Problem report for Technical Support 15
About gathering information for NetBackup-Java applications 17

Chapter 2 Troubleshooting procedures 19

About troubleshooting procedures 20
Troubleshooting NetBackup problems 22
Verifying that all processes are running on UNIX servers 24
Verifying that all processes are running on Windows servers 26
Troubleshooting installation problems 28
Troubleshooting configuration problems 29
Device configuration problem resolution 31
Testing the master server and clients 34
Testing the media server and clients 38
Resolving network communication problems with UNIX clients 41
Resolving network communication problems with PC clients 46
About troubleshooting networks and host names 49
Verifying host name and service entries in NetBackup 53
Example of host name and service entries on UNIX master server and client 57
Example of host name and service entries on UNIX master server and media server 59
Example of host name and service entries on UNIX PC clients 60
Example of host name and service entries on UNIX clients in multiple networks 61
Example of host name and service entries on UNIX server that connects to multiple networks 64
About the bpclntcmd utility 65
Using the Host Properties window to access configuration settings 67
Resolving full disk problems 68

Frozen media troubleshooting considerations 69
Logs for troubleshooting frozen media 70
About conditions that cause media to freeze 70
Resolving PBX problems 73
Checking PBX installation 74
Checking that PBX is running 74
Checking that PBX is set correctly 75
Accessing the PBX logs 76
Troubleshooting PBX security 77
Determining if the PBX daemon or service is available 78
Resolving no jobs displayed on Activity Monitor 79
About troubleshooting Auto Image Replication 79
Troubleshooting Auto Image Replication 80
About troubleshooting automatic import jobs 86
Troubleshooting network interface card performance 90
About SERVER entries in the bp.conf file 91
About unavailable storage unit problems 91
Resolving a NetBackup Administration operations failure on Windows 92
About troubleshooting NetBackup in a SAN environment 92
NetBackup enterprise lifecycle best practices 93
Using CommandCentral Storage to troubleshoot NetBackup in a SAN environment 94

Chapter 3 Using NetBackup utilities 99

About NetBackup troubleshooting utilities 99
About the analysis utilities for NetBackup debug logs 100
About network troubleshooting utilities 104
About the NetBackup support utility (nbsu) 105
Output from the NetBackup support utility (nbsu) 107
Status code information gathered by the NetBackup support utility (nbsu) 110
Example of a progress display for the NetBackup support utility (nbsu) 110
About the NetBackup consistency check utility (NBCC) 111
Output from the NetBackup consistency check utility (NBCC) 113
Example of an NBCC progress display 114
About the NetBackup consistency check repair (NBCCR) utility 120
About the nbcplogs utility 122
About the robotic test utilities 123
Robotic tests on UNIX 124

Robotic tests on Windows 125

Chapter 4 Using logs 127

About logs 127
About UNIX system logs 129
About unified logging 129
Gathering unified logs for NetBackup 130
Types of unified logging messages 132
File name format for unified logging 133
Originator IDs for the entities that use unified logging 134
About changing the location of unified log files 140
About rolling over unified log files 141
About recycling unified log files 142
About using the vxlogview command to view unified logs 143
About query strings used with the vxlogview command 144
Examples of using vxlogview to view unified logs 147
Examples of using vxlogmgr to manage unified logs 148
Examples of using vxlogcfg to configure unified logs 151
About legacy logging 153
UNIX client processes that use legacy logging 154
PC client processes that use legacy logging 155
File name formats for legacy logging 158
Directory names for legacy debug logs for servers 159
Directory names for legacy debug logs for media and device management 161
How to control the amount of information written to legacy logging files 162
About limiting the size and the retention of legacy logs 163
Configuring legacy log rotation 165
Creating legacy log directories to accompany problem reports for synthetic backup 166
About global logging levels 166
Changing the logging level 168
Changing the logging level on Windows clients 169
Setting debug logging to a higher level 169
Logs to accompany problem reports for synthetic backups 170
Setting retention limits for logs on clients 171
Logging options with the Windows Event Viewer 171
Troubleshooting error messages in the NetBackup Administration Console for UNIX 174
About extra disk space required for logs and temporary files 175
Enabling detailed debug logging 176

Chapter 5 Backup logging 178

About backup logging 178
Sending backup logs to Symantec Technical Support 181

Chapter 6 Restore logging 184

About restore logging 184
Sending restore logs to Symantec Technical Support 189

Chapter 7 Locating logs 191

acsssi logging 192
bpbackup logging 192
bpbkar logging 193
bpbrm logging 193
bpcd logging 194
bpcompatd logging 194
bpdbm logging 194
bpjobd logging 195
bprd logging 195
bprestore logging 196
bptm logging 196
daemon logging 197
ltid logging 197
nbemm logging 198
nbjm logging 198
nbpem logging 198
nbproxy logging 199
nbrb logging 199
PBX logging 200
reqlib logging 200
robots logging 201
tar logging 201
t*xx*d and t*xx*cd logging 202
vnetd logging 202

Chapter 8 Disaster recovery 204

About disaster recovery 204
Recommended backup practices 205
About disk recovery procedures for UNIX and Linux 207
Recovering the master server disk for UNIX and Linux 208
About recovering the NetBackup media server disk for UNIX 213
Recovering the system disk on a UNIX client workstation 213

About clustered NBU server recovery for UNIX and Linux 213
Replacing a failed node on a UNIX or Linux cluster 214
Recovering the entire UNIX or Linux cluster 215
About disk recovery procedures for Windows 216
About recovering the master server disk for Windows 217
About recovering the NetBackup media server disk for Windows 223
Recovering a Windows client disk 223
About clustered NBU server recovery for Windows 225
Replacing a failed node on a Windows VCS cluster 226
Recovering the shared disk on a Windows VCS cluster 226
Recovering the entire Windows VCS cluster 227
About recovering the NetBackup catalog 228
About NetBackup catalog recovery on Windows computers 230
About NetBackup catalog recovery from disk devices 230
About NetBackup catalog recovery and symbolic links 231
About NetBackup catalog recovery and OpsCenter 231
About recovering the entire NetBackup catalog 232
About recovering the NetBackup catalog image files 243
About recovering the NetBackup relational database 257
Recovering the NetBackup catalog when NetBackup Access Control is configured 264
Recovering the NetBackup catalog from a nonprimary copy of a catalog backup 266
Recovering the NetBackup catalog without the disaster recovery file 266
Recovering a NetBackup user-directed online catalog from the command line 270
Restoring files from a NetBackup online catalog backup 273
Unfreezing the NetBackup online catalog recovery media 274
Importing backup images, Phase I 274
Importing backup images, Phase II 276

Appendix A Backup and restore functional overview 278

About backup and restore functional overview 278
Backup and restore startup process 279
Backup and archive processes 279
Backups and archives - UNIX clients 280
Backup process 281
Snapshot backup and Windows open file backups 285
SAN client 288
Backups and archives - Windows 291

Synthetic backups 292
NetBackup hot catalog backup 295
About UNIX client restoration 296
About SAN client restoration 300
About Windows client restoration 303
About catalog backup restoration 304
NetBackup directories and files 306
NetBackup directory structure - UNIX 306
Contents of /usr/openv/netbackup 308
NetBackup programs and daemons 310
NetBackup catalogs 322

Appendix B Media and device management functional description 324

Media and device management startup process 324
Media and device management process 326
Shared Storage Option management process 328
Barcode operations 330
Media and device management components 332

Index 341

Chapter 1

Introduction

This chapter includes the following topics:

- Troubleshooting a problem
- Problem report for Technical Support
- About gathering information for NetBackup-Java applications

Troubleshooting a problem

The following steps offer general guidelines to help you resolve any problems you may encounter while you use NetBackup. The steps provide links to more specific troubleshooting information.

Table 1-1 Steps for troubleshooting NetBackup problems

Step	Action	Description
Step 1	Remember the error message	Error messages are usually the vehicle for telling you something went wrong. If you don't see an error message in an interface, but still suspect a problem, check the reports and logs. NetBackup provides extensive reporting and logging facilities. These can provide an error message that points you directly to a solution. The logs also show you what went right and the NetBackup operation that was ongoing when the problem occurred. For example, a restore operation needs media to be mounted, but the required media is currently in use for another backup. Logs and reports are essential troubleshooting tools. See "About logs" on page 127.

Table 1-1 Steps for troubleshooting NetBackup problems *(continued)*

Step	Action	Description
Step 2	Identify what you were doing when the problem occurred	Ask the following questions: ■ What operation was tried? ■ What method did you use? For example, more than one way exists to install software on a client. Also more than one possible interface exists to use for many operations. Some operations can be performed with a script. ■ What type of server platform and operating system was involved? ■ If your site uses both the master server and the media server, was it a master server or a media server? ■ If a client was involved, what type of client was it? ■ Have you performed the operation successfully in the past? If so, what is different now? ■ What is the service pack level? ■ Do you use operating system software with the latest fixes supplied, especially those required for use with NetBackup? ■ Is your device firmware at a level, or higher than the level, at which it has been tested according to the posted device compatibility lists?
Step 3	Record all information	Capture potentially valuable information: ■ NetBackup progress logs ■ NetBackup Reports ■ NetBackup Utility Reports ■ NetBackup debug logs ■ Media and Device Management debug logs ■ On UNIX NetBackup servers, check for error or status messages in the system log or standard output. ■ Error or status messages in dialog boxes ■ On Windows, NetBackup servers, check for error or status information in the Event Viewer Application and System log. Record this information for each try. Compare the results of multiple tries. A record of tries is also useful for others at your site and for Technical Support in the event that you cannot solve the problem. You can get more information about logs and reports. See "About logs" on page 127.

Table 1-1 Steps for troubleshooting NetBackup problems *(continued)*

Step	Action	Description
Step 4	Correct the problem	After you define the problem, use the following information to correct it: ■ Take the corrective action that the status code or message recommends. See the Status Codes Reference Guide. ■ If no status code or message exists, or the actions for the status code do not solve the problem, use additional troubleshooting procedures to isolate common problems. See "Troubleshooting NetBackup problems" on page 22.
Step 5	Complete a problem report for Technical Support	If your troubleshooting is unsuccessful, prepare to contact Technical Support by filling out a problem report. See "Problem report for Technical Support" on page 15. See "About gathering information for NetBackup-Java applications" on page 17. On UNIX systems, the `/usr/openv/netbackup/bin/goodies/support` script creates a file containing data necessary for Technical Support to debug any problems you encounter. For more details, consult the usage information of the script by using `support -h`.
Step 6	Contact Technical Support	The Symantec Technical Support website has a wealth of information that can help you solve NetBackup problems. Access Technical Support at the following URL: www.symantec.com/business/support/

Note: The term media server may not apply to the NetBackup server product. It depends on the context. When you troubleshoot a server installation, be aware that only one host exists: The master and the media server are one and the same. Ignore references to a media server on a different host.

Problem report for Technical Support

Fill out the following information before you contact support to report a problem.

Date: _____

Record the following product, platform, and device information:

- Product and its release level.
- Server hardware type and operating system level.

- Client hardware type and operating system level, if a client is involved.
- Storage units being used, if it is possible that storage units are involved.
- If it looks like a device problem, be ready to supply the following device information: The types of robots and drives and their version levels along with Media and Device Management and system configuration information.
- Software patches to the products that were installed.
- The service packs and hot fixes that were installed.

_____
_____
_____
_____
_____
_____

Define the problem.

_____
_____
_____

What were you doing when the problem occurred? (for example, a backup on a Windows client)

_____
_____

What were the error indications? (for example, status code, error dialog box)

_____
_____
_____

Did this problem occur during or shortly after any of the following:

_____ Initial installation

_____ Configuration change (explain)

_____ System change or problem (explain)

_____ Have you observed the problem before? (If so, what did you do that time?)

_____
_____
_____

Logs or other failure data you have saved:

_____ All log entries report

_____ Media and Device Management debug logs

_____ NetBackup debug logs

_____ System logs (UNIX)

_____ Event Viewer Application and System logs (Windows)

Ways that you can communicate with us:

_____ ftp

_____ telnet

_____ email

_____ WebEx

About gathering information for NetBackup-Java applications

If you encounter problems with the NetBackup-Java applications, use the following methods to gather data for support.

The following scripts are available for gathering information:

`jnbSA` (NetBackup-Java administration application startup script)	Logs the data in a log file in `/usr/openv/netbackup/logs/user_ops/nbjlogs`. At startup, the script tells you which file in this directory it logs to. Normally, this file does not become very large (usually less than 2 KB). Consult the file `/usr/openv/java/Debug.properties` for the options that can affect the contents of this log file.
NetBackup-Java administration application on Windows	Logs the data in a log file if NetBackup is installed on the computer where the application was started. It logs on *`install_path`*`\NetBackup\logs\user_ops\nbjlogs`. If NetBackup was not installed on this computer, then no log file is created. To produce a log file, modify the last “java.exe” line in the following to redirect output to a file: `install_path\java\nbjava.bat`. .
`/usr/openv/java/get_trace`	Provides a Java Virtual Machine stack trace for support to analyze. This stack trace is written to the log file that is associated with the instance of execution.

`/usr/openv/netbackup/bin/goodies/support`	Creates a file containing data necessary for customer support to debug any problems you encounter. For more details, consult the usage information of the script by using `support -h`.

The following example describes how you can gather troubleshooting data for Symantec Technical Support to analyze.

An application does not respond.	Wait for several minutes before you assume that the operation is hung. Some operations can take quite a while to complete, especially operations in the **Activity Monitor** and **Reports** applications.
Still no response after several minutes.	Run `/usr/openv/java/get_trace` under the account where you started the Java application. This script causes a stack trace to write to the log file. For example, if you started `jnbSA` from the root account, start `/usr/openv/java/get_trace` as root. Otherwise, the command runs without error, but fails to add the stack trace to the debug log. This failure occurs because root is the only account that has permission to run the command that dumps the stack trace.
Get data about your configuration.	Run `/usr/openv/netbackup/bin/goodies/support`. Run this script after you complete the NetBackup installation and every time you change the NetBackup configuration.
Contact Symantec Technical Support	Provide the log file and the output of the `support` script for analysis.

Chapter 2

Troubleshooting procedures

This chapter includes the following topics:

- About troubleshooting procedures
- Troubleshooting NetBackup problems
- Troubleshooting installation problems
- Troubleshooting configuration problems
- Device configuration problem resolution
- Testing the master server and clients
- Testing the media server and clients
- Resolving network communication problems with UNIX clients
- Resolving network communication problems with PC clients
- About troubleshooting networks and host names
- Verifying host name and service entries in NetBackup
- About the bpclntcmd utility
- Using the Host Properties window to access configuration settings
- Resolving full disk problems
- Frozen media troubleshooting considerations
- Resolving PBX problems
- About troubleshooting Auto Image Replication
- Troubleshooting network interface card performance

- About SERVER entries in the bp.conf file
- About unavailable storage unit problems
- Resolving a NetBackup Administration operations failure on Windows
- About troubleshooting NetBackup in a SAN environment

About troubleshooting procedures

These procedures for finding the cause of NetBackup errors are general in nature and do not try to cover every problem that can occur. They do, however, recommend the methods that usually result in successful problem resolution.

The Symantec Technical Support site has a wealth of information that can help you solve NetBackup problems. See the following site for comprehensive troubleshooting details:

http://www.symantec.com/business/support/

When you perform these procedures, try each step in sequence. If you already performed the action or it does not apply, skip to the next step. If it branches you to another topic, use the solutions that are suggested there. If you still have a problem, go to the next step in the procedure. Also, alter your approach according to your configuration and what you have already tried.

Troubleshooting procedures can be divided into the following categories:

Preliminary troubleshooting	The following procedures describe what to check first. They branch off to other procedures as appropriate. See "Troubleshooting NetBackup problems" on page 22. See "Verifying that all processes are running on UNIX servers" on page 24. See "Verifying that all processes are running on Windows servers" on page 26.
Installation troubleshooting	Problems that apply specifically to installation. See "Troubleshooting installation problems" on page 28.
Configuration troubleshooting	Problems that apply specifically to configuration. See "Troubleshooting configuration problems" on page 29.

General test and troubleshooting	These procedures define general methods for finding server and client problems and should be used last. See "Testing the master server and clients" on page 34. See "Testing the media server and clients" on page 38. See "Resolving network communication problems with UNIX clients" on page 41. See "Resolving network communication problems with PC clients" on page 46. See "Verifying host name and service entries in NetBackup" on page 53. See "About the bpclntcmd utility" on page 65. See "Verifying host name and service entries in NetBackup" on page 53.
Other troubleshooting procedures	See "Resolving full disk problems" on page 68. See "Frozen media troubleshooting considerations" on page 69. See "About conditions that cause media to freeze" on page 70. See "Troubleshooting network interface card performance" on page 90. See "About troubleshooting NetBackup in a SAN environment" on page 92.

A set of examples is also available that shows host name and service entries for UNIX systems.

- See "Example of host name and service entries on UNIX master server and client" on page 57.
- See "Example of host name and service entries on UNIX master server and media server" on page 59.
- See "Example of host name and service entries on UNIX PC clients" on page 60.
- See "Example of host name and service entries on UNIX clients in multiple networks" on page 61.
- See "Example of host name and service entries on UNIX server that connects to multiple networks" on page 64.

Troubleshooting NetBackup problems

If you have problems with NetBackup, perform these actions first.

This preliminary NetBackup troubleshooting procedure explains what to check first and branches to other procedures as appropriate. These procedures do not try to cover every problem that can occur. However, they do recommend the methods that usually result in successful problem resolution.

When you perform these procedures, try each step in sequence. If you already performed the action or it does not apply, skip to the next step. If you branch to another topic, use the solutions that are suggested there. If you still have a problem, go to the next step in the procedure. Also, alter your approach according to your configuration and what you have already tried.

Table 2-1 Steps for troubleshooting NetBackup problems

Step	Action	Description
Step 1	Verify operating systems and peripherals.	Ensure that your servers and clients are running supported operating system versions and that any peripherals you use are supported. Refer to the NetBackup release notes and the NetBackup compatibility lists on the following website: http://www.symantec.com/docs/TECH59978
Step 2	Use reports to check for errors.	Use the **All Log Entries** report and check for NetBackup errors for the appropriate time period. This report can show the context in which the error occurred. Often it provides specific information, which is useful when the status code can result from a variety of problems. See the Reports information in the NetBackup Administrator's Guide, Volume I. If the problem involved a backup or archive, check the **Status of Backups** report. This report gives you the status code. If you find a status code or message in either of these reports, perform the recommended corrective actions. See the Status Codes Reference Guide.

Table 2-1 Steps for troubleshooting NetBackup problems *(continued)*

Step	Action	Description
Step 3	Check the operating system logs.	Check the system log (UNIX) or the **Event Viewer** Application and System log (Windows) if the problem pertains to media or device management and one of the following is true: ■ NetBackup does not provide a status code. ■ You cannot correct the problem by following the instructions in NetBackup status codes and messages. ■ You cannot correct the problem by following the instructions in media and device management status codes and messages. These logs can show the context in which the error occurred. The error messages are usually descriptive enough to point you to a problem area.
Step 4	Review the debug logs.	Read the applicable enabled debug logs and correct any problems you detect. If these logs are not enabled, enable them before you retry the failed operation. See "About logs" on page 127.
Step 5	Retry the operation.	If you performed corrective actions, retry the operation. If you did not perform corrective actions or if the problem persists, continue with the next step.
Step 6	Get more information for installation problems.	If you see the problem during a new installation or upgrade installation, or after you make changes to an existing configuration, see the following procedures: See "Troubleshooting installation problems" on page 28. See "Troubleshooting configuration problems" on page 29.
Step 7	Ensure that the servers and clients are operational.	If you experienced a server or a client disk crash, procedures are available on how to recover the files that are critical to NetBackup operation. See "About disk recovery procedures for UNIX and Linux" on page 207. See "About disk recovery procedures for Windows" on page 216.

Table 2-1 Steps for troubleshooting NetBackup problems *(continued)*

Step	Action	Description
Step 8	Ensure that the partitions have enough disk space.	Verify that you have enough space available in the disk partitions that NetBackup uses. If one or more of these partitions is full, NetBackup processes that access the full partition fail. The resulting error message depends on the process. Possible error messages: "unable to access" or "unable to create or open a file." On UNIX systems, use the `df` command to view disk partition information. On Windows systems, use Disk Manager or Explorer. Check the following disk partitions: ■ The partition where NetBackup software is installed. ■ On the NetBackup master or media server, the partition where the NetBackup databases reside. ■ The partition where the NetBackup processes write temporary files. ■ The partition where NetBackup logs are stored. ■ The partition where the operating system is installed.
Step 9	Increase the logging level.	Enable verbose logging either for everything or only for the areas that you think are related to the problem. See "Changing the logging level" on page 168. See "How to control the amount of information written to legacy logging files" on page 162. See "Changing the logging level on Windows clients" on page 169.
Step 10	Determine which daemons or processes are running.	Follow the procedures for UNIX or Windows NetBackup servers. See "Verifying that all processes are running on UNIX servers" on page 24. See "Verifying that all processes are running on Windows servers" on page 26.

Verifying that all processes are running on UNIX servers

For NetBackup to operate properly, the correct set of processes (daemons) must be running on your UNIX servers. This procedure determines which processes are running and shows how to start the processes that may not be running.

To verify that all processes are running on UNIX servers

1. To see the list of processes (daemons) running on the server and on the **Media Manager**, enter the following command:

   ```
   /usr/openv/netbackup/bin/bpps -x
   ```

2. If the master server is also the EMM server, ensure that the `nbemm` and the `nbrb` services are running. If neither service is running, start them by entering the following two commands. If only one of the services is running, start the other service by using the appropriate command.

   ```
   /usr/openv/netbackup/bin/nbemm
   /usr/openv/netbackup/bin/nbrb
   ```

3. The `nbpem` and the `nbjm` services must be running on the master server. If neither service is running, start them by entering the following two commands. If only one of the services is running, start the other service by using the appropriate command.

   ```
   /usr/openv/netbackup/bin/nbjm
   /usr/openv/netbackup/bin/nbpem
   ```

4. If either the NetBackup request daemon (`bprd`) or database manager daemon (`bpdbm`) is not running, start them by entering the following command:

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

5. Make sure that the following media and device management processes are running:

   - `ltid` (needs to be running only if drives are configured on the server)
   - `vmd` (volume)
   - `avrd` (automatic volume recognition), only if drives are configured on the server
   - Processes for all configured robots

6. If any of these processes are not running, stop the device daemon `ltid` by running the following command:

   ```
   /usr/openv/volmgr/bin/stopltid
   ```

7 To verify that the `ltid`, `avrd`, and robotic control daemons are stopped, run the following command:

```
/usr/openv/volmgr/bin/vmps
```

8 If you use ACS robotic control, the `acsssi` and the `acssel` daemons may continue to run when `ltid` is terminated. Stop any robot control daemons that may continue to run by entering the following command:

```
/usr/openv/netbackup/bin/bp.kill_all
```

9 Then, start all daemons by running the following command:

```
/usr/openv/volmgr/bin/ltid
```

For debugging, start `ltid` with the `-v` (verbose) option.

Verifying that all processes are running on Windows servers

Use the following procedure to make sure that all the processes that need to run on Windows server are actually running.

Table 2-2 Steps to ensure that all necessary processes are running on Windows servers

Step	Action	Description
Step 1	Start all services.	The following services must be running. If these services are not running, start them by using the NetBackup **Activity Monitor** or the Services application in the Windows Control Panel. To start all of the services, run *install_path*\NetBackup\bin\bpup.exe. Services on master servers: ■ NetBackup Request Manager service ■ NetBackup Policy Execution Manager service ■ NetBackup Job Manager service ■ NetBackup Database Manager service ■ NetBackup Device Manager service (if the system has configured devices) ■ NetBackup Volume Manager service ■ NetBackup Client service Services on EMM servers: ■ NetBackup Enterprise Media Manager service ■ NetBackup Resource Broker service Services on media servers: ■ NetBackup Device Manager service (if the system has configured devices) ■ NetBackup Volume Manager NetBackup Client service ■ NetBackup Client service Services on clients (including NetBackup Remote Administration Consoles): ■ NetBackup Client service
Step 2	Start `avrd` and processes for robots.	Use the NetBackup **Activity Monitor** to see if the following processes are running: ■ `avrd` (automatic media recognition), only if drives are configured on the server ■ Processes for all configured robots. See the NetBackup Administrator's Guide, Volume I. If these processes are not running, stop and restart the NetBackup **Device Manager** service. Use the NetBackup **Activity Monitor** or the Services application in the Windows Control Panel.

Table 2-2 Steps to ensure that all necessary processes are running on Windows servers *(continued)*

Step	Action	Description
Step 3	Restart the operation or do additional troubleshooting.	If you had to start any of the processes or services in the previous steps, retry the operation. If the processes and services are running or the problem persists, you can try to test the servers and clients. See "Testing the master server and clients" on page 34. See "Testing the media server and clients" on page 38. If you cannot start any of these processes or services, check the appropriate debug logs for NetBackup problems. See "About logs" on page 127. When these processes and services start, they continue to run unless you stop them manually or a problem occurs on the system. On Windows systems, we recommend that you add commands for starting them to your startup scripts, so they restart in case you have to reboot

Troubleshooting installation problems

Use the following steps to troubleshoot installation problems.

Table 2-3 Steps for troubleshooting installation problems.

Step	Action	Description
Step 1	Determine if you can install the software on the master server and the media servers by using the release media.	Some reasons for failure are as follows: ■ Not logged on as an administrator on a Windows system (you must have permission to install services on the system) ■ Permission denied (ensure that you have permission to use the device and to write the directories and files being installed) ■ Bad media (contact Technical Support) ■ Defective drive (replace the drive or refer to vendor's hardware documentation) ■ Improperly configured drive (refer to the system and the vendor documentation)

Table 2-3 Steps for troubleshooting installation problems. *(continued)*

Step	Action	Description
Step 2	Determine if you can install NetBackup client software on the clients.	**Note:** Before you install or use NetBackup on a Linux client, verify that the `inetd` (or `xinetd`) service is started on that computer. This service ensures proper communication between the NetBackup master and the Linux client. **Note:** You cannot install PC client software from a UNIX NetBackup server. Do the following: ■ For an install to a trusting UNIX client, verify the following: ■ The correct client name is in your policy configuration ■ The correct server name is in the client `/.rhosts` file If the installation hangs, check for problems with the shell or the environment variables for the root user on the client. The files that you check depend on the platform, operating system, and shell you use. For example, your `.login` on a Sun system runs an `stty` (such as `stty ^erase`) before it defines your terminal type. If this action causes the install process to hang, you can modify the `.login` file to define the terminal before you run the `stty`. Or, move the client `.login` to another file until the install is complete. ■ For an installation to a secure UNIX client, check your `ftp` configuration. For example, you must use a user name and password that the client considers valid.
Step 3	Resolve network problems.	Determine if the problem is related to general network communications. See "Resolving network communication problems with UNIX clients" on page 41. See "Resolving network communication problems with PC clients" on page 46.

Troubleshooting configuration problems

Use the following steps to check for problems after an initial installation or after changes are made to the configuration.

Table 2-4 Steps for troubleshooting configuration problems

Step	Action	Description
Step 1	Check for device configuration problems.	Check for the following device configuration problems: ■ Configuration for robotic drive does not specify the robot. ■ Drive is configured as wrong type or density. ■ Incorrect Robotic Drive Number. ■ SCSI ID for the robotic control is specified instead of the logical Robot Number that is assigned to the robot. ■ The same robot number is used for different robots. ■ SCSI ID for the drive is specified instead of a unique Drive Index number. ■ A platform does not support a device or was not configured to recognize it. ■ Robotic device is not configured to use LUN 1, which some robot hardware requires. ■ On UNIX, drive no-rewind device path is specified as a rewind path. ■ On UNIX, tape devices are not configured with "Berkeley style close." NetBackup requires this feature which is configurable on some platforms. Further explanation is available. ■ On UNIX, tape devices (other than QIC) are not configured as "variable mode." NetBackup requires this feature which is configurable on some platforms. When this condition exists, you can frequently perform backups but not restores. For more information, see the Status Codes Reference Guide. ■ On UNIX, pass-through paths to the tape drives have not been established. More description is available on device configuration problems: See the NetBackup Device Configuration Guide.
Step 2	Check the daemons or services.	Check for the following problems with the daemons or services: ■ Daemons or services do not start during restart (configure system so they start). ■ Wrong daemons or services are started (problems with media server startup scripts). ■ Configuration was changed while daemons or services were running. ■ On Windows, the `%SystemRoot%\System32\drivers\etc\services` file does not have an entry for `vmd`, `bprd`, `bpdbm`, and `bpcd`. Also, ensure that the processes have entries for configured robots. A list of these processes is available. See the NetBackup Administrator's Guide, Volume I. ■ On UNIX, the `/etc/services` file (or NIS or DNS) does not have an entry for `vmd`, `bprd`, `bpdbm`, or robotic daemons.

Table 2-4 Steps for troubleshooting configuration problems *(continued)*

Step	Action	Description
Step 3	Retry the operation and check for status codes and messages.	If you found and corrected any configuration problems, retry the operation and check for NetBackup status codes or messages in the following: ■ Check the **All Log Entries** report for NetBackup errors for the appropriate time period. This report can show the context in which the error occurred. Often it provides specific information, which is useful when the error can result from a variety of problems. If the problem involved a backup or archive, check the **Status of Backups** report. This report gives you the status code. If you find a status code or message in either of these reports, perform the recommended corrective actions. See the Status Codes Reference Guide. ■ Check the system logs on UNIX or the Event Viewer Application and System log on Windows if the following is true: The problem pertains to media or device management, and NetBackup does not provide a status code, or you cannot correct the problem by following the instructions in the status codes ■ Check the appropriate enabled debug logs. Correct any problems you detect. If these logs are not enabled, enable them before your next try. See "About logs" on page 127.
Step 4	Retry the operation and do additional troubleshooting.	If you performed corrective actions, retry the operation. If you did not perform corrective actions or the problem persists, go to one of the following procedures. See "Resolving full disk problems" on page 68. See "Frozen media troubleshooting considerations" on page 69. See "About conditions that cause media to freeze" on page 70. See "Troubleshooting network interface card performance" on page 90. See "About troubleshooting NetBackup in a SAN environment" on page 92.

Device configuration problem resolution

An auto-configuration warning message appears in the second panel of the Device Configuration Wizard if the selected device meets any of the following conditions:

- Not licensed for NetBackup server
- Exceeds a license restriction
- Has some inherent qualities that make it difficult to auto-configure

The following messages relate to device configuration, along with their explanations and recommended actions.

Table 2-5 Recommended actions for device configuration messages

Message	Explanation	Recommended action
Drive does not support serialization	The drive does not return its serial number. Note that some manufacturers do not support serial numbers. Although automatic device configuration does not function optimally, the drive can be manually configured and operated without its serial number.	Ask the manufacturer for a newer firmware version that returns serial numbers (if available), or manually configure and operate the drive without a serial number.
Robot does not support serialization	The robot does not return its serial number or the serial numbers of the drives that are contained within it. Note that some manufacturers do not support serial numbers. Although automatic device configuration does not function optimally, the robot and drives can be manually configured and operated without serial numbers.	Ask the manufacturer for a newer firmware version that returns serial numbers (if available). Or manually configure and operate the robot and drives without serial numbers.
No license for this robot type	NetBackup server does not support the robotic type that is defined for this robot.	Define a different robot. Use only the robotic libraries that NetBackup server supports.
No license for this drive type	The drive type that is defined for this drive that the NetBackup server does not support.	Define a different drive. Use only the drives that NetBackup supports
Unable to determine robot type	NetBackup does not recognize the robotic library. The robotic library cannot be auto-configured.	Do the following: ■ Download a new device_mapping file from the Symantec Support website, and try again. ■ Configure the robotic library manually. ■ Use only the robotic libraries that NetBackup supports.
Drive is standalone or in unknown robot	Either the drive is standalone, or the drive or robot does not return a serial number. Note that some manufacturers do not support serial numbers. Although automatic device configuration does not function optimally, the drive or robot can be manually configured and operated without a serial number.	Ask the manufacturer for a newer firmware version that returns serial numbers (if available), or manually configure and operate the drive robot without serial numbers.

Table 2-5 Recommended actions for device configuration messages *(continued)*

Message	Explanation	Recommended action
Robot drive number is unknown	Either the drive or robot does not return a serial number. Note that some manufacturers do not support serial numbers. Although automatic device configuration does not function optimally, the drive or robot can be manually configured and operated without a serial number.	Ask the manufacturer for a newer firmware version that returns serial numbers (if available). Or manually configure and operate the drive and robot without serial numbers.
Drive is in an unlicensed robot	The drive is in a robotic library that cannot be licensed for NetBackup server. Since the robot cannot be licensed for NetBackup server, any drives that were configured in that robot are unusable.	Configure a drive that does not reside in the unlicensed robot.
Drive's SCSI adapter does not support pass-thru (or pass-thru path does not exist)	A drive was found that does not have a SCSI pass-through path configured. The possible causes are: ■ The drive is connected to an adapter that does not support SCSI pass-through. ■ The pass-through path for this drive has not been defined.	Change the drive's adapter or define a pass-through path for the drive. For information about the SCSI adapter pass-through, see the NetBackup Device Configuration Guide.
No configuration device file exists	A device has been detected without the corresponding device file necessary to configure that device.	For directions about how to create device files, see the NetBackup Device Configuration Guide.
Unable to determine drive type	The NetBackup server does not recognize the drive. The drive cannot be auto-configured.	Do the following: ■ Download a new device_mapping file from the Symantec Support website, and try again. ■ Configure the drive manually. ■ Use only the drives that NetBackup supports.

Table 2-5 Recommended actions for device configuration messages *(continued)*

Message	Explanation	Recommended action
Unable to determine compression device	A drive was detected without the expected compression device file that is used to configure that device. Automatic device configuration tries to use a device file that supports hardware data compression. When multiple compression device files exist for a drive, automatic device configuration cannot determine which compression device file is best. It uses a non-compression device file instead.	If you do not need hardware data compression, no action is necessary. The drive can be operated without hardware data compression. Hardware data compression and tape drive configuration help are available. For directions about how to create device files, see the NetBackup Device Configuration Guide.

Testing the master server and clients

If the NetBackup, installation, and configuration troubleshooting procedures do not reveal the problem, perform the following procedure. Skip those steps that you have already performed.

The procedure assumes that the software was successfully installed, but not necessarily configured correctly. If NetBackup never worked properly, you probably have configuration problems. In particular, look for device configuration problems.

You may also want to perform each backup and restore twice. On UNIX, perform them first as a root user and then as a nonroot user. On Windows, perform them first as a user that is a member of the Administrators group. Then perform them as a user that is not a member of the Administrator group. In all cases, ensure that you have read and write permissions on the test files.

The explanations in these procedures assume that you are familiar with the functional overview information.

See “About backup and restore functional overview” on page 278.

Several steps in this procedure mention the **All Log Entries** report. To access more information on this report and others, refer to the following:

See the NetBackup Administrator’s Guide, Volume I.

Table 2-6 Steps for testing the master server and clients

Step	Action	Description
Step 1	Enable debug logs.	Enable the appropriate debug logs on the master server. See "About logs" on page 127. See "About unified logging" on page 129. See "About legacy logging" on page 153. If you do not know which logs apply, enable them all until you solve the problem. Delete the debug log directories when you have resolved the problem.
Step 2	Configure a test policy.	Configure a test policy and set the backup window to be open while you test. Name the master server as the client and a storage unit that is on the master server (preferably a nonrobotic drive). Also, configure a volume in the NetBackup volume pool and insert the volume in the drive. If you don't label the volume by using the `bplabel` command, NetBackup automatically assigns a previously unused media ID.
Step 3	Verify the daemons and services.	To verify that the NetBackup daemons or services are running on the master server, do the following: ■ To check the daemons on a UNIX system, enter the following command: `/usr/openv/netbackup/bin/bpps -a` ■ To check the services on a Windows system, use the NetBackup Activity Monitor or the Services application of the Windows Control Panel.
Step 4	Backup and restore a policy.	Start a manual backup of a policy by using the manual backup option in the NetBackup administration interface. Then, restore the backup. These actions verify the following: ■ NetBackup server software is functional, which includes all daemons or services, programs, and databases. ■ NetBackup can mount the media and use the drive you configured.
Step 5	Check for failure.	If a failure occurs, first check the NetBackup **All Log Entries** report. For the failures that relate to drives or media, verify that the drive is in an UP state and that the hardware functions. To isolate the problem further, use the debug logs. A functional overview sequence of events is available. See "About backup and restore functional overview" on page 278.

Table 2-6 Steps for testing the master server and clients *(continued)*

Step	Action	Description
Step 6	Consult information besides the debug logs.	If the debug logs do not reveal the problem, check the following: ■ Systems Logs or Event Viewer System logs ■ Event Viewer Application and System logs on Windows systems ■ `vmd` debug logs on the EMM database host for the device ■ `bptm` debug logs See the vendor manuals for information on hardware failures.
Step 7	Verify robotic drives.	If you use a robot and the configuration is an initial configuration, verify that the robotic drive is configured correctly. In particular, verify the following: ■ The same robot number is used both in the Media and Device Management and storage unit configurations. ■ Each robot has a unique robot number. On a UNIX NetBackup server, you can verify only the Media and Device Management part of the configuration. To verify, use the `tpreq` command to request a media mount. Verify that the mount completes and check the drive on which the media was mounted. Repeat the process until the media is mounted and unmounted on each drive from the host where the problem occurred. If this works, the problem is probably with the policy or the storage unit configuration. When you are done, `tpunmount` the media.
Step 8	Include a robot in the test policy.	If you previously configured a nonrobotic drive and your system includes a robot, change your test policy now to specify a robot. Add a volume to the robot. The volume must be in the NetBackup volume pool on the EMM database host for the robot. Return to step 3 and repeat this procedure for the robot. This procedure verifies that NetBackup can find the volume, mount it, and use the robotic drive.
Step 9	Use the robotic test utilities.	If you have difficulties with the robot, try the test utilities. See "About the robotic test utilities" on page 123. Do not use the Robotic Test Utilities when backups or restores are active. These utilities prevent the corresponding robotic processes from performing robotic actions, such as loading and unloading media. The result is that it can cause media mount timeouts and prevent other robotic operations like robotic inventory and inject or eject from working.
Step 10	Enhance the test policy.	Add a user schedule to your test policy (the backup window must be open while you test). Use a storage unit and media that was verified in previous steps.

Table 2-6 Steps for testing the master server and clients *(continued)*

Step	Action	Description
Step 11	Backup and restore a file.	Start a user backup and restore of a file by using the client-user interface on the master server. Monitor the status and the progress log for the operation. If successful, this operation verifies that the client software is functional on the master server. If a failure occurs, check the NetBackup **All Log Entries** report. To isolate the problem further, check the appropriate debug logs from the following list. On a UNIX system, the debug logs are in the `/usr/openv/netbackup/logs/` directory. On a Windows system, the debug logs are in the *`install_path`*`\NetBackup\logs\` directory. Debug log directories exist for the following processes: ■ `bparchive` (UNIX only) ■ `bpbackup` (UNIX only) ■ `bpbkar` ■ `bpcd` ■ `bplist` ■ `bprd` ■ `bprestore` ■ `nbwin` (Windows only) ■ `bpinetd` (Windows only) Explanations about which logs apply to specific client types are available. See "About logs" on page 127. See "About unified logging" on page 129. See "About legacy logging" on page 153.
Step 12	Reconfigure the test policy.	Reconfigure your test policy to name a client that is located elsewhere in the network. Use a storage unit and media that has been verified in previous steps. If necessary, install the NetBackup client software.

Table 2-6 Steps for testing the master server and clients *(continued)*

Step	Action	Description
Step 13	Create debug log directories.	Create debug log directories for the following processes: ■ `bprd` on the server ■ `bpcd` on the client ■ `bpbkar` on the client ■ `nbwin` on the client (Windows only) ■ `bpbackup` on the client (except Windows clients) ■ `bpinetd` (Windows only) Explanations about which logs apply to specific client types are available. See "About logs" on page 127. See "About unified logging" on page 129. See "About legacy logging" on page 153.
Step 14	Verify communication between the client and the master server.	Perform a user backup and then a restore from the client that is specified in step 8. These actions verify communications between the client and the master server, and NetBackup software on the client. If an error occurs, check the **All Log Entries** report and the debug logs that you created in the previous step. A likely cause for errors is a communications problem between the server and the client.
Step 15	Test other clients or storage units.	When the test policy operates satisfactorily, repeat specific steps as necessary to verify other clients and storage units.
Step 16	Test the remaining policies and schedules.	When all clients and storage units are functional, test the remaining policies and schedules that use storage units on the master server. If a scheduled backup fails, check the **All Log Entries** report for errors. Then follow the recommended actions as is part of the error status code.

Testing the media server and clients

If you use media servers, use the following steps to verify that they are operational. Before testing the media servers, eliminate all problems on the master server.

See "Testing the master server and clients" on page 34.

Table 2-7 Steps for testing the media server and clients

Step	Action	Description
Step 1	Enable legacy debug logs.	Enable appropriate legacy debug logs on the servers See "About logs" on page 127. See "About legacy logging" on page 153. If you are uncertain which logs apply, enable them all until you solve the problem. Delete the legacy debug log directories when you have resolved the problem.
Step 2	Configure a test policy.	Configure a test policy with a user schedule (set the backup window to be open while you test) by doing the following: ■ Name the media server as the client and a storage unit that is on the media server (preferably a nonrobotic drive). ■ Add a volume on the EMM database host for the devices in the storage unit. Ensure that the volume is in the NetBackup volume pool. ■ Insert the volume in the drive. If you do not pre-label the volume by using the `bplabel` command, NetBackup automatically assigns a previously unused media ID.
Step 3	Verify the daemons and services.	Verify that all NetBackup daemons or services are running on the master server. Also, verify that all Media and Device Management daemons or services are running on the media server. To perform this check, do one of the following: ■ On a UNIX system, run: `/usr/openv/netbackup/bin/bpps -a` ■ On a Windows system, use the Services application in the Windows Control Panel.
Step 4	Backup and restore a file.	Perform a user backup and then a restore of a file from a client that has been verified to work with the master server. This test verifies the following: ■ NetBackup media server software ■ NetBackup on the media server can mount the media and use the drive that you configured ■ Communications between the master server processes `nbpem`, `nbjm`, `nbrb`, EMM server process `nbemm`, and media server processes `bpcd` and `bpbrm` ■ Communications between media server process `bpbrm` and client processes `bpcd` and `bpbkar` For the failures that relate to drives or media, ensure that the drive is in an UP state and that the hardware functions.

Table 2-7 Steps for testing the media server and clients *(continued)*

Step	Action	Description
Step 5	Verify communication between the master server and the media servers.	If you suspect a communications problem between the master server and the media servers, check the debug logs for the pertinent processes. If the debug logs don't help you, check the following: ■ On a UNIX server, the System log ■ On a Windows server, the **Event Viewer** Application and System log ■ `vmd` debug logs
Step 6	Ensure that the hardware runs correctly.	For the failures that relate to drives or media, ensure that the drive is running and that the hardware functions correctly. See the vendor manuals for information on hardware failures. If you use a robot in an initial configuration condition, verify that the robotic drive is configured correctly. In particular, verify the following: ■ The same robot number is used both in the Media and Device Management and storage unit configurations. ■ Each robot has a unique robot number. On a UNIX server, you can verify only the Media and Device Management part of the configuration. To verify, use the `tpreq` command to request a media mount. Verify that the mount completes and check the drive on which the media was mounted. Repeat the process until the media is mounted and unmounted on each drive from the host where the problem occurred. Perform these steps from the media server. If this works, the problem is probably with the policy or the storage unit configuration on the media server. When you are done, use `tpunmount` to unmount the media.

Table 2-7 Steps for testing the media server and clients *(continued)*

Step	Action	Description
Step 7	Include a robotic device in the test policy.	If you previously configured a non-robotic drive and a robot was attached to your media server, change the test policy to name the robot. Also, add a volume for the robot to the EMM server. Verify that the volume is in the NetBackup volume pool and in the robot. Start with step 3 to repeat this procedure for a robot. This procedure verifies that NetBackup can find the volume, mount it, and use the robotic drive. If a failure occurs, check the NetBackup **All Log Entries** report. Look for any errors that relate to devices or media. See the NetBackup Administrator's Guide, Volume I. If the **All Log Entries** report doesn't help, check the following: ■ On a UNIX server, the system logs on the media server ■ `vmd` debug logs on the EMM server for the robot ■ On a Windows system, the **Event Viewer** Application and System log In an initial configuration, verify that the robotic drive is configured correctly. Do not use a robot number that is already configured on another server. Try the test utilities. See "About the robotic test utilities" on page 123. Do not use the Robotic Test Utilities when backups or restores are active. These utilities prevent the corresponding robotic processes from performing robotic actions, such as loading and unloading media. The result is that it can cause media mount timeouts and prevent other robotic operations like robotic inventory and inject or eject from working.
Step 8	Test other clients or storage units.	When the test policy operates satisfactorily, repeat specific steps as necessary to verify other clients and storage units.
Step 9	Test the remaining policies and schedules.	When all clients and storage units are in operation, test the remaining policies and schedules that use storage units on the media server. If a scheduled backup fails, check the **All Log Entries** report for errors. Then follow the suggested actions for the appropriate status code.

Resolving network communication problems with UNIX clients

The following procedure is for resolving NetBackup communications problems, such as those associated with NetBackup status codes 25, 54, 57, and 58. This procedure consists of two variations: one for UNIX clients and another for PC clients.

Note: In all cases, ensure that your network configuration works correctly outside of NetBackup before trying to resolve NetBackup problems.

For UNIX clients, perform the following steps. Before you start this procedure, add the `VERBOSE=5` option to the `/usr/openv/netbackup/bp.conf` file.

Table 2-8 Steps for resolving network communication problems with UNIX clients

Step	Action	Description
Step 1	Create debug log directories.	During communication retries, the debug logs provide detailed debug information, which can help you analyze the problem. Create the following directories: ■ `bpcd` (on server and clients) ■ `vnetd` (on server and clients) ■ `bprd` (on server) Use the `bprd` log directory to debug client to master server communication, not client to media server communication problems.
Step 2	Test a new configuration or modified configuration.	If this configuration is a new or a modified configuration, do the following: ■ Check any recent modifications to ensure that they did not introduce the problem. ■ Ensure that the client software was installed and that it supports the client operating system. ■ Check the client names, server names, and service entries in your NetBackup configuration as explained in the following topic: See "Verifying host name and service entries in NetBackup" on page 53. You can also use the `hostname` command on the client to determine the host name that the client sends with requests to the server. Check the `bprd` debug log on the server to determine what occurred when the server received the request.
Step 3	Verify name resolution.	To verify name resolution, run the following command on the master server and the media servers: `# bpclntcmd -hn clientname` If the results are unexpected, review the configuration of these name resolution services: `nsswitch.conf` file, `hosts` file, `ipnodes` file, and `resolv.conf` file.

Table 2-8 Steps for resolving network communication problems with UNIX clients *(continued)*

Step	Action	Description

Step 4	Verify network connectivity.	Verify network connectivity between client and server by pinging the client from the server.
		`# ping clientname`
		Where ***clientname*** is the name of the client as configured in the NetBackup policy configuration.
		For example, to `ping` the policy client that is named `ant`:
		`# ping ant`
		`ant.nul.nul.com: 64 byte packets`
		`64 bytes from 199.199.199.24: icmp_seq=0. time=1. ms`
		`----ant.nul.nul.com PING Statistics----`
		`2 packets transmitted, 2 packets received, 0% packet loss round-trip (ms)  min/avg/max = 1/1/1`
		A successful `ping` verifies connectivity between the server and client. If the ping fails and ICMP is not blocked between the hosts, resolve the network problem outside of NetBackup before you proceed.
		Some forms of the `ping` command let you ping the `bpcd` port on the client as in the following command:
		`# ping ant 13782`
		Ping 1556 (`PBX`), 13724 (`vnetd`), and 13782 (`bpcd`) in sequence, the same sequence that NetBackup tries by default. You then know which ports are closed so that you can open them or adjust the Connect Options for more efficient connection tries.

Table 2-8 Steps for resolving network communication problems with UNIX clients *(continued)*

Step	Action	Description

Step 5	Ensure that the client listens on the correct port for the `bpcd` connections.	Run one of the following commands (depending on platform and operating system):
		`netstat -a | grep bpcd`
		`netstat -a | grep 13782`
		`rpcinfo -p | grep 13782`
		Repeat for 1556 (`PBX`) and 13724 (`vnetd`). If no problems occur with the ports, the expected output is as follows:
		`# netstat -a | egrep '1556|PBX|13724|vnetd|13782|bpcd' | grep LISTEN`
		`*.1556 *.* 0 0 49152 0 LISTEN`
		`*.13724 *.* 0 0 49152 0 LISTEN`
		`*.13782 *.* 0 0 49152 0 LISTEN`
		LISTEN indicates that the client listens for connections on the port.
		If the NetBackup processes are running correctly, the expected output is as follows (this output is for NetBackup 7.0.1 and later):
		`# ps -ef | egrep 'pbx_exchange|vnetd|bpcd' | grep -v grep`
		`root 306 1 0 Jul 18 ? 13:52 /opt/VRTSpbx/bin/pbx_exchange`
		`root 10274 1 0 Sep 13 ? 0:11 /usr/openv/netbackup/bin/vnetd -standalone`
		`root 10277 1 0 Sep 13 ? 0:45 /usr/openv/netbackup/bin/bpcd -standalone`

Step 6	Connect to the client through `telnet`.	`telnet` to 1556 (`PBX`), 13724 (`vnetd`), and 13782 (`bpcd`) on the client. Check all three ports to make sure that a connection is made on at least one of them, then modify the NetBackup configuration accordingly. If the `telnet` connection succeeds, keep the connection until after you perform step 8, then terminate it with Ctrl-c.
		`telnet` *`clientname`* `1556`
		`telnet` *`clientname`* `13724`
		`telnet` *`clientname`* `13782`
		Where *clientname* is the name of the client as configured in the NetBackup policy configuration.
		For example,
		`# telnet ant bpcd`
		`Trying 199.999.999.24 ...`
		`Connected to ant.nul.nul.com.`
		`Escape character is '^]'.`
		In this example, `telnet` can establish a connection to the client `ant`.

Table 2-8 Steps for resolving network communication problems with UNIX clients *(continued)*

Step	Action	Description

Step 7	Identify the outbound socket on the server host.	Use the following command to identify the outbound socket that is used for the telnet command from step 6. Specify the appropriate IP address to which the server resolves the policy client. Note the source IP (10.82.105.11), the source port (45856) and the destination port (1556).
		
		`# netstat -na | grep '<client_IP_address>' | egrep '1556|13724|13782|'`
		`10.82.105.11.45856 10.82.104.99.1556 49152 0 49152 0 ESTABLISHED`
		
		If `telnet` is still connected and a socket is not displayed, remove the port number filtering and observe the port number to which the site has mapped the service name. Check that process listens on the port number in step 5.
		
		`$ netstat -na | grep '<client_IP_address>'`
		`10.82.105.11.45856 10.82.104.99.1234 49152 0 49152 0 ESTABLISHED`
		
		If the socket is in a SYN_SENT state instead of an ESTABLISHED state, the server host is trying to make the connection. However, a firewall blocks the outbound TCP SYN from reaching the client host or blocks the return bound TCP SYN+ACK from reaching the server host.

Step 8	Confirm that the telnet connection reaches this client host.	To confirm that the `telnet` connection reaches this client host, run the following command:
		
		`$ netstat -na | grep '<source_port>'`
		`10.82.104.99.1556  10.82.105.11.45856  49152 0 49152 0 ESTABLISHED`
		
		One of the following conditions occurs:
		
		■ If the telnet is connected but the socket is not present, then the telnet reached some other host that incorrectly shares the same IP address as the client host.
		■ If the socket is in a SYN_RCVD state instead of an ESTABLISHED state, then the connection reached this client host. However, a firewall blocks the return of the TCP SYN+ACK to the server host.

Step 9	Verify communication between the client and the master server.	To verify client to master server communications, use the `bpclntcmd` utility. When `-pn` and `-sv` run on a NetBackup client, they initiate inquiries to the NetBackup master server (as configured in the client `bp.conf` file). The master server then returns information to the requesting client. More information is available about `bpclntcmd`. See "About the bpclntcmd utility" on page 65. If you confirm connectivity from the server host to the client host through PBX (port 1556) or to both `bpcd` (port 13782) and `vnetd` (port 13724), then the PBX, `bpcd`, or `vnetd` debug logs should provide details on the nature of any remaining failure.

Resolving network communication problems with PC clients

The following procedure is for resolving NetBackup communications problems, such as those associated with NetBackup status codes 54, 57, and 58. This procedure consists of two variations: one for UNIX clients and another for PC clients.

Note: In all cases, ensure that your network configuration works correctly outside of NetBackup before trying to resolve NetBackup problems.

This procedure helps you resolve network communication problems with PC clients.

To resolve network communication problems

1. Before you retry the failed operation, do the following:
   - Increase the logging level on the client (see the client's user guide).
   - On the NetBackup server, create a `bprd` debug log directory and on the clients create a `bpcd` debug log.
   - On the NetBackup server, set the **Verbose** level to 1.
     See "Changing the logging level on Windows clients" on page 169.
2. If this client is new, verify the client and the server names in your NetBackup configuration.

   See "Verifying host name and service entries in NetBackup" on page 53.
3. Verify network connectivity between client and server by pinging from the server to the client and vice versa. Use the following command:

   ```
   # ping hostname
   ```

   Where *hostname* is the name of the host as configured in the following:
   - NetBackup policy configuration
   - WINS
   - DNS (if applicable).
   - `hosts` file in system directory `%SystemRoot%\system32\drivers\etc\hosts` (Windows XP or 2003)

   If `ping` succeeds in all instances, it verifies connectivity between the server and client.

   If `ping` fails, you have a network problem outside of NetBackup that must be resolved before you proceed. As a first step, verify that the workstation is turned

on. A workstation that is not turned on is a common source of connection problems with PC workstations.

4 On Microsoft Windows clients, ensure that the NetBackup Client service is active by checking the logs. Use the Services application in the Control Panel to verify that the NetBackup Client service is running. Start it if necessary.

- Check the `bpcd` debug logs for problems or errors. Instructions are available on how to enable and use these logs.
  See "About legacy logging" on page 153.
- Verify that the same NetBackup client service (`bpcd`) port number is specified on both the NetBackup client and server (by default, 13782). Do one of the following:

Windows	Check the NetBackup client service port number. Start the **Backup, Archive, and Restore** interface on the client. On the **File** menu, click **NetBackup Client Properties**. In the **NetBackup Client Properties** dialog box on the **Network** tab, check the NetBackup client service port number. Verify that the setting on the **Network** tab matches the one in the services file. The `services` file is located in: `%SystemRoot%\system32\drivers\etc\services` (Windows) The values on the **Network** tab are written to the `services` file when the NetBackup client service starts.
UNIX NetBackup servers	The `bpcd` port number is in the `/etc/services` file. On Windows NetBackup servers, see the Client Properties dialog box in the **Host Properties** window. See "Using the Host Properties window to access configuration settings" on page 67.

Correct the port number if necessary. Then, on Windows clients and servers, stop and restart the NetBackup Client service.

Do not change NetBackup port assignments unless it is necessary to resolve conflicts with other applications. If you do change them, do so on all NetBackup clients and servers. These numbers must be the same throughout your NetBackup configuration.

5 Verify that the NetBackup Request Service (`bprd`) port number on Microsoft Windows is the same as on the server (by default, 13720). Do one of the following:

Windows clients	Check the NetBackup client service port number. Start the **Backup, Archive, and Restore** interface on the client. On the **File** menu, click **NetBackup Client Properties**. In the **NetBackup Client Properties** dialog box on the **Network** tab, check the NetBackup client service port number. Verify that the setting on the **Network** tab matches the one in the services file. The `services` file is located in: `%SystemRoot%\system32\drivers\etc\services` (Windows) The values on the **Network** tab are written to the `services` file when the NetBackup client service starts.
UNIX NetBackup servers	The `bprd` port number is in the `/etc/services` file. See "Using the Host Properties window to access configuration settings" on page 67.
Windows NetBackup servers	Set these numbers in the **Client Properties** dialog box in the Host Properties window. See "Using the Host Properties window to access configuration settings" on page 67.

6 Verify that the `hosts` file or its equivalent contains the NetBackup server name. The `hosts` files are the following:

Windows XP or 2003	`%SystemRoot%\system32\drivers\etc\hosts`
UNIX	`/etc/hosts`

7 Verify client-to-server connectability by using `ping` or its equivalent from the client (step 3 verified the server-to-client connection).

8 If the client's TCP/IP transport allows `telnet` and `ftp` from the server, try these services as additional connectivity checks.

9 Use the `bpclntcmd` utility to verify client to master server communications. When `-pn` and `-sv` run on a client, they initiate inquiries to the master server (as configured in the server list on the client). The master server then returns information to the requesting client.

See "About the bpclntcmd utility" on page 65.

10 Use the `bptestbpcd` utility to try to establish a connection from a NetBackup server to the `bpcd` daemon on another NetBackup system. If successful, it reports information about the sockets that are established.

See "About the bpclntcmd utility" on page 65.

11 Verify that the client operating system is one of those supported by the client software.

About troubleshooting networks and host names

In a configuration with multiple networks and clients with more than one host name, NetBackup administrators must configure the policy entries carefully. They must consider the network configuration (physical, host names and aliases, NIS/DNS, routing tables, and so on). If administrators want to direct backup and restore data across specific network paths, they especially need to consider these things.

For a backup, NetBackup connects to the host name as configured in the policy. The operating system's network code resolves this name and sends the connection across the network path that the system routing tables define. The `bp.conf` file is not a factor making this decision.

For restores from the client, the client connects to the master server. For example, on a UNIX system, the master server is the first one named in the `/usr/openv/netbackup/bp.conf` file. On a Windows system, the master server is specified on the **Server to use for backups and restores** drop-down of the Specify NetBackup Machines and Policy Type dialog box. To open this dialog, start the NetBackup Backup, Archive, and Restore interface and click **Specify NetBackup Machines and Policy Type** on the **File** menu. The client's network code that maps the server name to an IP address determines the network path to the server.

Upon receipt of the connection, the server determines the client's configured name from the peer name of its connection to the server.

The peer name is derived from the IP address of the connection. This means that the address must translate into a host name (using the `gethostbyaddr()` network routine). This name is visible in the `bprd` debug log when a connection is made as in the line:

```
Connection from host peername ipaddress ...
```

The client's configured name is then derived from the peer name by querying the bpdbm process on UNIX systems. On Windows systems, you must query the NetBackup Database Manager service.

The bpdbm process compares the peer name to a list of client names that are generated from the following:

- All clients for which a backup has been attempted
- All clients in all policies

The comparison is first a simple string comparison. The comparison is verified by comparing host names and the aliases that are retrieved by using the network function gethostbyname().

If none of the comparisons succeed, a more brute force method is used, which compares all names and aliases using gethostbyname().

The configured name is the first comparison that succeeds. Note that other comparisons might also have succeeded if aliases or other "network names" are configured.

If the comparison fails, the client's host name as returned by the gethostname() function on the client is used as the configured name. An example of a failed comparison is when the client changes its host name but its new host name is not yet reflected in any policies.

These comparisons are logged in the bpdbm debug log if VERBOSE is set. You can determine a client's configured name by using the bpclntcmd command on the client. For example:

```
# /usr/openv/netbackup/bin/bpclntcmd -pn
```
(UNIX)

```
# install_path\NetBackup\bin\bpclntcmd -pn
```
(Windows)

```
expecting response from server wind.abc.me.com
danr.abc.me.com danr 194.133.172.3 4823
```

Where the first output line identifies the server to which the request is directed and the second output line is the server's response in the following order:

- Peer name of the connection to the server
- Configured name of the client
- IP address of the connection to the server
- Port number that is used in the connection

When the client connects to the server, it sends the following three names to the server:

- Browse client
- Requesting client
- Destination client

The browse client name is used to identify the client files to list or restore from. The user on the client can modify this name to restore files from another client. For example, on a Windows client, the user can change the client name by using the Backup, Archive, and Restore interface. (See the NetBackup online Help for instructions). For this change to work, however, the administrator must also have made a corresponding change on the server.

See the NetBackup Administrator's Guide, Volume I.

The requesting client is the value from the `gethostname()` function on the client.

The destination client name is a factor only if an administrator pushes a restore to a client from a server. For a user restore, the destination client and the requesting client are the same. For an administrator restore, the administrator can specify a different name for the destination client.

By the time these names appear in the `bprd` debug log, the requesting client name has been translated into the client's configured name.

The name that used to connect back to the client to complete the restore is either the client's peer name or its configured name. The type of restore request (for example, from root on a server, from a client, to a different client, and so on) influences this action.

When you modify client names in NetBackup policies to accommodate specific network paths, the administrator needs to consider:

- The client name as configured on the client. For example, on UNIX the client name is `CLIENT_NAME` in the client's `bp.conf` file. On a Windows client, it is on the **General** tab of the NetBackup Client Properties dialog box. To open this dialog box, select **NetBackup Client Properties** from the **File** menu in the Backup, Archive, and Restore interface.
- The client as currently named in the policy configuration.
- The client backup and archive images that already exist as recorded in the `images` directory on the master server. On a UNIX server, the `images` directory is `/usr/openv/netbackup/db/`. On a Windows NetBackup server, the `images` directory is *`install_path`*`\NetBackup\db\images`.

Any of these client names can require manual modification by the administrator if the following: a client has multiple network connections to the server and restores from the client fail due to a connection-related problem.

On UNIX, the public domain program `traceroute` (not included with NetBackup) often can provide valuable information about a network's configuration. Some system vendors include this program with their systems.

The master server may be unable to reply to client requests, if the Domain Name Services (DNS) are used and the following is true: The name that the client obtains through its `gethostname()` library (UNIX) or `gethostbyname()` network (Windows) function is unknown to the DNS on the master server. The client and the server configurations can determine if this situation exists. `gethostname()` or `gethostbyname()` on the client may return an unqualified host name that the DNS on the master server cannot resolve.

Although you can reconfigure the client or the master server DNS hosts file, this solution is not always desirable. For this reason, NetBackup provides a special file on the master server. This file is as follows:

`/usr/openv/netbackup/db/altnames/host.xlate` (UNIX)

`install_path``\NetBackup\db\altnames\host.xlate` (Windows)

You can create and edit this file to force the desired translation of NetBackup client host names.

Each line in the `host.xlate` file has three elements: a numeric key and two host names. Each line is left justified, and a space character separates each element of the line.

`key hostname_from_client client_as_known_by_server`

The following describes the preceding variables:

- *key* is a numeric value used by NetBackup to specify the cases where the translation is to be done. Currently this value must always be 0, which indicates a configured name translation.
- *hostname_from_client* is the value to translate. This value must correspond to the name that the client's `gethostname()` function obtains and sends to the server in the request.
- *client_as_known_by_server* is the name to substitute for *hostname_from_client* when the client responds to requests. This name must be the name that is configured in the NetBackup configuration on the master server. It must also be known to the master server's network services.

This following is an example:

```
0 danr danr.eng.aaa.com
```

When the master server receives a request for a configured client name (numeric key 0), the name `danr` always replaces the name `danr.eng.aaa.com`. The problem is resolved, assuming the following:

- The client's `gethostname()` function returns `danr`.
- The master server's network services `gethostbyname()` 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.

Verifying host name and service entries in NetBackup

This procedure is useful if you encounter problems with host names or network connections and want to verify that the NetBackup configuration is correct. Several examples follow the procedure.

For more information on host names, see the NetBackup Administrator's Guide, Volume II.

See "About troubleshooting networks and host names" on page 49.

To verify the host name and service entries in NetBackup

1 Verify that the correct client and server host names are configured in NetBackup. The action you take depends on the computer that you check.

On Windows servers and Windows clients

Do the following:

- On the **Server to use for backups and restores** drop-down list, ensure that a server entry exists for the master server and each media server.
  Start the **Backup, Archive, and Restore** interface on the client. On the **File** menu, click **Specify NetBackup Machines and Policy Type**. In the **Specify NetBackup Machines and Policy Type** dialog box, click the **Server to use for backups and restores** drop-down list.
  On Windows systems, the correct server must be designated as the current master server in the list. If you add or modify server entries on the master server, stop and restart the NetBackup Request service and NetBackup Database Manager services.
  On UNIX systems, if you add or modify `SERVER` entries on the master server, stop and restart `bprd` and `bpdbm`.
- On the **General** tab, verify that the client name setting is correct and matches what is in the policy client list on the master server.
  Start the **Backup, Archive, and Restore** interface on the client. On the **File** menu, click **NetBackup Client Properties**. In the **NetBackup Client Properties** dialog box, click the **General** tab.
- On a master or a media server, ensure that a server entry exists for each Windows administrative client to use to administer that server.
- Ensure that host names are spelled correctly in the `bp.conf` file (UNIX) or in the servers list (Windows) on the master server. If a host name is misspelled or cannot be resolved by using `gethostbyname`, the following error messages are logged on the NetBackup error log:

```
Gethostbyname failed for
<host_name>:<h_errno_string> (<h_errno>)
One or more servers was excluded from the server
list because gethostby name() failed.
```

You can also make these changes on the appropriate tabs in the properties dialog boxes on a Windows NetBackup server

See "Using the Host Properties window to access configuration settings" on page 67.

On UNIX NetBackup servers and clients and Macintosh clients

Check the server and the client name entries in the `bp.conf` file by doing the following:

- Ensure that a `SERVER` entry exists for the master server and each media server in the configuration. The master server must be the first name in the list.
  If you add or modify `SERVER` entries on the master server, stop and restart `bprd` and `bpdbm` before the changes take effect.
- The bp.conf of the master server does not require the addition of other clients, other than the master server as CLIENT_NAME = master server name. The name is added by default.

The `bp.conf` file is in the `/usr/openv/netbackup` directory on UNIX clients and it is in the `Preferences:NetBackup` folder on Macintosh clients.

Users on UNIX clients can also have a personal `bp.conf` file in their home directory. A `CLIENT_NAME` option in `$HOME/bp.conf` overrides the option in `/usr/openv/netbackup/bp.conf`.

On the master server

Verify that you have created any of the following required files:

- `/usr/openv/netbackup/db/altnames` files (UNIX)
- `install_path\NetBackup\db\altnames` files (Windows)

Pay particular attention to requirements for `host.xlate` file entries.

2 Verify that each server and client have the required entries for NetBackup reserved port numbers.

The following examples show the default port numbers.

See "Example of host name and service entries on UNIX master server and client" on page 57.

See "Example of host name and service entries on UNIX master server and media server" on page 59.

See "Example of host name and service entries on UNIX PC clients" on page 60.

See "Example of host name and service entries on UNIX clients in multiple networks" on page 61.

See "Example of host name and service entries on UNIX server that connects to multiple networks" on page 64.

Do not change NetBackup port assignments unless it is necessary to resolve conflicts with other applications. If you do change them, do so on all NetBackup clients and servers. These numbers must be the same throughout your NetBackup configuration.

3 On NetBackup servers, check the services files to ensure that they have entries for the following:

- bpcd and bprd
- vmd
- bpdbm
- Processes for configured robots (for example, tl8cd).
  See the NetBackup Device Configuration Guide.

Verify the NetBackup client daemon or service number, and the request daemon or service port number. The action you take depends on whether the client is UNIX or Microsoft Windows.

On UNIX clients	Check the bprd and the bpcd entries in the /etc/services file.
On Microsoft Windows clients	Verify that the NetBackup Client Service Port number and NetBackup Request Service Port number match settings in the services file by doing the following: Start the Backup, Archive, and Restore interface on the client. On the **File** menu, click **NetBackup Client Properties**. In the **NetBackup Client Properties** dialog box on the **Network** tab, select the following: The NetBackup Client Service Port number and NetBackup Request Service Port number. The values on the **Network** tab are written to the services file when the NetBackup Client service starts. The services file is in the following location: %SystemRoot%\system32\drivers\etc\services

4 On UNIX servers and clients, check the /etc/inetd.conf file to ensure that it has the following entry:

```
bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd
```

5 On Windows servers and clients, verify that the NetBackup Client service is running.

6 If you use NIS in your network, update those services to include the NetBackup information that is added to the /etc/services file.

7 NIS, WINS, or DNS host name information must correspond to what is in the policy configuration and the name entries. On Windows NetBackup servers and Microsoft Windows clients, do the following:

- Check the **General** tab:

Start the **Backup, Archive, and Restore** interface on the client. On the **File** menu, click **NetBackup Client Properties**. In the **NetBackup Client Properties** dialog box, click the **General** tab.

- Check the **Server to use for backups and restores** drop-down list: Start the **Backup, Archive, and Restore** interface on the client. On the **File** menu, click **Specify NetBackup Machines and Policy Type**. In the **Specify NetBackup Machines and Policy Type** dialog box, click the **Server to use for backups and restores** drop-down list.
- The `bp.conf` file on UNIX servers and clients and Macintosh clients.

Also, verify that reverse DNS addressing is configured.

8 Use the `bpclntcmd` utility to confirm the setup of the IP addresses and host names in DNS, NIS, and local hosts files on each NetBackup node.

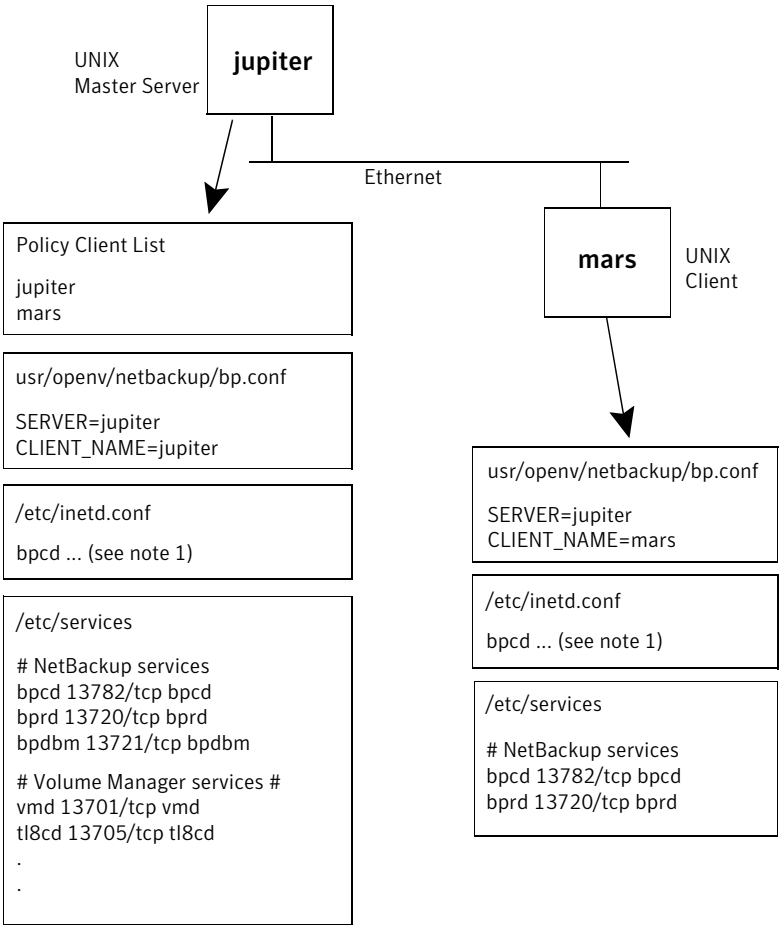
Note: FT (Fibre Transport) target devices are named based on the host name or domain name response from the device. If any alternate computer names for different VLAN network interface names appear in the SERVER/MEDIA_SERVER entries of the DNS (Domain Name System) or the host files, the primary name must appear first.

See "About the bpclntcmd utility" on page 65.

Example of host name and service entries on UNIX master server and client

The following illustration shows a UNIX master server with one UNIX client.

Figure 2-1 UNIX master server and client



Consider the following notes about Figure 2-1:

- The following is the complete `inetd.conf` entry:

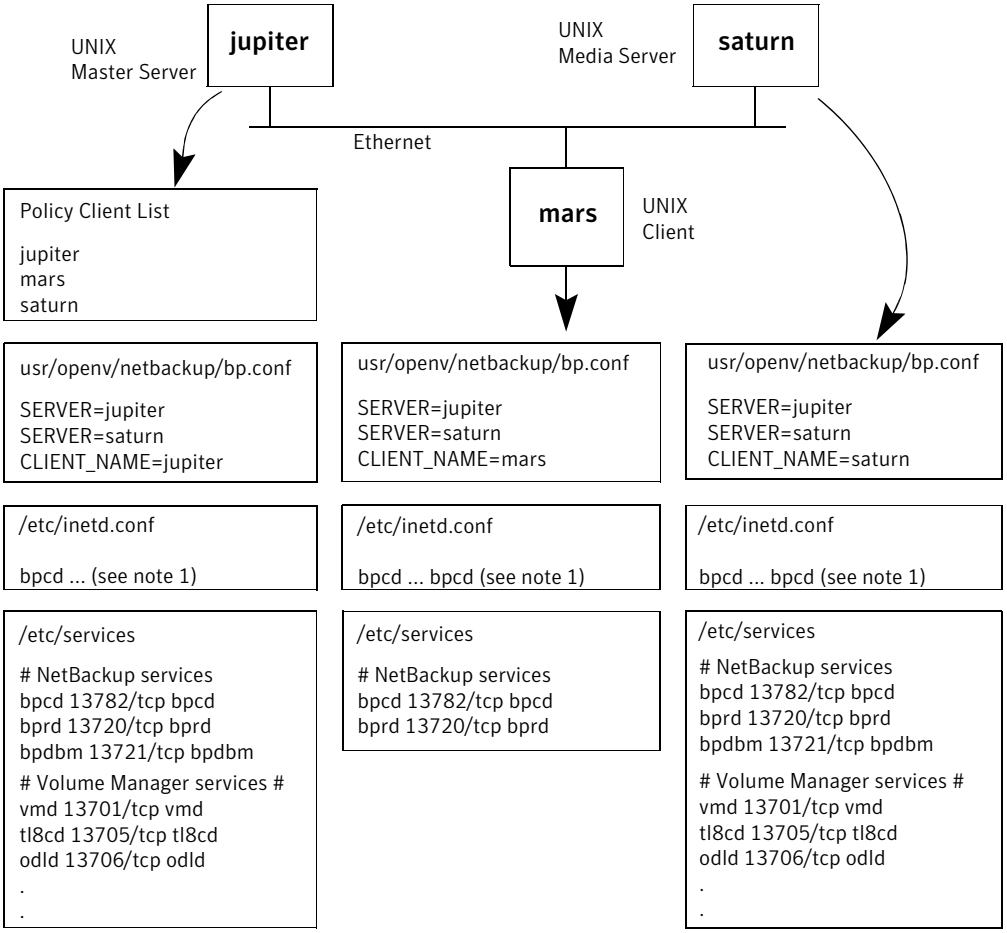
  ```
  bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd
  ```

- All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this information could include the `/etc/hosts` file and NIS, and DNS (if used).

Example of host name and service entries on UNIX master server and media server

The following illustration shows a UNIX NetBackup media server named *saturn*. Note the addition of a `SERVER` entry for *saturn* in the `bp.conf` files on all the systems. This entry is second, beneath the one for the master server *jupiter*.

Figure 2-2 UNIX master and media servers



Consider the following notes about Figure 2-2:

- The following is the complete `inetd.conf` entry:

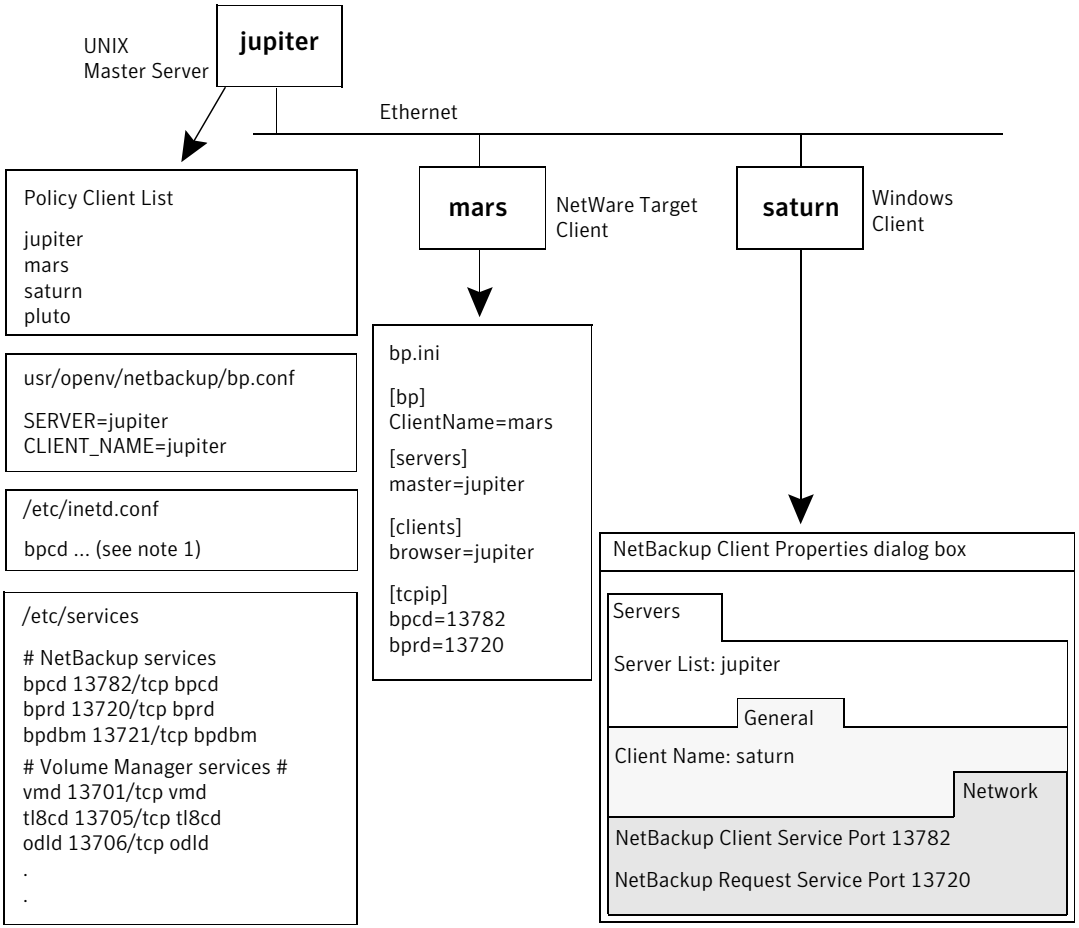
```
bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd
```

- All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this information could include the `/etc/hosts` file and NIS, and DNS (if used).

Example of host name and service entries on UNIX PC clients

The following illustration shows a NetBackup master server with PC clients, defined here as Windows or Macintosh clients. Server configuration is the same as it is for UNIX clients. These clients do not have `inetd.conf` entries.

Figure 2-3 UNIX PC clients



Consider the following notes about Figure 2-3:

- The following is the complete `inetd.conf` entry:

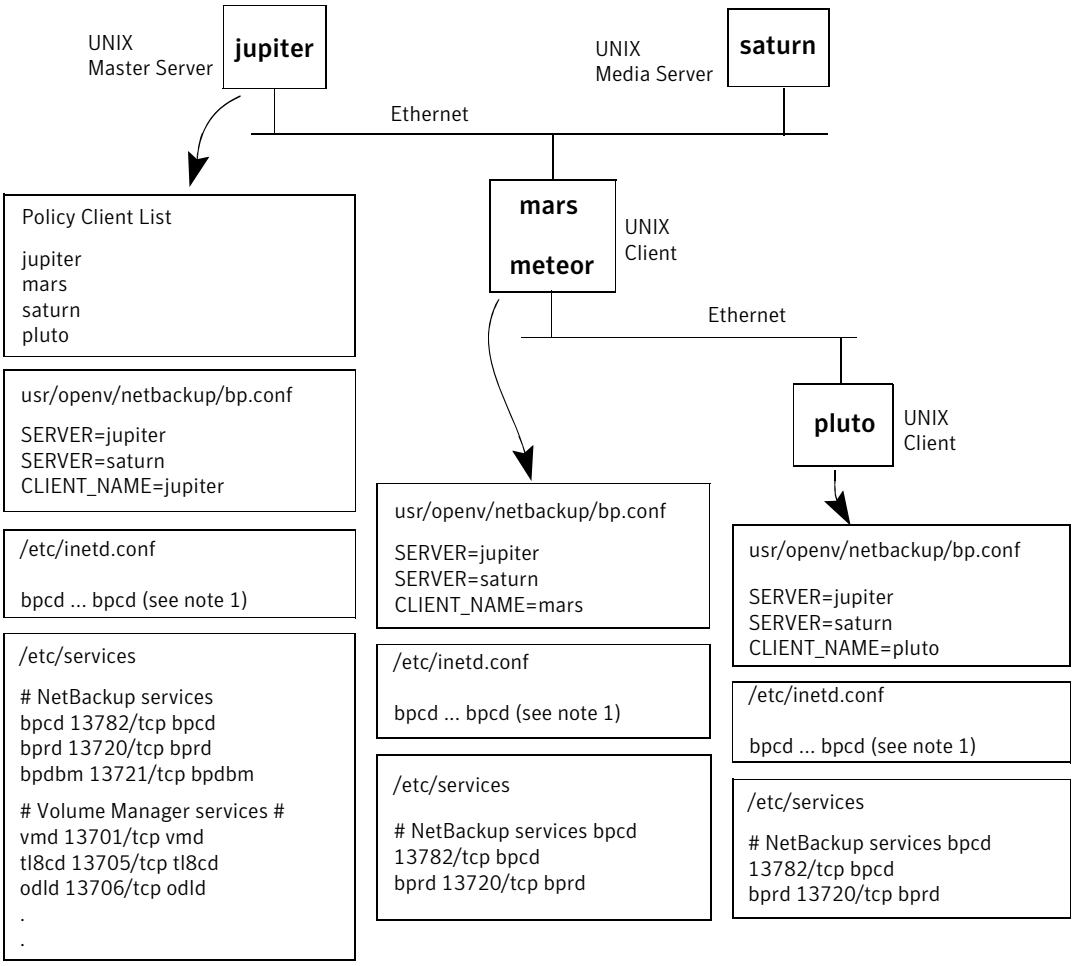
  ```
  bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd
  ```

- All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this information could include the `/etc/hosts` file and NIS, and DNS (if used).

Example of host name and service entries on UNIX clients in multiple networks

The following illustration shows a client that is a router to clients in another network. The client host name on the master server side is *mars* and the host name that is presented to the client *pluto* is *meteor*.

Figure 2-4 UNIX clients in multiple networks



Consider the following notes about Figure 2-4:

- The following is the complete `inetd.conf` entry:

  ```
  bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd
  ```

- All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this information could include the `/etc/hosts` file and NIS, and DNS (if used).

The policy client list shows the configuration of the router system as *mars* because that is the name of the interface to the master server. Other than the client name

setting, this setup has no special configuration. This name must be set to *mars*, because *mars* is the name that the master server recognizes.

The second client, *pluto*, is also configured no differently than if it were in the same network as the master server. If all the standard networking files (hosts, NIS, DNS, WINS, and routing tables) are set up correctly, all the required network connections can be made.

However, to restore files from *pluto* would be a problem in the following situation: the *mars-meteor* system is a type of router that hides the name of the originating host when it routes requests between the two networks. For example, a router between an Ethernet and a token ring network exhibits this behavior.

To illustrate what occurs, assume that *pluto* is on FDDI (token ring) and the server is on Ethernet. Then a user on *pluto* starts a restore. The router can use the name of its network interface to *pluto* (*meteor*) as the peer name when it forwards the request to the server. The server interprets the request as coming from a host that is named *meteor*. It does not allow the restore because *meteor* is not in the client list.

To resolve this problem, the administrator creates an `altnames` directory on the master server and adds a file for *meteor* to that directory.

On a Windows NetBackup server, the file path is:

```
install_path\netbackup\db\altnames\meteor
```

On a UNIX NetBackup server, the file path is:

```
/usr/openv/netbackup/db/altnames/meteor
```

Then, the administrator adds the following line to this file:

```
pluto
```

The master server now recognizes as legitimate any of the restore requests with a peer name of *meteor* and client name of *pluto*.

Regardless of the type of router, the configuration for the media server, *saturn*, is the same as in another example.

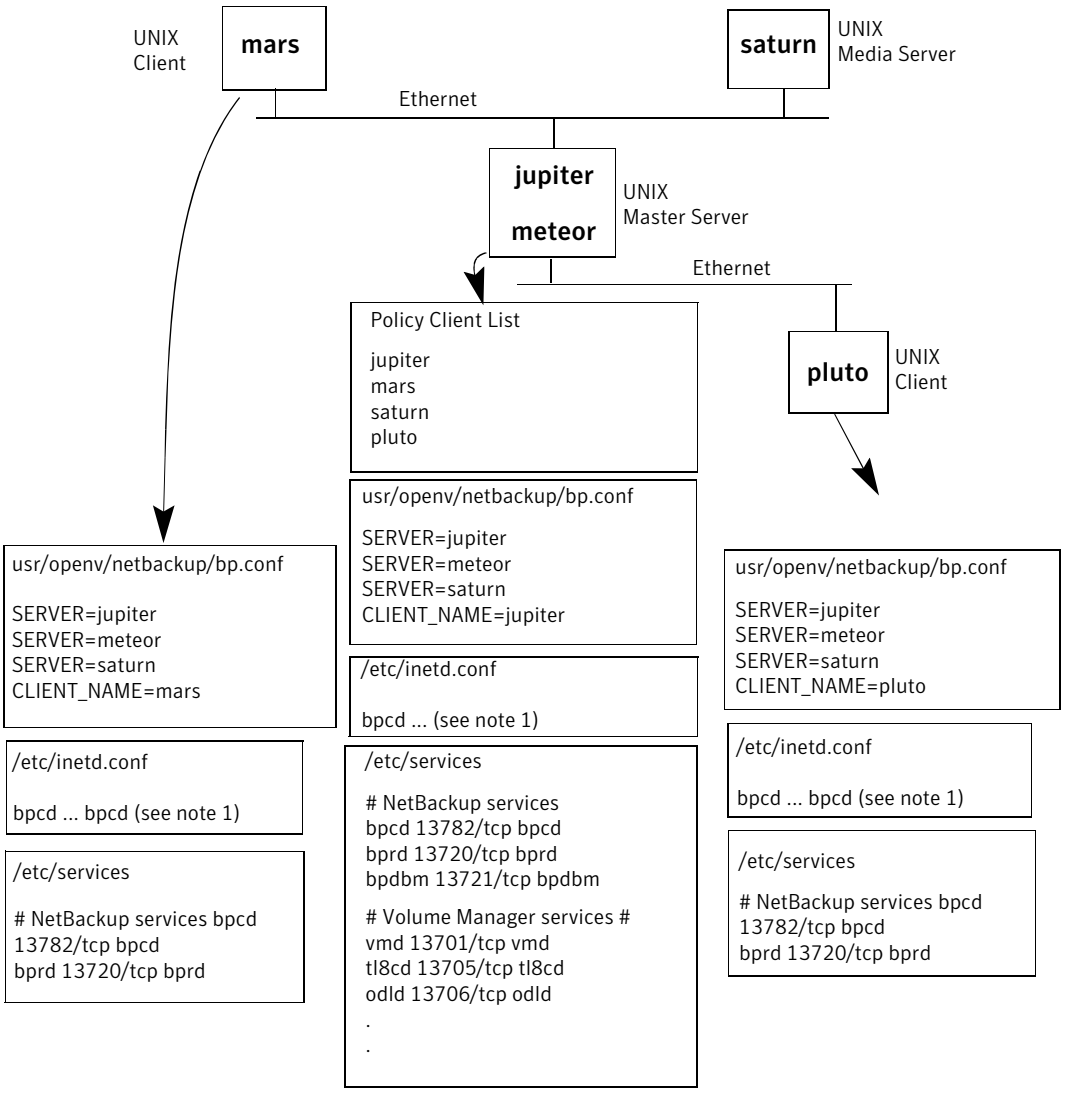
See “Example of host name and service entries on UNIX master server and media server” on page 59.

If a media server is involved in a backup or restore for *pluto*, the master server provides the following: the correct peer name and client name for the media server to use to establish connections.

Example of host name and service entries on UNIX server that connects to multiple networks

The following illustration shows an NBU server with two Ethernet connections and clients in both networks. The server host name is *jupiter* on one and *meteor* on the other.

Figure 2-5 UNIX server connects to multiple networks



Consider the following notes about Figure 2-5:

- The complete inetd.conf entry is:

```
bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd
```

- All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this information could include the `/etc/hosts` file and NIS, and DNS (if used).

This example illustrates a UNIX server that connects to multiple networks. The NetBackup policy client list specifies *jupiter* as the client name for the master server. The list can show either *jupiter* or *meteor* but not both.

The NetBackup server list on the master server has entries for both *jupiter* and *meteor*. The reason for both is that when the server does a backup, it uses the name that is associated with the client it backs up. For example, it uses the *meteor* interface when it backs up *pluto* and the *jupiter* interface when it backs up *mars*. The first server entry (master server name) is *jupiter* because that is the name used to back up the client on the master server.

The NetBackup server list for the other systems also has entries for both the *jupiter* and the *meteor* interfaces. This setup is recommended to keep the server entries the same on all clients and servers in the configuration. It would be adequate to list only the master-server name for the local network interface to the client system or media server. (For example, list *meteor* for *pluto*.)

For the network that is shown, the only configurations that are required are the differences for the policy client list and the server list. If all the standard networking files (hosts, WINS, NIS, DNS, and routing tables) are set up correctly, all required network connections can be made.

A problem exists to restore the files in the following situation: the master server system is a router that hides the originating host name when it routes requests between networks. For example, if *pluto* were on FDDI (token ring), the master server would use *meteor* as the peer name when it forwards the request to NetBackup. NetBackup would then interpret the request as coming from a host that is named *meteor*, which was not in the client list. The restore would fail.

The solution, in this case, is identical to the solution that is discussed in the following:

About the bpclntcmd utility

The `bpclntcmd` utility resolves IP addresses into host names and host names into IP addresses. It uses the same system calls as the NetBackup application modules. The following directory contains the command that starts the utility:

Windows	`install_path\NetBackup\bin`
UNIX	`/usr/openv/netbackup/bin`

On Windows, run this `bpclntcmd` command in an MS-DOS command window so you can see the results.

The `bpclntcmd` options that are useful for testing the functionality of the host name and IP address resolution are `-ip`, `-hn`, `-sv`, and `-pn`. The following topics explain each of these options:

-ip `bpclntcmd -ip IP_Address`

The `-ip` option lets you specify an IP address. `bpclntcmd` uses `gethostbyaddr()` on the NetBackup node and `gethostbyaddr()` returns the host name with the IP address as defined in the following: the node's DNS, WINS, NIS, or local hosts file entries. No connection is established with the NetBackup server.

-hn `bpclntcmd -hn Hostname`

The `-hn` option specifies a host name. `bpclntcmd` uses `gethostbyname()` on the NetBackup node to obtain the IP address that is associated with the host name defined in the following: the node's DNS, WINS, NIS, or local hosts file entries. No connection is established with the NetBackup server.

-sv `bpclntcmd -sv`

The `-sv` option displays the NetBackup version number on the master server.

-pn When the `-pn` option is run on a NetBackup client, it initiates an inquiry to the NetBackup master server. The server then returns information to the requesting client. First, the server is the Current Server in the server list. Then it displays the information that the server returns. For example:

```
bpclntcmd -pn
expecting response from server rabbit.friendlyanimals.com
dove.friendlyanimals.com dove 123.145.167.3 57141
```

The following is true of this command example:

- `expecting response from server rabbit.friendlyanimals.com` is the master server entry from the server list on the client.
- `dove.friendlyanimals.com` is the connection name (peer name) returned by the master server. The master server obtained this name through `gethostbyaddress()`.
- `dove` is the client name configured in the NetBackup policy client list.
- `123.145.167.3` is the IP address of the client connection at the master server.
- `57141` is the port number of the connection on the client.

Use `-ip` and `-hn` to verify the ability of a NetBackup node to resolve the IP addresses and host names of other NetBackup nodes.

For example, to verify that a NetBackup server can connect to a client, do the following:

- On the NetBackup server, use `bpclntcmd -hn` to verify the following: The operating system can resolve the host name of the NetBackup client (as configured in the client list for the policy) to an IP address. The IP address is then used in the node's routing tables to route a network message from the NetBackup server.
- On the NetBackup client, use `bpclntcmd -ip` to verify that the operating system can resolve the IP address of the NetBackup server. (The IP address is in the message that arrives at the client's network interface.)

Using the Host Properties window to access configuration settings

The **Host Properties** window in the **NetBackup Administration Console** provides access to many configuration settings for NetBackup clients and servers. For example, you can modify the server list, email notification settings, and various timeout values for servers and clients. The following are general instructions for using this window.

The **NetBackup Client Properties** dialog box in the **Backup, Archive, and Restore** interface on Windows clients lets you change NetBackup configuration settings only for the local system where you are running the interface. Most settings in the **NetBackup Client Properties** dialog box are also available in the **Host Properties** window.

To use the Host Properties window to access configuration settings

1. In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Host Properties**.
2. Depending on the host to be configured, select **Master Servers**, **Media Servers**, or **Clients**.
3. On the **Actions** menu, select **Properties**.
4. In the **Properties** dialog box, in the left pane, click the appropriate property and make your change.

Resolving full disk problems

If the NetBackup installation directory fills up, such as with logging files, a number of problems can result. NetBackup may become unresponsive. For example, NetBackup jobs may remain queued for long periods, even though all NetBackup processes and services are running.

To resolve full disk problems

1. The NetBackup Resource Broker (`nbrb`) log may have database connection errors in it. These errors indicate failed tries to establish connections to the `nbemm` database. The following is an example of such errors in the `nbrb` log:

```
7/20/2005 12:33:47.239 [RBDatabase::connectDatabase()] ODBC connection failed.
ErrMsg: [Sybase][ODBC Driver][Adaptive Server Anywhere]Disk write failure
'Fatal error: disk write failure C:\Program Files\VERITAS\NetBackupDB\data\NBDB.log' --
transaction rolled back ErrCode: -1Sqlstate: HY000
```

   The `nbrb` log (originator ID 118) is written in `/usr/openv/logs` (UNIX) or *`install_path`*`\NetBackup\logs` (Windows). .

   See "About logs" on page 127. for more information about unified logging.

2. To correct the situation, clear up disk space in the directory where NetBackup is installed by doing the following:
   - You may need to delete log files manually, reduce logging levels, and adjust log retention to have log files automatically deleted sooner.
     More information is available about logging levels, log file retention, and how to configure unified logging.

See “About logs” on page 127.

- Consider moving the NetBackup unified logging files to a different file system.
  See “About changing the location of unified log files” on page 140.

3. Use the Activity Monitor to verify that the NetBackup relational database service is running. This service is the `NB_dbsrv` daemon on UNIX and the "Adaptive Server Anywhere - Veritas_NB" service on Windows.
4. If the NetBackup relational database service is stopped, note the following:
   - Do not stop the `nbrb` service. If you stop the `nbrb` service while the NetBackup relational database service is down, it can result in errors.
   - Restart the NetBackup relational database service.

   Verify that the NetBackup relational database service is running. If it is not and you remove files to free up disk space, you may not fix the problem. The relational database service must be restarted to allow the Resource Broker (`nbrb`) to allocate job resources.

Frozen media troubleshooting considerations

Frozen media can cause a number of problems including one of the following status codes: 84, 85, 86, 87 and 96.

When troubleshooting frozen media, be aware of the following:

- Be sure that the media server that freezes the media stores the actual FROZEN status of that media in its media database (`MediaDB`). Every media server including the master server has its own unique media database.
- Use the `bpmedialist` command to access the `MediaDB` information including the media status (Frozen, Full, or Active).
- To unfreeze the media, use the `bpmedia` command. Specify the media server that contains that frozen record in the command syntax. Unfreeze the media one at a time.
- Frozen media does not necessarily mean that the media is defective. NetBackup may freeze media as a safety measure to prevent further errors, drive damage, or data loss.
- Investigate any patterns to the media IDs, tape drives, or media servers that are involved when media is frozen.

Logs for troubleshooting frozen media

The following logs are useful when you troubleshoot frozen media:

UNIX

- The `bptm` log from the media servers that froze the media:

  `/usr/openv/netbackup/logs/bptm`

- The Admin messages or syslog from the operating system.

Windows

- The `bptm` log from the media servers that froze the media:

  `install_dir``\VERITAS\NetBackup\logs\bptm`

- The Windows Event Viewer System Log
- The Windows Event Viewer Application Log

Set the verbosity of the `bptm` process log to 5 to troubleshoot any media and drive-related issues. This log does not use excessive drive space or resources even at an elevated verbosity. When media is frozen, the `bptm` logs may contain more detailed information that the Activity Monitor or Problems Report. Set the verbosity for `bptm` on individual media servers by changing their logging levels under Host Properties on the NetBackup Administration Console.

See "Frozen media troubleshooting considerations" on page 69.

See "About conditions that cause media to freeze" on page 70.

About conditions that cause media to freeze

The following conditions can cause media to freeze:

- The same media has excessive errors during backup. An example of the log entry is as follows:

  ```
  FREEZING media id E00109, it has had at least 3 errors in the last
  12 hour(s)
  ```

  Causes and resolutions for this problem include:

Dirty drives	Clean the drives that are freezing the media according to the manufacturer's suggestions. Frozen media is one of the first symptoms of a dirty drive.
The drive itself	Check for the tape device errors that the operating system logs or the device driver reports. If any are found, follow the hardware manufacturer's recommendations for this type of error.

Communication issues at the SCSI or host bus adapter (HBA) level	Check for SCSI or HBA device errors the operating system logs or the device driver reports. If any are found, follow the hardware manufacturer's recommendations for this type of error.
Drive not supported	Ensure that the tape drives appear on the hardware compatibility list as supported for NetBackup. This list is located on the following Symantec Support website: http://www.symantec.com/business/support/overview.jsp?pid=15143
Media not supported	Ensure that the media is supported for use with the tape drive by the tape drive vendor.

- An unexpected media is found in the drive. An example of the log entry is as follows:

```
Incorrect media found in drive index 2, expected 30349,     \
found 20244, FREEZING 30349
```

  The following conditions can cause this error:

  - NetBackup requests a media ID to be mounted in a drive. If the media ID that is physically recorded on the tape is different than the NetBackup media ID, the media freezes. This error occurs if the robot needs to be inventoried, or if barcodes have been physically changed on the media.
  - Another NetBackup installation previously wrote to the media with different barcode rules.
  - The drives in the robot are not configured in order within NetBackup, or they are configured with the wrong tape paths. The correct robot drive number is important to the proper mounting and use of media. The robot drive number is normally based on the relationship of the drive serial number with the drive serial number information from the robotic library. Validate this number before you consider that the device configuration is complete.

- The media contain a non-NetBackup format. An example of the log entry is as follows:

```
FREEZING media id 000438, it contains MTF1-format data and cannot
be used for backups
FREEZING media id 000414, it contains tar-format data and cannot
be used for backups
FREEZING media id 000199, it contains ANSI-format data and cannot
be used for backups
```

  These library tapes may have been written outside of NetBackup. By default, NetBackup only writes to a blank media or other NetBackup media. Other media

types (DBR, TAR, CPIO, ANSI, MTF1, and recycled Backup Exec BE-MTF1 media) are frozen as a safety measure. Change this behavior by using the following procedure:

On UNIX

To allow NetBackup to overwrite foreign media, add the following to the `bp.conf` file that is located at `/usr/openv/netbackup/bp.conf` for the related media server:

```
ALLOW_MEDIA_OVERWRITE = DBR
ALLOW_MEDIA_OVERWRITE = TAR
ALLOW_MEDIA_OVERWRITE = CPIO
ALLOW_MEDIA_OVERWRITE = ANSI
ALLOW_MEDIA_OVERWRITE = MTF1
ALLOW_MEDIA_OVERWRITE = BE-MTF1
```

Stop and restart the NetBackup daemons for the changes to take effect.

On Windows

On the Administration Console, proceed to **Host Properties | Media Server**

Open the properties for the media server in question.

Select the **Media** tab.

The **Allow Media Overwrite** property overrides the NetBackup overwrite protection for specific media types. To disable the overwrite protection, select one or more of the listed media formats. Then stop and restart the NetBackup services for the changes to take effect.

Do not select a foreign media type for overwriting unless you are sure that you want to overwrite this media type.

For more details about each media type, see the NetBackup Device Configuration Guide.

- The media is a tape formerly used for the NetBackup catalog backup. For example, the log entry may be the following:

  ```
  FREEZING media id 000067: it contains Symantec NetBackup (tm)
  database backup data and cannot be used for backups.
  ```

  The media is frozen because it is an old catalog backup tape which NetBackup does not overwrite by default. The `bplabel` command must label the media to reset the media header.

- The media is intentionally frozen. You can use the `bpmedia` command to manually freeze media for a variety of administrative reasons. If no record exists of a specific job freezing the media, the media may have been frozen manually.

- The media is physically write protected. If the media has a write-protect notch that is set for write protection, NetBackup freezes the media.

To unfreeze frozen media, enter the following `bpmedia` command:

```
# bpmedia -unfreeze -m mediaID -h media_server
```

The *media_server* variable is the one that froze the media. If this item is unknown, run the `bpmedialist` command and note the "Server Host:" listed in the output. The following example shows that media server `denton` froze media `div008`:

```
# bpmedialist -m div008

Server Host = denton

ID    rl images  allocated      last updated    density  kbytes restores
         vimages expiration      last read      <------- STATUS ------->
-------------------------------------------------------------------------

DIV08  1    1    04/22/2010 10:12 04/22/2010 10:12  hcart     35     5
            1    05/06/2010 10:12 04/22/2010 10:25  FROZEN
```

Resolving PBX problems

The Enterprise Media Manager (EMM) services and other services of NetBackup require a common services framework that is called Private Branch Exchange (PBX). Like `vnetd`, PBX helps limit the number of TCP/IP ports that the CORBA services of NetBackup use.

To resolve PBX problems

1. Check that the PBX is properly installed. If PBX is not installed, NetBackup is unresponsive. Refer to the following procedure:

   See "Checking PBX installation" on page 74.

2. Check that PBX is running, and initiate PBX if necessary by using the following procedure:

   See "Checking that PBX is running" on page 74.

3. Check that PBX is correctly configured. If PBX is incorrectly configured, NetBackup is unresponsive. Refer to the following procedure:

   See "Checking that PBX is set correctly" on page 75.

4. Access and check the PBX logs by using the following procedure:

   See "Accessing the PBX logs" on page 76.

5 Check the PBX security and correct any problem by using the following procedure:

See “Troubleshooting PBX security” on page 77.

6 Check that the required NetBackup daemon or service is running. If necessary, start the needed daemon or service by using the following procedure:

See “Determining if the PBX daemon or service is available” on page 78.

Checking PBX installation

NetBackup requires the Symantec Private Branch Exchange service (PBX). PBX can be installed before NetBackup or during NetBackup installation.

See the NetBackup Installation Guide.

If you uninstall PBX, you must reinstall it.

To check PBX installation

1 Look for the following directory on the NetBackup master server:

- On UNIX: `/opt/VRTSpbx`
- On Windows: *`install_path`*`\VxPBX`

2 To check the version of PBX, enter the following:

- On UNIX: `/opt/VRTSpbx/bin/pbxcfg -v`
- On Windows: *`install_path`*`\VxPBX\bin\pbxcfg -v`

Checking that PBX is running

After you know that PBX is installed on the NetBackup master server, you need to verify that it is running.

To see if PBX is running

1 On UNIX, check for the PBX process:

```
ps | grep pbx_exchange
```

2 To start PBX on UNIX, type the following:

```
/opt/VRTSpbx/bin/vxpbx_exchanged start
```

On Windows, make sure that the Private Branch Exchange service isSymantec started. (Go to **Start > Run** and enter `services.msc`.)

Checking that PBX is set correctly

Two settings are vital to the correct functioning of PBX: Auth User (authenticated user) and Secure Mode. When PBX is installed, they are automatically set as required.

To check that PBX is set correctly

1 To display the current PBX settings, do one of the following:

- On UNIX, type the following:

  /opt/VRTSpbx/bin/pbxcfg -p

  Example output:

  ```
  Auth User:0 : root
   Secure Mode: false
   Debug Level: 10
   Port Number: 1556
   PBX service is not cluster configured
  ```

  `Auth User` must be `root` and `Secure Mode` must be `false`.

- On Windows, type the following:

  ***install_path*\VxPBX\bin\pbxcfg -p**

  Example output:

  ```
  Auth User:0 : localsystem
   Secure Mode: false
   Debug Level: 10
   Port Number: 1556
   PBX service is not cluster configured
  ```

  `Auth User` must be `localsystem` and `Secure Mode` must be `false`.

2 Reset `Auth User` or `Secure Mode` as needed:

- To add the correct user to the authenticated user list (UNIX example):

  /opt/VRTSpbx/bin/pbxcfg -a -u root

- To set `Secure Mode` to false:

  /opt/VRTSpbx/bin/pbxcfg -d -m

  For more information on the `pbxcfg` command, refer to the `pbxcfg` man page.

Accessing the PBX logs

PBX uses unified logging. PBX logs are written to the following:

- `/opt/VRTSpbx/log` (UNIX)
- *`install_path`*`\VxPBX\log` (Windows)

The unified logging originator number for PBX is 103. More information is available about unified logging.

See "About unified logging" on page 129.

Error messages regarding PBX may appear in the PBX log or in the unified logging logs for `nbemm`, `nbpem`, `nbrb`, or `nbjm`. The following is an example of an error that is related to PBX:

```
05/11/10 10:36:37.368 [Critical] V-137-6 failed to initialize ORB:
 check to see if PBX is running or if service has permissions to
 connect to PBX. Check PBX logs for details
```

To access the PBX logs

1. Use the `vxlogview` command to view PBX and other unified logs. The originator ID for PBX is 103. For more information, see the `vxlogview` man page. You can also refer to the following topic:

   See "About unified logging" on page 129.

2. To change the logging level for PBX, enter the following:

   ```
   pbxcfg -s -l debug_level
   ```

   where *debug_level* is a number from 0 to 10, where the settings 10 is the most verbose.

   PBX may log messages by default to the UNIX system logs (`/var/adm/messages` or`/var/adm/syslog`) or to the Windows event log. As a result, the system logs may fill up with unnecessary PBX log messages, since the messages are also written to the PBX logs (/opt/VRTSpbx/log on UNIX and <install_path>\VxPBX\log on Windows).

3. To disable PBX logging to the system or event logs, enter the following command:

   ```
   # vxlogcfg -a -p 50936 -o 103 -s LogToOslog=false
   ```

   You do not have to restart PBX for this setting to take effect.

Troubleshooting PBX security

The PBX `Secure Mode` must be set to `false`. If `Secure Mode` is `true`, NetBackup commands such as `bplabel` and `vmoprcmd` do not work. PBX messages similar to the following appear in `/opt/VRTSpbx/log` (UNIX) or *`install_path`*`\VxPBX\log` (Windows).

```
5/12/2008 16:32:17.477 [Error] V-103-11 User MINOV\Administrator
 not authorized to register servers
 5/12/2008 16:32:17.477 [Error] Unauthorized Server
```

To troubleshoot PBX security

1. Set `Secure Mode` to `false` by entering the following:
   - On UNIX:

     ```
     /opt/VRTSpbx/bin/pbxcfg -d -m
     ```

   - On Windows:

     ```
     install_path\VxPBX\bin\pbxcfg -d -m
     ```

2. Verity the PBX security settings by entering the following:

   `pbxcfg -p`

3. Stop NetBackup:
   - On UNIX:

     ```
     /usr/openv/netbackup/bin/bp.kill_all
     ```

   - On Windows:

     ```
     install_path\NetBackup\bin\bpdown
     ```

4. Stop PBX:
   - On UNIX:

     ```
     /opt/VRTSpbx/bin/vxpbx_exchanged stop
     ```

   - On Windows: Go to **Start > Run**, enter `services.msc`, and stop the Symantec Private Branch Exchange service.

5. Start PBX:

- On UNIX:

  ```
  /opt/VRTSpbx/bin/vxpbx_exchanged start
  ```

- On Windows: Go to **Start > Run**, enter `services.msc`, and start the Symantec Private Branch Exchange service.

6 Start NetBackup:

- On UNIX:

  ```
  /usr/openv/netbackup/bin/bp.start_all
  ```

- On Windows:

  install_path\NetBackup\bin\bpup

Determining if the PBX daemon or service is available

If NetBackup does not work as configured, a required NetBackup service may have stopped. For example, backups may not be scheduled or may be scheduled but are not running. The type of problem depends on which process is not running.

When a NetBackup service is not running and another process tries to connect to it, messages similar to the following appear in `/usr/openv/logs` for PBX. (The unified logging originator for PBX is 103.)

```
05/17/10 9:00:47.79 [Info] PBX_Manager:: handle_input with fd = 4
05/17/10 9:00:47.79 [Info] PBX_Client_Proxy::parse_line, line = ack=1
05/17/10 9:00:47.79 [Info] PBX_Client_Proxy::parse_line, line =
extension=EMM
05/17/10 9:00:47.80 [Info] hand_off looking for proxy for = EMM
05/17/10 9:00:47.80 [Error] No proxy found.
05/17/10 9:00:47.80 [Info] PBX_Client_Proxy::handle_close
```

To determine if the PBX daemon or service is available

1 Start the needed service.

  In this example, the missing NetBackup service is EMM. To start the needed service, enter the `nbemm` command (UNIX) or start the NetBackup Enterprise Media Manager service (Windows; **Start > Run**, enter `services.msc`).

2 If necessary, stop and restart all NetBackup services.

- On UNIX:

```
/usr/openv/netbackup/bin/bp.kill_all
/usr/openv/netbackup/bin/bp.start_all
```

- On Windows:

```
install_path\NetBackup\bin\bpdown
install_path\NetBackup\bin\bpup
```

Resolving no jobs displayed on Activity Monitor

If the EMM server is remote to the master server, the master server must be able to reach the PBX/EMM port 1556 and the Sybase database ODBC port 2638 on the EMM server. If a firewall prevents these connections, `bpjobd` cannot communicate with the EMM server and the Activity Monitor cannot display or update jobs.

To resolve port problems with remote EMM server

1. Verify that the `bpjobd` daemon is running.
2. Verify that EMMSERVER is configured to be a host other than the master.
3. Check the network connectivity between the master server and the EMMSERVER host.
4. Check to make sure that any firewall allows ports 1556 (PBX/EMM) and 2638 (Database ODBC) to be reachable on the EMMSERVER host.

Note: Intermittent network failure (maintenance, for example) should recover jobs data without intervention.

About troubleshooting Auto Image Replication

Auto Image Replication operations are characterized by storage lifecycle policies in at least two NetBackup master server domains. Verify that the two master servers follow these rules:

- The name of the storage lifecycle policy (SLP) in the source master server domain must match the SLP name in the target master server domain. The names are case-sensitive
- The name of the data classification used by the storage lifecycle policy in the source master server domain must match the name of the data classification in

the storage lifecycle policy in the target master server domain. The names are case-sensitive

- The duplicate-to-remote-master copy in the source storage lifecycle policy must use hierarchical duplication and specify a source copy with a residence capable of replication. (The disk pool replication column must show Source.)
- The storage lifecycle policy in the target domain must specify an import for its first copy. The residence for the import must include the device that is the replication partner of the source copy in the source storage lifecycle policy. The import copy may specify a storage unit group or a storage unit but not Any Available.
- The storage lifecycle policy in the target domain must have at least one copy that specifies the Remote Retention type.

Troubleshooting Auto Image Replication

Auto Image Replication replicates backups that are generated in one NetBackup domain to another media server in one or more NetBackup domains.

Note: Although Auto Image Replication supports replication across different master server domains, the Replication Director does not.

Auto Image Replication operates like any duplication job except that its job contains no write side. The job must run on a media server that runs NetBackup 7.1 or higher. It also must consume a read resource from the disk volume on which the duplicated images reside. If no media server is available with NetBackup 7.1 or higher, the job fails with status 800.

The Auto Image Replication job operates at a disk volume level. Within the storage unit that is specified in the storage lifecycle policy for the source copy, some disk volumes may not support replication and some media servers may not be running NetBackup 7.1 or higher. Use the **Disk Pools** interface of the **System Administration Console** to verify that the image is on a disk volume that supports replication. If the interface shows that the disk volume is not a replication source, click **Update Replication** to update the disk volumes in the disk pool. If the problem persists, check your disk device configuration.

The following procedure is based on NetBackup that operates in an OpenStorage configuration. This configuration communicates with a media server deduplication pool (MSDP) that uses Auto Image Replication.

To troubleshoot Auto Image Replication jobs

1 Display the storage server information by using the following command:

```
# bpstsinfo -lsuinfo -stype PureDisk -storage_server woodridge
LSU Info:
Server Name: PureDisk:woodridge.min.veritas.com
LSU Name: PureDiskVolume
Allocation : STS_LSU_AT_STATIC
Storage: STS_LSU_ST_NONE
Description: PureDisk storage unit (/woodridge.min.veritas.com#1/2)
Configuration:
Media: (STS_LSUF_DISK | STS_LSUF_ACTIVE | STS_LSUF_STORAGE_NOT_FREED
   | STS_LSUF_REP_ENABLED | STS_LSUF_REP_SOURCE)
Save As : (STS_SA_CLEARF | STS_SA_OPAQUEF | STS_SA_IMAGE)
Replication Sources: 0 ( )
Replication Targets: 1 ( PureDisk:bayside:PureDiskVolume )
...
```

This output shows the logical storage unit (LSU) flags STS_LSUF_REP_ENABLED and STS_LSUF_REP_SOURCE for PureDiskVolume. PureDiskVolume is enabled for Auto Image Replication and is a replication source.

2 To verify that NetBackup recognizes these two flags, run the following command:

```
# nbdevconfig -previewdv -stype PureDisk -storage_server woodridge
   -media_server woodridge -U
Disk Pool Name      :
Disk Type           : PureDisk
Disk Volume Name    : PureDiskVolume
...
Flag                : ReplicationSource
...
```

The ReplicationSource flag confirms that NetBackup recognizes the LSU flags.

3 To display the replication targets by using the raw output, run the following command:

```
# nbdevconfig -previewdv -stype PureDisk -storage_server woodridge
   -media_server woodridge
V7.0 DiskVolume < "PureDiskVolume" "PureDiskVolume" 46068048064
   46058373120 0 0 0 16 1 >
V7.0 ReplicationTarget < "bayside:PureDiskVolume" >
```

The display shows that the replication target is a storage server called bayside and the LSU (volume) name is PureDiskVolume.

4 To ensure that NetBackup captured this configuration correctly, run the following command:

```
# nbdevquery -listdv -stype PureDisk -U
Disk Pool Name      : PDpool
Disk Type           : PureDisk
Disk Volume Name    : PureDiskVolume
...
Flag                : AdminUp
Flag                : InternalUp
Flag                : ReplicationSource
Num Read Mounts     : 0
...
```

The listing shows that disk volume PureDiskVolume is configured in disk pool PDPool, and that NetBackup recognizes the replication capability.

5 If NetBackup does not recognize the replication capability, run the following command:

```
# nbdevconfig -updatedv -stype PureDisk -dp PDpool
```

6 To ensure that you have a storage unit that uses this disk pool, run the following command:

```
# bpstulist
PDstu 0 _STU_NO_DEV_HOST_ 0 -1 -1 1 0 "*NULL*"
   1 1 51200 *NULL* 2 6 0 0 0 0 PDpool *NULL*
```

The output shows that storage unit `PDstu` uses disk pool `PDpool`.

7 Check the settings on the disk pool by running the following command:

```
nbdevquery -listdp -stype PureDisk -dp PDpool -U
Disk Pool Name   : PDpool
Disk Pool Id     : PDpool
Disk Type        : PureDisk
Status           : UP
Flag             : Patchwork
...
Flag             : OptimizedImage
Raw Size (GB)    : 42.88
Usable Size (GB) : 42.88
Num Volumes      : 1
High Watermark   : 98
Low Watermark    : 80
Max IO Streams   : -1
Comment          :
Storage Server   : woodridge.min.veritas.com (UP)
```

Max IO Streams is set to -1, which means the disk pool has unlimited input-output streams.

8 To check the media servers, run the following command:

```
# tpconfig -dsh -all_host
============================================================
Media Server:                   woodridge.min.veritas.com
Storage Server:                 woodridge.min.veritas.com
User Id:                        root
    Storage Server Type:        BasicDisk
    Storage Server Type:        SnapVault
    Storage Server Type:        PureDisk
============================================================
```

This disk pool only has one media server, `woodridge`. You have completed the storage configuration validation.

9 The last phase of validation is the storage lifecycle policy configuration. To run Auto Image Replication, the source copy must be on storage unit `PDstu`. Run the following command:

```
nbstl woodridge2bayside -L
                                Name: woodridge2bayside
                 Data Classification: (none specified)
           Duplication job priority: 0
                               State: active
                             Version: 0
 Destination  1             Use for: backup
                             Storage: PDstu
                         Volume Pool: (none specified)
                        Server Group: (none specified)
                      Retention Type: Fixed
                     Retention Level: 1 (2 weeks)
                Alternate Read Server: (none specified)
                Preserve Multiplexing: false
     Enable Automatic Remote Import: true
                               State: active
                              Source: (client)
                      Destination ID: 0
 Destination  2             Use for: Auto Image Replication
                             Storage: Remote Master
                         Volume Pool: (none specified)
                        Server Group: (none specified)
                                 ...
                Preserve Multiplexing: false
     Enable Automatic Remote Import: false
                               State: active
                              Source: Destination 1 (backup:PDstu)
                      Destination ID: 0
```

To troubleshoot the Auto Image Replication job flow, use the same command lines as you use for other storage lifecycle policy managed jobs. For example, to list images that have been duplicated to remote master, run the following:

```
nbstlutil list -copy_type replica -U -copy_state 3
```

To list images that have not been duplicated to remote master (either pending or failed), run the following:

```
nbstlutil list -copy_type replica -U -copy_incomplete
```

10 To list the target storage devices that complete Auto Image Replication copies (replication destination), run the following command:

```
nbstlutil repllist
Image:
 Master Server            : woodridge.min.veritas.com
 Backup ID                : woodridge_1287610477
 Client                   : woodridge
 Backup Time              : 1287610477 (Wed Oct 20 16:34:37 2010)
 Policy                   : two-hop-with-dup
 Client Type              : 0
 Schedule Type            : 0
 Storage Lifecycle Policy : woodridge2bayside2pearl_withdup
 Storage Lifecycle State  : 3 (COMPLETE)
 Time In Process          : 1287610545 (Wed Oct 20 16:35:45 2010)
 Data Classification ID   : (none specified)
 Version Number           : 0
 OriginMasterServer       : (none specified)
 OriginMasterServerID     : 00000000-0000-0000-0000-000000000000
 Import From Replica Time : 0 (Wed Dec 31 18:00:00 1969)
 Required Expiration Date : 0 (Wed Dec 31 18:00:00 1969)
 Created Date Time        : 1287610496 (Wed Oct 20 16:34:56 2010)

 Copy:
   Master Server       : woodridge.min.veritas.com
   Backup ID           : woodridge_1287610477
   Copy Number         : 102
   Copy Type           : 3
   Expire Time         : 1290288877 (Sat Nov 20 15:34:37 2010)
   Expire LC Time      : 1290288877 (Sat Nov 20 15:34:37 2010)
   Try To Keep Time    : 1290288877 (Sat Nov 20 15:34:37 2010)
   Residence           : Remote Master
   Copy State          : 3 (COMPLETE)
   Job ID              : 25
   Retention Type      : 0 (FIXED)
   MPX State           : 0 (FALSE)
   Source              : 1
   Destination ID      :
   Last Retry Time     : 1287610614

 Replication Destination:
   Source Master Server: woodridge.min.veritas.com
   Backup ID           : woodridge_1287610477
```

```
Copy Number          : 102
Target Machine       : bayside
Target Info          : PureDiskVolume
Remote Master        : (none specified)
```

About troubleshooting automatic import jobs

The automatic import jobs that the storage lifecycle policy (SLP) components manage are different than legacy import jobs. Automatic import jobs asynchronously notify NetBackup that an image needs to be imported. Also, an Auto Image Replication job gives the catalog entries for this copy to the storage device so that the job does not have to read the entire image. Automatic import jobs simply read the catalog record off the storage device and add it into its own catalog. This process is so fast that NetBackup batches images for import for efficiency. A pending import is the state where NetBackup has been notified, but the import has not yet occurred.

More information is available about automatic import and how to tune the batch interval of the import manager process.

See the NetBackup Administrator's Guide, Volume I.

The notify event from the storage server provides the following: the image name, the storage server location to read the catalog for this image, and the name of the SLP that processes the image. Images for automatic import jobs are batched by storage lifecycle policy name and disk volume. The import job consumes an input-output stream on the disk volume.

To view images that are pending import, run the following command:

```
# nbstlutil pendimplist -U
Image:
 Master Server            : bayside.min.veritas.com
 Backup ID                : gdwinlin04_1280299412
 Client                   : gdwinlin04
 Backup Time              : 1280299412 (Wed Jul 28 01:43:32 2010)
 Policy                   : (none specified)
 Client Type              : 0
 Schedule Type            : 0
 Storage Lifecycle Policy : (none specified)
 Storage Lifecycle State  : 1 (NOT_STARTED)
 Time In Process          : 0 (Wed Dec 31 18:00:00 1969)
 Data Classification ID   : (none specified)
 Version Number           : 0
 OriginMasterServer       : master_tlk
 OriginMasterServerID     : 00000000-0000-0000-0000-000000000000
```

```
Import From Replica Time : 0 (Wed Dec 31 18:00:00 1969)
Required Expiration Date : 0 (Wed Dec 31 18:00:00 1969)
Created Date Time        : 1287678771 (Thu Oct 21 11:32:51 2010)

Copy:
  Master Server       : bayside.min.veritas.com
  Backup ID           : gdwinlin04_1280299412
  Copy Number         : 1
  Copy Type           : 4
  Expire Time         : 0 (Wed Dec 31 18:00:00 1969)
  Expire LC Time      : 0 (Wed Dec 31 18:00:00 1969)
  Try To Keep Time    : 0 (Wed Dec 31 18:00:00 1969)
  Residence           : (none specified)
  Copy State          : 1 (NOT_STARTED)
  Job ID              : 0
  Retention Type      : 0 (FIXED)
  MPX State           : 0 (FALSE)
  Source              : 0
  Destination ID      :
  Last Retry Time     : 0

  Fragment:
    Master Server     : bayside.min.veritas.com
    Backup ID         : gdwinlin04_1280299412
    Copy Number       : 1
    Fragment Number   : -2147482648
    Resume Count      : 0
    Media ID          : @aaaab
    Media Server      : bayside.min.veritas.com
    Storage Server    : bayside.min.veritas.com
    Media Type        : 0 (DISK)
    Media Sub-Type    : 0 (DEFAULT)
    Fragment State    : 1 (ACTIVE)
    Fragment Size     : 0
    Delete Header     : 1
    Fragment ID       : gdwinlin04_1280299412_C1_IM
```

The action taken on the automatic import job and the automatic import event depends on several conditions as shown in the following table.

Action	Condition
Automatic import jobs queue	No media server or I/O stream is available for this disk volume.

Action	Condition
Automatic import jobs never start (copy stays at storage lifecycle state 1)	■ The storage lifecycle policy is inactive. ■ The storage lifecycle policy import destination is inactive. ■ The storage lifecycle policy is between sessions. ■ The image has exceeded the extended retry count and the extended retry time has not passed.
Automatic import event is discarded and the image is ignored	■ The event specifies a backup ID that already exists in this master server catalog. ■ The event specifies a disk volume that is not configured in NetBackup for this storage server.
Automatic import job is started but the image is expired and deleted to clean up disk space in some cases. The event logs an error in the Problems Report or bperror output. An import job runs, but the import for this image fails showing a status code in the range 1532–1535.	■ The storage lifecycle policy that is specified in the event does not contain an import destination. ■ The storage lifecycle policy that is specified in the event has an import destination with a residence that does not include the disk volume specified by the event ■ The storage lifecycle policy that is specified does not exist. This is default behavior. More information is available for the storage lifecycle policy configuration options. See the NetBackup Administrator's Guide, Volume I.

Look at the Problems Report or the `bperror` list for these cases.

For troubleshooting job flow for automatic import jobs, use the same command lines as you would for other storage lifecycle policy managed jobs. To list images for which NetBackup has received notification from storage but not yet initiated import (either pending or failed), use the commands noted above or run the following command

```
# nbstlutil list -copy_type import -U -copy_incomplete
```

To list images that have been automatically imported, run the following command:

```
# nbstlutil list -copy_type import -U -copy_state 3 -U
Master Server             : bayside.min.veritas.com
 Backup ID                : woodridge_1287610477
 Client                   : woodridge
```

```
 Backup Time              : 1287610477 (Wed Oct 20 16:34:37 2010)
 Policy                   : two-hop-with-dup
 Client Type              : 0
 Schedule Type            : 0
 Storage Lifecycle Policy : woodridge2bayside2pearl_withdup
 Storage Lifecycle State  : 3 (COMPLETE)
 Time In Process          : 1287610714 (Wed Oct 20 16:38:34 2010)
 Data Classification ID   : (none specified)
 Version Number           : 0
 OriginMasterServer       : woodridge.min.veritas.com
 OriginMasterServerID     : f5cec09a-da74-11df-8000-f5b9412d8988
 Import From Replica Time : 1287610672 (Wed Oct 20 16:37:52 2010)
 Required Expiration Date : 1290288877 (Sat Nov 20 15:34:37 2010)
 Created Date Time        : 1287610652 (Wed Oct 20 16:37:32 2010)
```

The OriginMasterServer, OriginMasterServerID, Import From Replica Time, and Required Expiration Date are not known until after the image is imported so a pending record may look like this:

```
Image:
 Master Server            : bayside.min.veritas.com
 Backup ID                : gdwinlin04_1280299412
 Client                   : gdwinlin04
 Backup Time              : 1280299412 (Wed Jul 28 01:43:32 2010)
 Policy                   : (none specified)
 Client Type              : 0
 Schedule Type            : 0
 Storage Lifecycle Policy : (none specified)
 Storage Lifecycle State  : 1 (NOT_STARTED)
 Time In Process          : 0 (Wed Dec 31 18:00:00 1969)
 Data Classification ID   : (none specified)
 Version Number           : 0
 OriginMasterServer       : master_tlk
 OriginMasterServerID     : 00000000-0000-0000-0000-000000000000
 Import From Replica Time : 0 (Wed Dec 31 18:00:00 1969)
 Required Expiration Date : 0 (Wed Dec 31 18:00:00 1969)
 Created Date Time        : 1287680533 (Thu Oct 21 12:02:13 2010)
```

The OriginMasterServer here is not empty, although it may be in some cases. In cascading Auto Image Replication, the master server sends the notification.

Troubleshooting network interface card performance

If backup or restore jobs are running slowly, verify that the network interface cards (NIC) are set to full duplex. Half duplex often causes poor performance.

Note: If the NIC in a NetBackup master or media server is changed, or if the server IP address changes, CORBA communications may be interrupted. To address this situation, stop and restart NetBackup.

For help on how to view and reset duplex mode for a particular host or device, consult the manufacturer's documentation. If the documentation is not helpful, perform the following procedure.

To troubleshoot network interface card performance

1. Log onto the host that contains the network interface card whose duplex mode you want to check.
2. Enter the following command to view the current duplex setting.

   ```
   ifconfig -a
   ```

   On some operating systems, this command is `ipconfig`.

   The following is an example output from a NAS filer:

   ```
   e0: flags=1948043<UP,BROADCAST,RUNNING,MULTICAST,TCPCKSUM> mtu
   1500
   inet 10.80.90.91 netmask 0xfffff800 broadcast 10.80.95.255
   ether 00:a0:98:01:3c:61 (100tx-fd-up) flowcontrol full
   e9a: flags=108042<BROADCAST,RUNNING,MULTICAST,TCPCKSUM> mtu 1500
   ether 00:07:e9:3e:ca:b4 (auto-unknown-cfg_down) flowcontrol full
   e9b: flags=108042<BROADCAST,RUNNING,MULTICAST,TCPCKSUM> mtu 1500
   ether 00:07:e9:3e:ca:b5 (auto-unknown-cfg_down) flowcontrol full
   ```

   In this example, the network interface that shows "100tx-fd-up" is running in full duplex. Only interface `e0` (the first in the list) is at full duplex.

   A setting of "auto" is not recommended, because devices can auto-negotiate to half duplex.

3 The duplex mode can be reset by using the `ifconfig` (or `ipconfig`) command. For example:

```
ifconfig e0 mediatype 100tx-fd
```

4 For most hosts, you can set full-duplex mode permanently, such as in the host's /etc/rc files. Refer to the host's documentation for more information.

About SERVER entries in the bp.conf file

On Solaris and Linux systems, every SERVER entry in a client bp.conf file must be a NetBackup master or media server. That is, each system that is listed as a SERVER must have either NetBackup master or media server software installed. The client service on some clients cannot be started if the client name is incorrectly listed as a server.

If a bp.conf SERVER entry specifies a NetBackup client-only computer, SAN client backups or restores over Fibre Channel may fail to start. In this case, determine if the `nbftclnt` process is running on the client. If it is not running, check the `nbftclnt` unified logging file (OID 200) for errors. You may see the following in the `nbftclnt` log:

```
The license is expired or this is not a NBU server. Please check
your configuration. Note: unless NBU server, the host name can't be
listed as server in NBU configuration.
```

Remove or correct the SERVER entry in the `bp.conf` file, restart `nbftclnt` on the client, and retry the operation.

Note: The `nbftclnt` process on the client must be running before you start a SAN client backup or restore over Fibre Channel.

About unavailable storage unit problems

NetBackup jobs sometimes fail because storage units are unavailable, due to drives that are down or configuration errors, such as referencing an incorrect robot number. NetBackup processes log messages to the NetBackup error log that help you pinpoint and resolve these types of issues.

In addition, the Job Details dialog box available from the Activity Monitor contains messages that describe the following:

- The resources that the job requests

- The granted (allocated) resources.

If a job is queued awaiting resources, the Job Details dialog lists the resources for which the job waits. The three types of messages begin with the following headers:

```
requesting resource ...
awaiting resource ...
granted resource ...
```

Resolving a NetBackup Administration operations failure on Windows

When a user who is part of the Administrator's group tries to execute some NetBackup operations, the operation may fail with the following error, where *command* is a NetBackup administrator command:

```
command: terminating - cannot open debug file: Permission denied (13)
```

When the Security Setting of the **User Account Control: Run All Administrators in Admin Approval Mode** policy on Windows is Enabled, a user has limited permissions. The user from the Administrator's group is not allowed to manage NetBackup.

Disable this security setting through: Control Panel -> Administrative Tools -> Local Security Policy -> Local Policies -> Security Options -> User Account Control: Run All administrators in Admin Approval Mode -> Disable.

The following is the Local Security Policy panel:

Once the security setting is disabled, the user can successfully perform NetBackup operations.

About troubleshooting NetBackup in a SAN environment

NetBackup administrators may encounter any or all of the following common problems in a SAN (storage area network) environment:

- Intermittent backup failures
- Connectivity issues (drives that are down)
- SAN configuration changes

If the SAN administrator rezones the network or masks an array in use by NetBackup, some of the devices that NetBackup needs may be unavailable. Either action causes backups to fail and drives to go down. The only information available to the NetBackup administrator is an error 83 (media open error) or error 84 (media write error) status code.

You can use Veritas CommandCentral Storage to check elements of the SAN configuration. For example, you can check whether a particular device is connected as well as the zoning and masking on the SAN.

Sometimes a switch or a Windows box is interrupted and sends out a reset command. Since NetBackup doesn't automatically maintain persistent bindings, the reset command can cause drives to be mapped differently. CommandCentral Storage can help find the problem by showing the changes in the drive mappings, although it cannot automatically fix the problem.

For information on how to implement persistent bindings, see the NetBackup Device Configuration Guide.

NetBackup lets you launch CommandCentral Storage in context. The CommandCentral Storage Web GUI precisely displays the area of the SAN configuration you plan to troubleshoot.

NetBackup enterprise lifecycle best practices

SAN-related problems generally involve the use of Shared Storage Option (SSO). The two types of NetBackup users generally are as follows:

- Operators who have limited access to hosts and to the fabric of the SAN
- System administrators who have administrator privileges, but no access to the fabric

The SAN administrator generally operates outside the NetBackup domain entirely. Troubleshooting NetBackup is difficult when it involves the SAN because administrative responsibility tends to be spread out. No one person has a clear picture of the overall backup structure.

CommandCentral Storage provides a consistent view of the entire SAN against which to measure performance. It gives NetBackup administrators the data they need to request changes of and collaborate with the SAN administrators. It helps NetBackup administrators when they design, configure, implement, or modify solutions in response to changes in backup environments (hardware, applications, demand).

CommandCentral Storage can help those responsible for managing a backup system in a SAN environment by integrating SAN management and backup operation information.

CommandCentral Storage can provide support during the following backup lifecycle stages:

- Design

  Use CommandCentral Storage during the design phase to determine the following:

  - Where to deploy a backup system on the SAN
  - If SAN redesign is required to meet backup windows at minimum hardware cost and application impact

    For example, a backup design may not require the purchase of additional switches if it takes into account the following: the performance trending reports that CommandCentral Storage keeps to determine the pattern of fabric utilization.

    Or perhaps if you re-zone the fabric through CommandCentral Storage, it may provide sufficient bandwidth for meeting backup window requirements. In addition, CommandCentral Storage can provide visibility into recovery designs and fabric performance in the event of large restores that critical business operations require.

- Configuration, testing

  Generally, backup systems are tested before implementation to obtain benchmarks and adjust (tune) the system for maximum efficiency. CommandCentral Storage can provide the performance metrics for end-to-end I/O capabilities for all elements in the backup path. Additionally, CommandCentral Storage can provide valuable environmental information for qualifying the backup environment as well as a baseline for future troubleshooting configuration management.

- Implementation, reconfiguration, production

  CommandCentral Storage can help to determine whether a host can see through the entire I/O path to the target backup device by pinpointing connectivity issues.

Using CommandCentral Storage to troubleshoot NetBackup in a SAN environment

CommandCentral Storage provides centralized visibility and control across physical and virtual heterogeneous storage environments. It helps you optimize your data center by providing you a single view of the full storage stack from application to spindle. By enabling storage capacity management, centralized monitoring, and mapping, CommandCentral Storage software helps improve storage utilization, optimizes resources, increases data availability, and reduces capital and operational costs.

You can use CommandCentral Storage in the following ways to troubleshoot NetBackup in a SAN environment:

In-context launch	The ability to launch CommandCentral Storage and access an overview of the SAN from NetBackup in context is valuable for quickly identifying root problems. Also, because NetBackup and SAN administrators are often in different groups, you can avoid the fragmented operations that lead to resolution delays. With CommandCentral Storage, the NetBackup administrator has a view of the overall health of the SAN as part of the initial troubleshooting process.
Connectivity and device check	The CommandCentral Storage view of the SAN environment can help you detect any failure in the topology. An environment inventory provides valuable troubleshooting support for the support process.
General troubleshooting tools	To investigate a backup failure: ■ Launch CommandCentral Storage in context from NetBackup to check fabric health. ■ Check reports for fabric events that occur about the time NetBackup generated the error log.

The following use cases demonstrate how CommandCentral Storage can be integrated into a NetBackup troubleshooting procedure to investigate the SAN context of a backup system. Most common NetBackup problems on SANs are associated with connectivity issues.

Table 2-9 Troubleshooting NetBackup using CommandCentral Storage

Symptom	Troubleshooting
Cannot access drives or robots. Backup jobs fail.	This problem represents a loss of connectivity and typically generates status code 213 (no storage units available for use). NetBackup freezes tapes with two write failures even when SAN problems cause the failures. Do the following in the order listed: ■ In the **NetBackup Administration Console**, check the **Device Monitor** for a device that is down. If so, try to bring it back up. ■ If the drive is still down, check the syslog, device logs, and NetBackup logs for status 219 (the required storage unit is unavailable) and 213 (no storage units available for use) on the media server. Check the NetBackup logs for status codes 83, 84, 85, or 86. These codes relate to write, read, open, and position failures to access the drive. ■ Try a `robtest` to check connectivity. If no connectivity exists, the likely problem is with hardware. ■ From the master server, select the robot or device that the storage unit is associated with. ■ Launch CommandCentral Storage for a view of the media server and devices. Check the fabric connectivity (whether any I/O path devices are down).

Table 2-9 Troubleshooting NetBackup using CommandCentral Storage *(continued)*

Symptom	Troubleshooting
After you run the Device Configuration Wizard, the new device does not appear in the discovered devices list.	CommandCentral Storage topology is a good visual tool to check connectivity between the hosts and the devices. Use it to find a dislodged network cable or other hardware problems. You may not be able to discover a drive or robot when you configure off-host backups which require the media server to detect all devices involved in the backup: disk array, disk cache, data mover, library, and drive. Connectivity must be correct. In addition, the `bptpcinfo` command in the NetBackup Snapshot Client generates a `3pc.conf` configuration file for running the backup. The WWN (world wide name) for some devices is often incorrect. Use CommandCentral Storage to verify that the contents of the `3pc.conf` file correlate to the actual fabric configuration. For a description of an off-host backup, the `bptpcinfo` command, and the `3pc.conf` file, refer to the *NetBackup Snapshot Client Configuration* document. Do the following in the order listed: ■ Run the device discovery again. If you still do not detect the new device, the likely problem is with hardware. ■ Launch CommandCentral Storage. If the new device does not appear in the CommandCentral Storage topology, check the SAN hardware connections to determine if the device is connected. If the new device shows up as disconnected or offline, contact the SAN administrator and check switch configuration. Compare this troubleshooting procedure to a similar problem without the benefit of CommandCentral Storage, such as status code 214: robot number does not exist. ■ Rerun the Device Configuration Wizard.

Table 2-9 Troubleshooting NetBackup using CommandCentral Storage *(continued)*

Symptom	Troubleshooting
The backup job fails intermittently and the drive is down intermittently. No errors appear in the error log other than that the job failed.	Sometimes a problem with a switch or bridge either before or during the backup job causes the job to fail and take down the drive. This problem is very difficult to diagnose. By the time the NetBackup administrator checks the SAN, everything may be fine again. Another possibility is that another application reserved the device. A SCSI device monitoring utility is required to resolve this issue, which neither CommandCentral Storage nor NetBackup currently supplies. Do the following in the order listed: ■ Select a drive inside the NetBackup Device Monitor. Launch CommandCentral Storage in the drive context to see if the drive is connected to the SAN. ■ Check for alerts around the time of the job failure and see if a SAN problem could have caused the job to fail.

Chapter 3

Using NetBackup utilities

This chapter includes the following topics:

- About NetBackup troubleshooting utilities
- About the analysis utilities for NetBackup debug logs
- About network troubleshooting utilities
- About the NetBackup support utility (nbsu)
- About the NetBackup consistency check utility (NBCC)
- About the NetBackup consistency check repair (NBCCR) utility
- About the nbcplogs utility
- About the robotic test utilities

About NetBackup troubleshooting utilities

Several utilities are available to help diagnose NetBackup problems. The analysis utilities for NetBackup debug logs and the NetBackup support utility (`nbsu`) are especially useful in troubleshooting.

Table 3-1 Troubleshooting utilities

Utility	Description
Analysis utilities for NetBackup debug logs	They enhance NetBackup's existing debug capabilities by providing a consolidated view of a job debug log. See "About the analysis utilities for NetBackup debug logs" on page 100.

Table 3-1 Troubleshooting utilities *(continued)*

Utility	Description
Network troubleshooting utilities	They verify various aspects of the network configuration inside and outside NetBackup to ensure that there is no misconfiguration See "About network troubleshooting utilities" on page 104.
NetBackup support utility (`nbsu`)	It queries the host and gathers appropriate diagnostic information about NetBackup and the operating system. See "About the NetBackup support utility (nbsu)" on page 105.
NetBackup consistency check utility (`NBCC`)	It analyzes the integrity of portions of the NetBackup configuration and catalog and database information as they pertain to tape media. See "About the NetBackup consistency check utility (NBCC)" on page 111.
NetBackup consistency check repair (`NBCCR`) utility	It processes database-catalog repair actions and automates the application of approved suggested repair actions. See "About the NetBackup consistency check repair (NBCCR) utility" on page 120.
`nbcplogs` utility	It simplifies the process of gathering logs for deliver to Symantec technical support. See "About the nbcplogs utility" on page 122.

About the analysis utilities for NetBackup debug logs

The debug log analysis utilities enhance NetBackup's existing debug capabilities by providing a consolidated view of a job debug log.

NetBackup jobs span multiple processes that are distributed across servers.

You can get more information about legacy logging and unified logging.

See "About logs" on page 127.

To trace a NetBackup job you must view and correlate messages in multiple log files on multiple hosts. The log analysis utilities provide a consolidated view of the job debug logs. The utilities scan the logs for all processes that are traversed or

run for the job. The utilities can consolidate job information by client, job ID, start time for the job, and policy that is associated with the job.

Table 3-2 describes the log analysis utilities. To see the parameters, limitations, and examples of use for each utility, use the command with the `-help` option. All the commands require administrative privileges. The log analysis utilities are available for all platforms that are supported for NetBackup servers.

Note: The utilities must be initiated on supported platforms. However, the utilities can analyze debug log files from most NetBackup client and server platforms for UNIX and Windows.

Table 3-2 Analysis utilities for NetBackup debug logs

Utility	Description
`backupdbtrace`	Consolidates the debug log messages for specified NetBackup database backup jobs and writes them to standard output. It sorts the messages by time. `backupdbtrace` attempts to compensate for time zone changes and clock drift between remote servers and clients. At a minimum, you must enable debug logging for `admin` on the master server, and for `bptm` and `bpbkar` on the media server. For best results, set the verbose logging level to 5 and enable debug logging for the following: `bpdbm` on the master server and `bpcd` on all servers in addition to the processes already identified. A complete description of `backupdbtrace` is in the NetBackup Commands Reference Guide.
`backuptrace`	Copies to standard output the debug log lines relevant to the specified backup jobs, including online (hot) catalog backups. The `backuptrace` utility can be used for regular file system, database extension, and alternate backup method backup jobs. It consolidates the debug logs for specified NetBackup jobs. The utility writes the relevant debug log messages to standard output and sorts the messages by time. `backuptrace` attempts to compensate for time zone changes and clock drift between remote servers and clients. The format of the output makes it relatively easy to sort or `grep` by timestamp , program name, and server or client name. The `backuptrace` utility works with the `nbpem`, `nbjm`, and `nbrb` logs on the master server. You should enable debug logging for `bpbrm` and `bptm` or `bpdm` on the media server and for `bpbkar` on the client. For best results, set the verbose logging level to 5. Enable debug logging for the following: `bpdbm` and `bprd` on the master server and for `bpcd` on all servers and clients in addition to the processes already identified. A complete description of `backuptrace` is in the NetBackup Commands Reference Guide.

Table 3-2 Analysis utilities for NetBackup debug logs *(continued)*

Utility	Description
bpgetdebuglog	A helper program for backuptrace and restoretrace. It can also be useful as a standalone program and is available for all NetBackup server platforms. bpgetdebuglog prints to standard output the contents of a specified debug log file. If only the remote machine parameter is specified, bpgetdebuglog prints the following to standard output: the number of seconds of clock drift between the local computer and the remote computer. A complete description of bpgetdebuglog is in the NetBackup Commands Reference Guide.
duplicatetrace	Consolidates the debug logs for the specified NetBackup duplicate jobs and writes them to standard output. It sorts the messages by time. duplicatetrace attempts to compensate for time zone changes and clock drift between remote servers and clients. At a minimum, you must enable debug logging for admin on the master server and for bptm or bpdm on the media server. For best results, set the verbose logging level to 5 and enable debug logging for the following: bpdbm on the master server and bpcd on all servers and clients in addition to the processes already identified. A complete description of duplicatetrace is in the NetBackup Commands Reference Guide.
importtrace	Consolidates the debug log messages for the specified NetBackup import jobs and writes them to standard output. It sorts the messages by time. importtrace attempts to compensate for time zone changes and clock drift between remote servers and clients. At a minimum, you must enable debug logging for admin on the master server. And for bpbrm, you must enable debug logging for bptm and tar on the media server. For best results, set the verbose logging level to 5 and enable debug logging for the following: bpdbm on the master server and bpcd on all servers and clients in addition to the processes already identified. A complete description of importtrace is in the NetBackup Commands Reference Guide.

Table 3-2 Analysis utilities for NetBackup debug logs *(continued)*

Utility	Description
`restoretrace`	Copies to standard output the debug log lines relevant to the specified restore jobs. The `restoretrace` utility consolidates the debug logs for specified NetBackup restore jobs. The utility writes debug log messages relevant to the specified jobs to standard output and sorts the messages by time. `restoretrace` attempts to compensate for time zone changes and clock drift between remote servers and clients. The format of the output makes it relatively easy to sort or grep by timestamp, program name, and server or client name. At a minimum, you must enable debug logging for `bprd` on the master server. Enable debug logging for `bpbrm` and `bptm` or `bpdm` on the media server and `tar` on the client. For best results, set the verbose logging level to 5. Enable debug logging for `bpdbm` on the master server and for `bpcd` on all servers and clients. A complete description of `restoretrace` is in the NetBackup Commands Reference Guide.
`verifytrace`	Consolidates the debug log messages for the specified verify jobs and writes them to standard output. It sorts the messages by time. The `verifytrace` command attempts to compensate for time zone changes and clock drift between remote servers and clients. At a minimum, you must enable debug logging as follows: for `admin` on the master server and for `bpbrm`, `bptm` (or `bpdm`) and `tar` on the media server. For best results, set the verbose logging level to 5 and enable debug logging for the following: `bpdbm` on the master server and `bpcd` on all servers and clients in addition to the processes already identified. A complete description of `verifytrace` is in the NetBackup Commands Reference Guide.

The analysis utilities have the following limitations:

- Media and device management logs are not analyzed.
- The legacy debug log files must be in standard locations on the servers and clients.

  UNIX `/usr/openv/netbackup/logs/<PROGRAM_NAME>/log.mmddyy`

  Windows `install_path/NetBackup/Logs/<PROGRAM_NAME>/mmddyy.log`

  An option may be added later that allows the analyzed log files to reside on alternate paths.

Note: For the processes that use unified logging, no log directories must be created.

- The consolidated debug log may contain messages from unrelated processes. You can ignore messages with timestamps outside the duration of the job from the following: `bprd`, `nbpem`, `nbjm`, `nbrb`, `bpdbm`, `bpbrm`, `bptm`, `bpdm`, and `bpcd`.

An output line from the log analysis utilities uses the following format:

```
daystamp.millisecs.program.sequence machine log_line
```

daystamp	The date of the log that is in the format *yyyymmdd*.
millisecs	The number of milliseconds since midnight on the local computer.
program	The name of program (BPCD, BPRD, etc.) being logged.
sequence	Line number within the debug log file.
machine	The name of the NetBackup server or client.
log_line	The line that appears in the debug log file.

For more information, see the *NetBackup Commands Reference Guide*.

About network troubleshooting utilities

A set of utility programs (commands) verifies various aspects of the network configuration inside and outside NetBackup to ensure that there is no misconfiguration. The utilities also provide user-friendly messages for any errors they find.

Network configuration broadly falls into the following categories:

- Hardware, operating system, and NetBackup level settings.
  Examples include correct DNS lookups, firewall port openings, and network routes and connections. The NetBackup Domain Network Analyzer (`nbdna`) verifies this configuration.
- A set of utilities that verifies the NetBackup level settings.
  The utilities include `bptestcd` and `bptestnetconn`, and the settings they verify include CONNECT_OPTIONS and CORBA endpoint selection.

Table 3-3 Network troubleshooting utilities

Utility	Description
`bptestbpcd`	Tries to establish a connection from a NetBackup server to the `bpcd` daemon on another NetBackup system. If successful, it reports information about the sockets that are established. A complete description of `bptestbpcd` is in the NetBackup Commands Reference Guide.
`bptestnetconn`	Performs several tasks that aid in the analysis of DNS and connectivity problems with any specified list of hosts. This list includes the server list in the NetBackup configuration. To help troubleshoot connectivity problems between the services that use CORBA communications, `bptestnetconn` can perform and report on CORBA connections to named services. A complete description of `bptestnetconn` is in the NetBackup Commands Reference Guide.
`nbdna` (NetBackup Domain Network Analyzer)	Evaluates the host names in the NetBackup Domain. The `nbdna` utility self-discovers the NetBackup domain and evaluates host name information, then tests connectivity to these host names and validates their network relationship status. Network connectivity evaluation in a NetBackup domain is difficult. NetBackup domains can scale to hundreds of servers, and thousands of clients across complex network topologies. A complete description of `nbdna` is in the NetBackup Commands Reference Guide.

About the NetBackup support utility (nbsu)

The NetBackup support utility (`nbsu`) is a command line tool. It queries the host and gathers appropriate diagnostic information about NetBackup and the operating system. `nbsu` provides a wide range of control over the types of diagnostic information gathered. For instance, you can obtain information about NetBackup configuration settings, about specific troubleshooting areas, or about NetBackup or media management job status codes.

The NetBackup support utility (`nbsu`) resides in the following location:

UNIX `/usr/openv/netbackup/bin/support/nbsu`

Windows *`install_path`*`\NetBackup\bin\support\nbsu.exe`

Symantec recommends that you run the NetBackup support utility (nbsu) in the following circumstances:

- To obtain baseline data on your NetBackup installation. If you encounter problems later, this data can be useful.
- To document changes in your NetBackup or operating system environment. Run nbsu periodically to keep your baseline data up to date.
- To help isolate a NetBackup or operating system issue.
- To report issues to Symantec technical support.

The following suggestions can help you run the nbsu utility more effectively:

- For a complete description of nbsu including examples and how to gather diagnostic information to send to Symantec Technical Support, see the NetBackup Commands Reference Guide.
- For troubleshooting, run nbsu when the system is in the same state as when the problem occurred. For example, do not stop and restart the NetBackup processes after the error occurs or make a change to the server or network. If you do, nbsu may not be able to gather key information about the problem.
- If a NetBackup component is not operational (for example, bpgetconfig does not return information), nbsu may be unable to properly report on the system. For these cases, use the -nbu_down command line option to bypass the need for NetBackup to be operational.

If nbsu does not perform as expected, try the following:

- By default, nbsu sends error messages to standard error (STDERR) and also includes the messages in its output files under the header STDERR. Note the following alternate ways to view nbsu error messages:

To redirect the nbsu error messages to standard output (STDOUT)	Enter the following: ■ UNIX /usr/openv/netbackup/bin/support/nbsu 2>&1 ■ Windows *install_path*\NetBackup\bin\support\nbsu.exe 2>&1
To send all nbsu screen output including error messages to a file	Enter the following: nbsu 2>&1 > *file_name* Where 2>&1 directs standard error into standard output, and file_name directs standard output into the designated file.

- To generate the debug messages that relate to `nbsu`, enter the following:

  ```
  # nbsu -debug
  ```

  The messages are written to the `nbsu_info.txt` file.

The `nbsu_info.txt` file provides an overview of the environment where `nbsu` is run. It contains the following:

- General operating system and NetBackup information on the environment that `nbsu` detects
- A list of diagnostics that were run
- A list of diagnostics that returned a non-zero status

The information in `nbsu_info.txt` may indicate why `nbsu` returned particular values, or why it did not run certain commands.

If `nbsu` does not produce adequate information or if it seems to perform incorrectly, run `nbsu` with the `-debug` option. This option includes additional debug messages in the `nbsu_info.txt` file.

A complete description of `nbsu` is in the NetBackup Commands Reference Guide.

Output from the NetBackup support utility (nbsu)

The NetBackup support utility (`nbsu`) writes the information it gathers to text files in the following directory:

UNIX `/usr/openv/netbackup/bin/support/output/nbsu/`*`hostname_timestamp`*

Windows *`install_path`*`\NetBackup\bin\support\output\nbsu\`*`hostname_timestamp`*

The NetBackup environment where `nbsu` runs determines the particular files that `nbsu` creates. `nbsu` runs only those diagnostic commands that are appropriate to the operating system and the NetBackup version and configuration. For each diagnostic command that it runs, `nbsu` writes the command output to a separate file. As a rule, the name of each output file reflects the command that `nbsu` ran to obtain the output. For example, `nbsu` created the `NBU_bpplclients.txt` by running the NetBackup `bpplclients` command and created the `OS_set.txt` file by running the operating system's `set` command.

Each output file begins with a header that identifies the commands that `nbsu` ran. If output from more than one command was included in the file, the header identifies the output as an “internal procedure.”

Figure 3-1 shows the actual commands and output follow the header.

Figure 3-1 Example nbsu output file: ipconfig command (excerpt)

```
-------------------- Network ipconfig information report --------------
----------------------------- Command used ----------------------------
> "C:\WINDOWS\system32\ipconfig" /all

Windows IP Configuration

    Host Name . . . . . . . . . . . . : host1
    Primary Dns Suffix  . . . . . . . :
    Node Type . . . . . . . . . . . . : Hybrid
    IP Routing Enabled. . . . . . . . : No
    WINS Proxy Enabled. . . . . . . . : No
    DNS Suffix Search List. . . . . . : company.com
```

Figure 3-2 shows an example of part of the `nbsu` output file for the `bpgetconfig` command.

Figure 3-2 Example nbsu output file: bpgetconfig command (excerpt)

```
------------------ NetBackup bpgetconfig information report ----------------
------------- nbsu diagnostic name and internal procedure used -------------
NBU_bpgetconfig - NBU_get_bpgetconfig_info
------------------------------ Command Used ------------------------------
> "C:\Program Files\VERITAS\netbackup\bin\admincmd\bpgetconfig" -g host1 -L
Client/Master = Master
NetBackup Client Platform = PC, Windows2000
NetBackup Client Protocol Level = 6.5.0
Product = NetBackup
Version Name = 6.5Alpha
Version Number = 650000
NetBackup Installation Path = C:\Program Files\VERITAS\NetBackup\bin
Client OS/Release = Windows2003 5
------------------------------ Command Used ------------------------------
> "C:\Program Files\VERITAS\netbackup\bin\admincmd\bpgetconfig"
SERVER = host1
SERVER = host2
SERVER = host3
SERVER = host4
SERVER = host5
SERVER = host6
SERVER = host7
```

If the executed command returned a non-zero status, an `EXIT STATUS` header indicates the status. For example:

```
---------------------- EXIT STATUS = 227 ------------------------
```

As part of the internal processing of each command that a diagnostic command runs, `nbsu` redirects each command's `STDERR` to an internal file. If the command writes information to `STDERR`, `nbsu` captures this information and includes a `STDERR` header along with the information. For example:

```
---------------------------- STDERR -----------------------------
bpclient: no entity was found (227)
```

If a supported archive program is available on the host where `nbsu` runs, `nbsu` bundles its output files into an archive file. If a supported compression utility is available, `nbsu` compresses the archive file. Otherwise, the individual output files remain unarchived and uncompressed.

An example of a compressed archive file that `nbsu` created is as follows:

`/usr/openv/netbackup/bin/support/output/nbsu/`*`host1_master_20060814_164443/host1_master_20060814_164443.tar.gz`*

where *host1* is the name of the host on which `nbsu` ran. *master* indicates that the host is a NetBackup master server.

`nbsu` supports tar for archive and gzip for compression. Symantec may add support for other archive and compression utilities in the future. For an up-to-date list of supported archive and compression utilities, run the `nbsu -H` command on your installed version of NetBackup.

Note: Archiving and compression utilities are usually available on UNIX and Linux systems. On Windows, it may be necessary to install these programs. Note that the archiving utility must be referenced in the system `PATH` environment variable.

If no archive utility is installed on your system, use the `-xml` option of the `nbsu` command. This option lets you create a single `.xml` file in place of the individual output files. The single `.xml` file contains all the diagnostic information that the individual files contain. Use this command to conveniently bundle `nbsu` output for Symantec technical support.

A complete description of `nbsu` is in the NetBackup Commands Reference Guide.

Status code information gathered by the NetBackup support utility (nbsu)

You can use `nbsu` to gather diagnostic information about certain NetBackup or Media Manager status codes. `nbsu` gathers this information by running one or more NetBackup commands whose output may indicate the cause of the problem.

See the Status Codes Reference Guide for more about the topics that describe the status codes.

A complete description of `nbsu` is in the NetBackup Commands Reference Guide.

The following are examples of the results you can get when you enter specific commands:

To gather diagnostic information about status code 25	Enter `nbsu -nbu_e 25`. This command runs only the diagnostic commands that are related to NetBackup status code 25. Since fewer commands are run, the result may be a smaller set of output files.
To determine what information `nbsu` can collect for a particular status code	Enter `nbsu -l -nbu_e 25`.

More information is available about the output files that `nbsu` generates.

See "Output from the NetBackup support utility (nbsu)" on page 107.

Note: You can also use a NetBackup exit script to call `nbsu`. The script passes the NetBackup status code to `nbsu` to gather associated diagnostics for a job.

A complete description of `nbsu` is in the NetBackup Commands Reference Guide.

Example of a progress display for the NetBackup support utility (nbsu)

By default, the NetBackup support utility (`nbsu`) displays its progress to standard output. First, it lists environment queries, and then it lists the diagnostic commands that it runs as in the following example:

```
C:\Program Files\VERITAS\NetBackup\bin\support>nbsu
1.0 Determining initial nbsu settings
1.1 Determining OS environment
1.2 Determining OS host services
1.3 Determining identified network interface hostnames
1.4 Determining NetBackup environment
```

```
2.0 Querying nbsu diagnostic lists
2.1 Determining nbsu diagnostics to run
3.0 Executing nbsu diagnostics
    Executing diagnostic DEV_scsi_reg
    Registry query of HKEY_LOCAL_MACHINE\hardware\DeviceMap\Scsi\

    Executing diagnostic MM_ndmp
        "C:\Program Files\VERITAS\volmgr\bin\set_ndmp_attr" -list
        "C:\Program Files\VERITAS\volmgr\bin\set_ndmp_attr" -probe
        <hostname>
        "C:\Program Files\VERITAS\volmgr\bin\set_ndmp_attr" -verify
        <hostname>

    Executing diagnostic MM_tpconfig
        "C:\Program Files\VERITAS\\Volmgr\Bin\tpconfig" -d

4.0 nbsu successfully completed the identified diagnostic commands.
    Creating support package...
Microsoft (R) Cabinet Maker - Version 5.2.3790.0
Copyright (c) Microsoft Corporation. All rights reserved..

770,201 bytes in 36 files
Total files:             36
Bytes before:       770,201
Bytes after:        105,503
After/Before:             13.70% compression
Time:                      0.67 seconds ( 0 hr 0 min 0.67 sec)
Throughput:             1119.27 Kb/second
         Cleaning up output files...

       The results are located in the
.\output\nbsu\lou4_master_20070409_160403 directory...
```

A complete description of `nbsu` is in the NetBackup Commands Reference Guide.

About the NetBackup consistency check utility (NBCC)

The NetBackup consistency check utility (`NBCC`) is a command line utility. It is used to analyze the integrity of portions of the NetBackup configuration, catalog, and database information. This analysis includes review of NetBackup storage units, the EMM server, volume pools, tape media, and backup images that are associated with tape media.

NBCC does the following:

- Queries the EMM database to obtain the primary host name, associated host names, and server attributes for host name normalization
- Through examination of the NetBackup configuration, identifies cluster, application cluster and servers
- Gathers the database and catalog information
- Analyzes the consistency of the gathered configuration and database and catalog information
- Creates a packaged bundle for Symantec technical support to review

NBCC resides in the following location:

UNIX	`/usr/openv/netbackup/bin/support/NBCC`
Windows	*`install_path`*`\NetBackup\bin\support\NBCC.exe`

Symantec recommends that you run NBCC in the following circumstances:

- To check the consistency of the NetBackup configuration and catalog and database information from a tape media perspective
- To gather and create a package bundle when directed to do so by Symantec technical support

The following items can help you run the NBCC utility:

- For an NBCC description, examples, and how to gather NetBackup catalog and database information to send to Symantec technical support , refer to the NBCC `-help` command.
- NBCC is designed to be run on NetBackup master servers.
- In some cases, a non-functioning operating system or NetBackup process or service can prevent NBCC from running properly or completing. As NBCC progresses through the interrogation of various operating system or NetBackup components, it outputs what processes to STDOUT. As NBCC processes catalog and database components, it displays how many records have been processed. The number of records that are processed is in direct relationship to the size of the catalog and database being processed. If NBCC detects a failure, related information is output to STDERR. Information to STDOUT or STDERR are also output to the `nbcc-info.txt` file (if available).

If NBCC does not perform as expected, try the following:

- Use a text editor to look for error notices in the `nbcc-into.txt` file.

- By default, NBCC sends error messages to standard error (STDERR) and also includes the messages in its output files under the header STDERR.
- If NBCC does not produce adequate information or if it seems to perform incorrectly, run NBCC with the -debug option to include additional debug messages in the nbcc-info.txt file.
- For troubleshooting, run NBCC when the system is in the same state as when the problem occurred. For example, do not stop and restart the NetBackup processes after the error occurs or make a change to the server or network. NBCC may not be able to gather key information about the problem.

The nbcc-info.txt file provides an overview of the environment where NBCC is run, and contains the following:

- General operating system and NetBackup configuration information on the environment that NBCC detects
- A copy of the NBCC processing information that is sent to STDOUT or STDERR.

This information indicates the processing that NBCC has done.

The nbcc-info.txt report contains a section of information that summarizes the NBCC processing for each system detected in the NetBackup configuration. This section is listed by the server types in EMM that NBCC detects. It begins with "Summary of NBCC <type> processing".

See "Example of an NBCC progress display" on page 114.

A complete description of NBCC is in the NetBackup Commands Reference Guide.

Output from the NetBackup consistency check utility (NBCC)

NBCC writes the information it gathers to packaged files in the following directory.

UNIX and Linux	/usr/openv/netbackup/bin/support/output /nbcc/*hostname_NBCC_timestamp*
Windows	*install_path*\NetBackup\bin\support\output \nbcc*hostname_NBCC_timestamp*

If a supported archive program is available on the host where NBCC runs, NBCC bundles its output files into an archive file. If a supported compression utility is available, NBCC compresses the archive file. Otherwise, the individual output files remain unarchived and uncompressed.

An example of a compressed (UNIX) archive file that NBCC created is as follows:

/usr/openv/netbackup/bin/support/output/NBCC/*host1_NBCC_20060814_164443/host1_NBCC_20060814_164443.tar.gz*

where *host1* is the name of the host where NBCC had been run.

On UNIX platforms, NBCC supports the tar, compress, and gzip utilities for UNIX file archiving and compression. On Windows platforms, NBCC supports the tar, Makecab, and gzip utilities for Windows file archiving and compression.

A complete description of NBCC is in the NetBackup Commands Reference Guide.

Example of an NBCC progress display

By default, NetBackup consistency check utility (NBCC) displays its progress numerically to standard output. The name of the output file is nbcc-info.txt.

The following example of NBCC output has been edited for brevity:

```
1.0  Gathering initial NBCC information
1.1  Obtaining initial NetBackup configuration information

      NBCC is being run on NetBackup master server
       server1
NBCC version 7.6 Gather mode = full
NBCC command line = C:\Veritas\NetBackup\bin\support\NBCC.exe -nozip \
-nocleanup
OS name  = MSWin32
OS version = Microsoft Windows [Version 6.1.7601]
NetBackup Install path = C:\Program Files\Veritas\
> dir output\nbcc\server1_NBCC_20130227_091747 2>&1
Parsed output for "bytes free"

               5 Dir(s)  862,367,666,176 bytes free

2.0  Gathering required NetBackup configuration information
2.1  Determining the date format to use with NetBackup commands...
       Using the date format /mm/dd/yyyy
2.2  Building EMM host configuration information...
     Detected the EMM Server hostname
         lidabl11
       Detected the EMM master server hostname
         lidabl11
       Detected the EMM Virtual Machine entry
         pambl11vm3
       Detected the EMM NDMP Host entry
```

```
        fas3240a
    ...
2.3 Obtaining EMM server aliases...
    EMM aliases for detected EMM Server
        server1
          lidabl11.rmnus.sen.symantec.com
      EMM aliases for detected master server
        server1
          lidabl11.rmnus.sen.symantec.com
      EMM aliases for detected media server
        server4
    ...
2.4 Obtaining Storage Server information...
      Detected FalconStor OST direct copy to tape Storage Server
            falconstorvtl5
2.5 Building NetBackup storage unit list...
    Detected Storage Unit for NetBackup for NDMP media server
        reabl3
      and NDMP Host
        falconstorvtl5
      Detected disk media storage unit host
        lidabl11
      Detected Disk Pool
        lidabl11_pdde_pool
    ...
2.6 Obtaining Disk Pool information...
      Detected Disk Pool
        lidabl11_pdde_pool
          host
            lidabl11
          Detected Disk Pool lidabl11_pdde_pool member
            lidabl11
    ...
2.7 Obtaining tpconfig Storage credential information...
      Detected the master server hostname
        lidabl11
      and associated Storage server hostname
        lidabl11
    ...
2.8 Obtaining tpconfig NDMP configuration information...
      Detected the EMM NDMP Host hostname
        fas3240a
      Detected the EMM NDMP Host hostname
```

```
        fas3240b
    ...
2.9  Analyzing EMM master and/or media servers and configured
    Storage Units...
      The following EMM server entries do not have configured
      Storage Units or Disk Pools:

      Media server - lidabl14

2.10 Obtaining NetBackup unrestricted media sharing status...
      Configuration state = NO
2.11 Obtaining NetBackup Media Server Groups...
      No Server Groups configured
2.12 Building NetBackup retention level list...
3.0  Obtaining NetBackup version from media servers
      lidabl11...
      lidabl14...
      reabl3...
      virtualization5400a...
      ...
3.1  Gathering required NetBackup catalog information
      Start time = 2013-02-27 09:41:07
3.2  Gathering NetBackup EMM conflict table list
      Found 0 EMM conflict records
3.3 Gathering list of all tapes associated with any Active Jobs
      Building NetBackup bpdbjobs list
3.4 Gathering all TryLog file names from the
    C:\Program Files\netbackup\db\jobs\trylogs
    directory
      Found 10 TryLogs for 10 active jobs.
      TryLogs found for all Active Jobs
3.5  Building NetBackup Image database contents list
      Reading Image number 1000
      Reading Image number 2000
      Reading Image number 3000
      Reading Image number 4000
      Found 4014 images in the Image database
3.6  Building EMM database Media and Device configuration
    attribute lists
      Obtaining the EMM database Media attribute list for disk
      virtual server
        lidabl11 ...
        There were 0 bpmedialist records detected for media server
```

```
         lidabl11
           Getting device configuration data from server
         lidabl11 ...
     ...
3.7  Building EMM database Unrestricted Sharing Media attribute lists
         Found 0 Unrestricted Sharing media records in the EMM database
3.8  Building the EMM database Volume attribute list...
       Getting the EMM database Volume attributes from EMM server
         mlbnbu ...
       Found 43 Volume attribute records in the EMM database
3.9  Building NetBackup volume pool configuration list
       EMM Server lidabl11
3.10 Building NetBackup scratch pool configuration list
       EMM Server lidabl11
3.11 Gathering NetBackup EMM merge table list
       Found 0 EMM merge table records

     Summary of gathered NetBackup catalog information
       End time = 2013-02-27 09:44:16
       Number of Images gathered = 4014
       Number of database corrupt images gathered = 0
       Number of EMM database Media attribute records gathered = 38
       Number of EMM database Volume attribute records gathered = 43

       Catalog data gathering took 189 seconds to complete

     dir results for created NBCC files:
02/27/2013  09:42 AM                 8 nbcc-active-tapes

02/27/2013  09:42 AM           752,698 nbcc-bpdbjobs-most_columns

07/07/2011  09:43 AM         2,211,811 nbcc-bpimagelist-l
...

4.0  Verifying required catalog components were gathered

5.0  Beginning NetBackup catalog consistency check
     Start time = 2013-02-27 09:44:18
5.1  There were no tape media involved in active NetBackup jobs
5.3  Processing EMM database Volume attribute records, pass 1 (of 2),
     4 records to be processed
       Processed 4 EMM database Volume attribute records.
5.4  Checking for duplicate EMM server host names in Volume
```

```
     attribute data
5.5  Processing Image DB, pass 1 (of 2),
     3751 images to be processed
       3751 images processed on pass 1
       There were 0 images with at least one copy on hold detected.
5.6  Processing EMM database Media attribute records, pass 1 (of 3),
     2 records to be processed
       Processed 2 EMM database Media attribute records.
       There were 0 tape media detected that are on hold.
5.8  Check for duplicate media server names in the EMM database
       Media attribute data
5.9  Processing EMM database Media attribute records, pass 2 (of 3),
      2 records to be processed
5.10  Processing Image DB, pass 2 (of 2),
     3751 images to be processed
CONSISTENCY_ERROR Oper_7_1

5.11  NetBackup catalog consistency check completed
       End time = 2013-02-27 09:19:25

5.12  Checking for the latest NBCCR repair output directory
       C:\Program Files\Veritas\netbackup\bin\support\output\nbccr
       No repair file output directory detected.

       Summary of NBCC EMM Server processing
       Summary of NBCC EMM Server processing
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+ Primary hostname:                                                   +
+ lidabl11                                                           +
+ Alias hostnames:                                                   +
+ lidabl11                                                           +
+ Sources:                                                           +
+ nbemmcmd vmoprcmd                                                  +
+ EMM Server = yes                                                   +
+ EMM NetBackup version = 7.6                                        +
+ NBCC NetBackup version = 7.6                                       +
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

       Summary of NBCC Master server processing
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+ Primary hostname:                                                   +
+ lidabl11                                                           +
+ Alias hostnames:                                                   +
```

```
+ lidabl11                                                                +
+ Sources:                                                                +
+ nbemmcmd bpstulist nbdevquery bpgetconfig                               +
+ Master server = yes                                                     +
+ EMM NetBackup version = 7.6.0.0                                         +
+ NBCC NetBackup version = 7.6                                            +
+ Tape STU detected = no - Disk STU detected = yes                        +
+ Disk Pool Host = yes                                                    +
+ Associated Storage servers:                                             +
+ lidabl11 lidaclvm1                                                      +
+ EMM tape media record extract attempted = yes                           +
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

       Summary of NBCC Media server processing
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+ Primary hostname:                                                       +
+ lidabl14                                                                +
+ Alias hostnames:                                                        +
+ lidabl14.rmnus.sen.symantec.com                                         +
+ Sources:                                                                +
+ nbemmcmd bpgetconfig                                                    +
+ Media server = yes                                                      +
+ EMM NetBackup version = 7.6.0.0                                         +
+ NBCC NetBackup version = 7.6                                            +
+ Tape STU detected = no - Disk STU detected = no                          +
+ EMM tape media record extract attempted = yes                           +
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

...

     ***NBCC DETECTED A NetBackup CATALOG INCONSISTENCY!***

Report complete, closing the
.\output\nbcc\lidabl11_NBCC_20130227_094057\nbcc-info.txt
output file.
```

A complete description of `NBCC` options is in the NetBackup Commands Reference Guide.

About the NetBackup consistency check repair (NBCCR) utility

The NetBackup consistency check repair (NBCCR) utility is a command line tool that processes database-catalog repair actions. It automates the application of approved suggested repair actions. Symantec technical support analyzes the data that is collected by the NBCC utility and site-specific configuration information. This analysis results in the generation of a suggested repair actions (SRA) file. Before NBCCR is run, Symantec technical support interacts with the customer to determine which repairs are needed. Undesirable repair actions are deleted or commented out of the SRA file. Each line of the SRA file contains one repair action that is paired with an associated parameter.

The NBCCR utility executes each repair action in several stages.

Table 3-4 Stages of repair

Stage	Name	Description
Stage 1	Data collection	NBCCR first collects the information that is required to perform a repair.
Stage 2	Repair qualification	Immediately before the suggested repair is applied, NBCCR verifies that the current status of the tape still qualifies for the requested repair. It recognizes that time has passed and the environment may have changed since the data was collected. If so, it reports in a history file that the repair is not qualified.
Stage 3	Repair	Finally, NBCCR performs up to three steps of repair for every repair entry in the SRA file. An element may be modified to enable the repair and steps may be necessary after the repair. If the repair fails during the repair operation, NBCCR tries to roll back the repair so that the corrective action does not introduce any new errors.

NBCCR resides in the following location:

UNIX `/usr/openv/netbackup/bin/support/NBCCR`

Windows *`install_path`*`\NetBackup\bin\support\NBCCR.exe`

NBCCR accepts one input file, creates two output files, and uses one temporary file.

Input file	NBCCR accepts as input the Suggested Repair Action (SRA) file named *mastername*_NBCCA_*timestamp*txt. Technical Support analyzes the NBCC support package and generates this file which is sent to the end user. This file is placed in the following directory for NBCCR processing: On Unix: /usr/openv/netbackup/bin/support/input/nbccr/SRA On Windows: *install_path*\NetBackup\bin\support\input\nbccr\SRA
Output files	NBCCR automatically creates a separate directory for each SRA file processed. The file name is based on the contents of the SRA file. The name of the directory is as follows: On UNIX: /usr/openv/netbackup/bin/support/output/nbccr/*mastername*_nbccr_*timestamp* On Windows: *install_path*\NetBackup\bin\support\output\nbccr*mastername*_nbccr_*timestamp*. After repair processing is complete, NBCCR relocates the SRA file to the same directory. NBCCR also creates the following output files and places them in the same directory. ■ NBCCR creates NBCCR.History.txt, which is a history file of all the repair actions attempted. ■ NBCCR creates NBCCR.output.txt.
Temporary file	While it runs, the NBCCR utility uses KeepOnTruckin.txt, which appears in the same location as the output files described above To terminate NBCCR while it processes repairs, delete this file. This action causes NBCCR to complete the current repair, then shut down. Any other interruption causes undetermined results.

The following sample NBCCR.output.txt files show the results of two MContents repairs. One where all images were found on tape and one where one or more images were not found on the tape:

- Example 1: NBCCR found all images on the tape. The MContents repair action is successful.

```
MContents for ULT001 MediaServerExpireImagesNotOnTapeFlag
  ExpireImagesNotOnTape flag not set
  ULT001 MContents - All images in images catalog found on tape
  MContents ULT001 status: Success
```

- Example 2: NBCCR did not find one or more images on the tape. The MContents repair action was not performed.

```
MContents for ULT000 MediaServerExpireImagesNotOnTapeFlag
ExpireImagesNotOnTape flag not set
  Did NOT find Backup ID winmaster_123436 Copy 1 AssignTime
    2011-02-11 01:19:13 (123436) on ULT000
  Leaving winmaster_123436 Copy 1 on ULT000 in ImageDB
ULT000 MContents - One or more images from images catalog NOT
  found on tape
MContents ULT000 status: ActionFailed
```

A complete description of NBCCR is in the NetBackup Commands Reference Guide.

About the nbcplogs utility

When you troubleshoot a customer problem, you must gather and copy the correct logs to debug the issue. The log types (NBU, vxul, vm, pbx,...) may be in many places. The process of getting the logs to Symantec technical support can be difficult and time consuming.

By default, nbcplogs (NetBackup log uploader) now runs the nbsu utility and uploads nbsu information for the host system. This capability improves the end-user experience with Technical Support by saving time and keystrokes to gather and upload information. The utility also gathers additional log information for clusters and pack history information.

nbcplogs uses file transfer protocol (FTP) to upload its support package to Technical Support. This process requires temporary disk space to build the compressed bundle that it transfers. You can configure this temporary space by setting up an environment variable (TMPDIR) and using a nbcplogs command line option (--tmpdir) as follows:

On Windows:

```
# nbcplogs --tmpdir=C:\temp -f ###-###-###
```

On UNIX:

In /bin/sh, enter the following:

```
# TMPDIR=/tmp
# export TMPDIR
# nbcplogs -f ###-###-###
```

In /bin/bash, enter the following:

```
# export TMPDIR=/tmp
# nbcplogs -f ###-###-###
```

In `/bin/csh` or `/bin/tcsh`, enter the following:

```
# nbcplogs --tmpdir=/tmp -f ###-###-###
```

This utility supports three types of search algorithms. These are command options that are part of the `nbcplogs` command line.

- `--filecopy`. File copy is the default condition. It copies the entire log file. File copy with compression is usually enough to get the job done.
- `--fast`. Fast search uses a binary search to strip out lines that are outside the time frame of the file. This mechanism is useful when copying extremely large log files such as `bpdbm`. This option is rarely needed and should be used with caution.

The default condition is the file copy, which copies the entire log file. A fast search algorithm uses a binary search to strip out lines that are outside the time frame of the file. This mechanism is useful when copying extremely large log files such as `bpdbm`.

The `nbcplogs` utility is intended to simplify the process of copying logs by specifying the following options:

- A time frame for the logs.
- The log types that you want to collect.
- Bundling and in-transit data compression.

In addition, you can preview the amount of log data to be copied.

A complete description of `nbcplogs` is in the NetBackup Commands Reference Guide.

About the robotic test utilities

Each of the robotic software packages includes a robotic test utility for communicating directly with robotic peripherals. The tests are for diagnostic purposes and the only documentation is the online Help that you can view by entering a question mark (?) after starting the utility. Specify `-h` to display the usage message.

Note: Do not use the robotic test utilities when backups or restores are active. The tests lock the robotic control path and prevent the corresponding robotic software from performing actions, such as loading and unloading media. If a mount is requested, the corresponding robotic process times out and goes to the DOWN state. This usually results in a media mount timeout. Also, be certain to quit the utility when your testing is complete.

Robotic tests on UNIX

If the robot has been configured (that is, added to the EMM database), start the robotic test utility by using the `robtest` command. This action saves time, since robotic and drive device paths are passed to the test utility automatically. The procedure is as follows:

To use the `robtest` command, do the following (in the order presented):

- Execute the following command:

  `/usr/openv/volmgr/bin/robtest`

  The test utility menu appears.

- Select a robot and press **Enter**.
  The test starts.

If the robot is not configured, you cannot use `robtest` and must execute the command that applies to the robot you test.

ACS	`/usr/openv/volmgr/bin/acstest -r` *`ACSLS_hostpath`* for `acstest` to work on UNIX and Linux, `acssel` and `acsssi` must be running
ODL	`/usr/openv/volmgr/bin/odltest -r` *`roboticpath`*
TL4	`/usr/openv/volmgr/bin/tl4test -r` *`roboticpath`*
TL8	`/usr/openv/volmgr/bin/tl8test -r` *`roboticpath`*
TLD	`/usr/openv/volmgr/bin/tldtest -r` *`roboticpath`*
TLH	`/usr/openv/volmgr/bin/tlhtest -r` *`robotic_library_path`*
TLM	`/usr/openv/volmgr/bin/tlmtest -r` *`DAS_host`*
TSH	`/usr/openv/volmgr/bin/tshtest -r` *`roboticpath`*

More information on ACS, TLH, and TLM robotic control is available.

See the NetBackup Device Configuration Guide.

In the previous list of commands, *roboticpath* is the full path to the device file for the robotic control (SCSI). You can review the section for your platform to find the appropriate value for *roboticpath*.

An optional parameter specifies the device file path for the drives so that this utility can unload the drives using the SCSI interface.

Robotic tests on Windows

If the robot has been configured (that is, added to the EMM database), start the robotic test utility by using the `robtest` command. This action saves time, since robotic and drive device paths are passed to the test utility automatically.

To use the `robtest` command, do the following (in the order presented):

- Execute the following command:

  install_path\Volmgr\bin\robtest.exe

  The test utility menu appears.
- Select a robot and press Enter.
  The test starts.

Note: If the robot is not configured, you cannot use `robtest` and must execute the command that applies to the robot you are testing (see following list).

ACS	*install_path*\Volmgr\bin\acstest -r *ACSLS_HOST*
TL4	*install_path*\Volmgr\bin\tl4test -r *roboticpath*
TL8	*install_path*\Volmgr\bin\tl8test -r *roboticpath*
TLD	*install_path*\Volmgr\bin\tldtest -r *roboticpath*
TLH	*install_path*\Volmgr\bin\tlhtest -r *robotic_library_name*
TLM	*install_path*\Volmgr\bin\tlmtest -r *DAS_Hostname*

More information on ACS, TLH, and TLM robotic control is available.

See the NetBackup Device Configuration Guide.

In the previous list of commands, *roboticpath* is the full path to the device file for the robotic control (SCSI). You can review the section for your platform to find the appropriate value for *roboticpath*.

An optional parameter specifies the device file path for the drives so that this utility can unload the drives using the SCSI interface.

Usage is:

```
install_path <-p port -b bus -t target -l lan | -r
roboticpath>
```

where: *roboticpath* is the changer name (e.g., Changer0).

Chapter 4

Using logs

This chapter includes the following topics:

- About logs
- About UNIX system logs
- About unified logging
- About legacy logging
- About global logging levels
- Logs to accompany problem reports for synthetic backups
- Setting retention limits for logs on clients
- Logging options with the Windows Event Viewer
- Troubleshooting error messages in the NetBackup Administration Console for UNIX

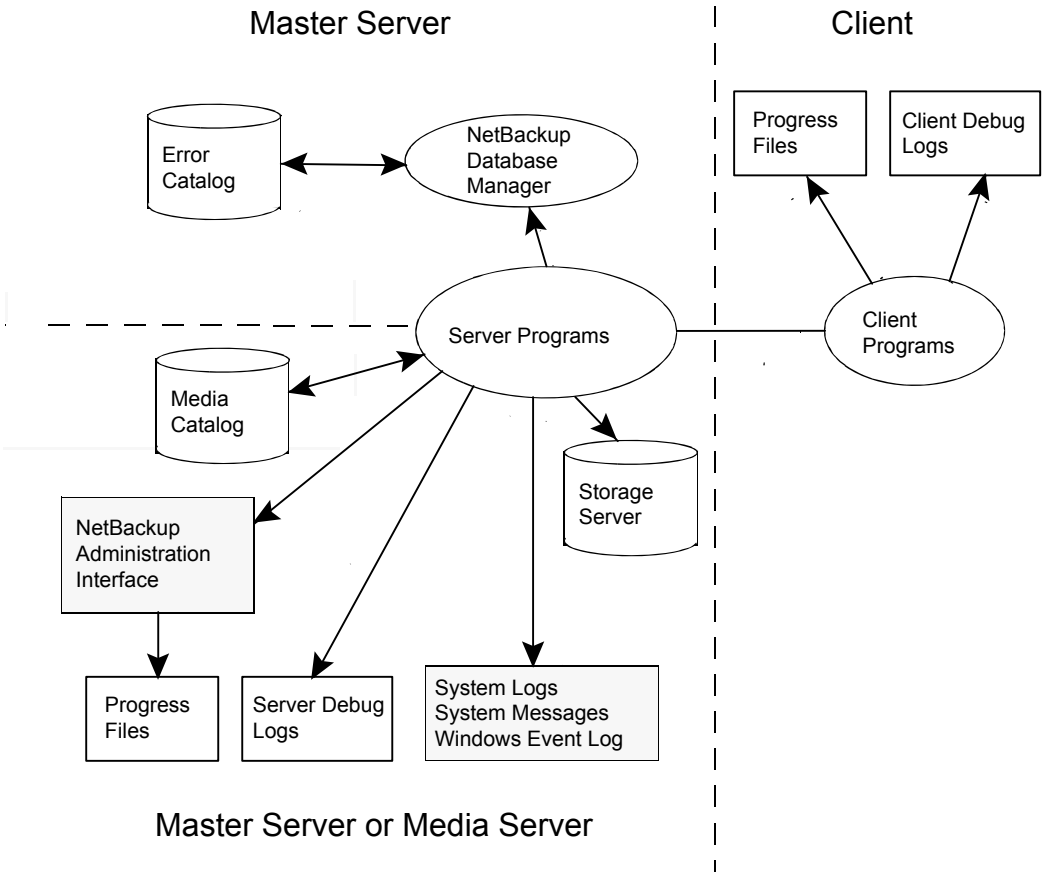
About logs

NetBackup uses several different logs and reports to help you troubleshoot any problems that you encounter.

Users need to know where log and report information is on their systems.

Figure 4-1 shows the location of the log and report information on the client and the server and the processes that make the information available.

Figure 4-1 Logs in the NetBackup Enterprise system



You can review a functional overview that describes the programs and daemons that are mentioned in this figure.

You can also use NetBackup reports to help troubleshoot problems. NetBackup reports give information about status and errors. To run reports, use the **NetBackup Administration Console**.

See the Reports information in the NetBackup Administrator's Guide, Volume I.

Note: The log-entry format in the NetBackup logs is subject to change without notice.

About UNIX system logs

The NetBackup server daemons and programs occasionally log information through the `syslogd` man page. `syslogd` then shows a message or writes the information in an appropriate system log or the console log.

On UNIX, NetBackup automatically records robotic and network errors in the system logs by using `syslogd`. On Windows, NetBackup records robotic and drive errors in the **Event Viewer** Application log. On both operating systems, log entries are also made when robotically controlled drives change between UP and DOWN states.

Note: On HP-UX, the `sysdiag` tool may provide additional information on hardware errors.

To enable system logs, use one of the following:

- Use the `ltid` command that started the device management processes. If the `-v` option is included on the `ltid` command, all daemons that were started as a result also have the `-v` option in effect.
- Use a command to start a specific daemon (for example, `acsd -v`).

On UNIX, enable debug logging to the system logs by including the verbose option (`-v`) on the command that you use to start a daemon.

To troubleshoot `ltid` or robotic software, you must enable system logging. See the `syslogd(8)` man page for information on setting up system logs. Errors are logged with `LOG_ERR`, warnings with `LOG_WARNING`, and debug information with `LOG_NOTICE`. The facility type is daemon.

See the `syslogd` man page for the locations of system log messages on your system.

About unified logging

Unified logging and legacy logging are the two forms of debug logging used in NetBackup. Unified logging creates log file names and messages in a standardized format. All NetBackup processes use either unified logging or legacy logging.

Unlike the files that are written in legacy logging, unified logging files cannot be viewed with a text editor. The unified logging files are in binary format, and some of the information is contained in an associated resource file.

See “About legacy logging” on page 153.

Server processes and client processes use unified logging.

See "Originator IDs for the entities that use unified logging" on page 134.

Unlike legacy logging, unified logging does not require that you create logging subdirectories. Log files for originator IDs are written to a subdirectory with the name specified in the log configuration file. All unified logs are written to subdirectories in the following directory:

UNIX	`/usr/openv/logs`
Windows	*`install_path`*`\NetBackup\logs`

You can access logging controls in the **NetBackup Administration Console**. In the left pane, expand **NetBackup Management > Host Properties > Master Servers** or **Media Servers**. Double-click the server you want to change. In the left pane of the dialog box, click **Logging**.

You can also manage unified logging by using the following commands:

`vxlogcfg`	Modifies the unified logging configuration settings. See "Examples of using vxlogcfg to configure unified logs" on page 151.
`vxlogmgr`	Manages the log files that the products that support unified logging generate. See "Examples of using vxlogmgr to manage unified logs" on page 148.
`vxlogview`	Displays the logs that unified logging generates. See "Examples of using vxlogview to view unified logs" on page 147.

See the NetBackup Commands Reference Guide for a complete description about these commands.

These commands are located in the following directory:

UNIX	`/usr/openv/netbackup/bin`
Windows	*`install_path`*`\NetBackup\bin`

Gathering unified logs for NetBackup

This topic uses an example to describe how to gather unified logs for NetBackup.

To gather unified logs for NetBackup

1. Create a directory named `/upload` by using the following command.

   ```
   # mkdir /upload
   ```

2. Copy unified logs (for NetBackup only) to the `/upload` directory by using the following command:

   ```
   # vxlogmgr -p NB -c --dir /upload
   ```

   Example output:

   ```
   Following are the files that were found:
   /usr/openv/logs/bmrsetup/51216-157-2202872032-050125-0000000.log
   /usr/openv/logs/nbemm/51216-111-2202872032-050125-0000000.log
   /usr/openv/logs/nbrb/51216-118-2202872032-050125-0000000.log
   /usr/openv/logs/nbjm/51216-117-2202872032-050125-0000000.log
   /usr/openv/logs/nbpem/51216-116-2202872032-050125-0000000.log
   /usr/openv/logs/nbsl/51216-132-2202872032-050125-0000000.log
   Total 6 file(s)
   Copying
   /usr/openv/logs/bmrsetup/51216-157-2202872032-050125-0000000.log ...
   Copying
   /usr/openv/logs/nbemm/51216-111-2202872032-050125-0000000.log ...
   Copying
   /usr/openv/logs/nbrb/51216-118-2202872032-050125-0000000.log ...
   Copying
   /usr/openv/logs/nbjm/51216-117-2202872032-050125-0000000.log ...
   Copying
   /usr/openv/logs/nbpem/51216-116-2202872032-050125-0000000.log ...
   Copying
   /usr/openv/logs/nbsl/51216-132-2202872032-050125-0000000.log ...
   ```

3 Change to the `/upload` directory and list its contents.

```
# cd /upload
  ls
```

Example output:

```
51216-111-2202872032-050125-0000000.log
51216-116-2202872032-050125-0000000.log
51216-117-2202872032-050125-0000000.log
51216-118-2202872032-050125-0000000.log
51216-132-2202872032-050125-0000000.log
51216-157-2202872032-050125-0000000.log
```

4 Tar the log files.

```
# tar -cvf file_name.logs ./*
```

Types of unified logging messages

The following message types can appear in unified logging files:

Application log messages

Application log messages include informational, warning, and error messages. They are always logged and cannot be disabled. These messages are localized.

An example of an application message follows:

```
05/02/10 11:02:01.717 [Warning] V-116-18
failed to connect to nbjm, will retry
```

Diagnostic log messages

Diagnostic log messages are the unified logging equivalent of the legacy debug log messages. They can be issued at various levels of detail (similar to verbose levels in legacy logging). These messages are localized.

Diagnostic messages can be disabled with the `vxlogcfg` command.

An example of a diagnostic message follows:

```
05/05/09 14:14:30.347 V-116-71
[JobScheduler::doCatIncr] no configured
session based incremental catalog schedules
```

Debug log messages

Debug log messages are intended primarily for Symantec engineering. Like diagnostic messages, they can be issued at various levels of detail. These messages are not localized.

Debug messages can be disabled with the `vxlogcfg` command.

An example of a debug message follows:

```
10/29/09 13:11:28.065 [taolog] TAO (12066|1) -
Transport_Cache_Manager::bind_i, 0xffbfc194 ->
0x7179d0 Transport[12]
```

File name format for unified logging

Unified logging uses a standardized naming format for log files. The following is an example of a log file name.

```
/usr/openv/logs/nbpem/51216-116-2201360136-041029-0000000000.log
```

Table 4-1 describes each part of the log file name.

Table 4-1 Description of the file name format for unified logging

Example	Description	Details
51216	Product ID	Identifies the product. The NetBackup product ID is 51216. The product ID is also known as the entity ID.
116	Originator ID	Identifies the log writing entity, such as a process, service, script, or other software. The number 116 is the originator ID of the `nbpem` process (the NetBackup policy execution manager).
2201360136	Host ID	Identifies the host that created the log file. Unless the file was moved, this ID is the host where the log resides.
041029	Date	Shows the date when the log was written in YYMMDD format.
0000000000	Rotation	Identifies the numbered instance of a log file for a given originator. The rollover number (rotation) indicates the instance of this log file. By default, log files roll over (rotate) based on file size. If the file reaches maximum size and a new log file is created for this originator, the new file is designated 0000000001. See "About rolling over unified log files" on page 141.

The log configuration file specifies the name of the directories where the log files for originator IDs are written. These directories and the log files that they hold are written to the following directory, except as noted in the following:

See "Originator IDs for the entities that use unified logging" on page 134..

UNIX	`/usr/openv/logs`
Windows	*`install_path`*`\NetBackup\logs`

Originator IDs for the entities that use unified logging

Many server processes, services, and libraries use unified logging. Also, UNIX and Windows clients use unified logging. An originator identifier (OID) corresponds to a NetBackup process, service, or library.

An OID identifies a process, a service, or a library. A process creates entries in its own log file. The process can call a library that also creates entries in the same file but with an OID unique to the library. Hence, a log file can contain entries with different OIDs. Multiple processes can use the same library, so a library OID may appear in several different log files.

Table 4-2 lists the NetBackup server and NetBackup client processes, services, and libraries that use unified logging.

Table 4-2 Originator IDs for the server entities that use unified logging

Originator ID	Entity	Description
18	`nbatd`	The authentication service (`nbatd`) is a service (daemon) that verifies the user identity and issues credentials. These credentials are used for Secure Sockets Layer (SSL) communication. The (`nbatd`) directory is created under the `usr/netbackup/sec/at/bin` directory (UNIX) or the *`install_path`*`\NetBackup\sec\at\bin` directory (Windows).
103	`pbx_exchange`	The Private Branch Exchange (PBX) service provides single-port access to clients outside the firewall that connect to Symantec product services. Service name: `VRTSpbx`. It writes logs to `/opt/VRTSpbx/log` (UNIX) or *`install_path`*`\VxPBX\log` (Windows).
111	`nbemm`	The Enterprise Media Manager (EMM) is a NetBackup service that manages the device and the media information for NetBackup. It runs only on the master server.

Table 4-2 Originator IDs for the server entities that use unified logging *(continued)*

Originator ID	Entity	Description
116	nbpem	The NetBackup Policy Execution Manager (nbpem) creates policy and client tasks and determines when jobs are due to run. It runs only on the master server.
117	nbjm	The NetBackup Job Manager (nbjm) accepts the jobs that the Policy Execution Manager submits and acquires the necessary resources. It.runs only on the master server.
118	nbrb	The NetBackup Resource Broker locates storage units, tape drives, and client reservations for jobs, then starts the jobs. It.works with EMM and runs only on the EMM server.
119	bmrd	The NetBackup Bare Metal Restore (BMR) master server daemon.
121	bmrsavecfg	The BMR Save Configuration is a data collection utility that runs on the NetBackup client, not the server.
122	bmrc	The BMR Client Utility originates on the BMR boot server and runs on the restoring client. UNIX clients use it to communicate to the BMR master server during a restore.
123	bmrs	The BMR Server Utility.
124	bmrcreatefloppy	The BMR Create Floppy utility is used by the BMR commands that create floppy disks. It runs on the BMR boot server and is Windows only.
125	bmrsrt	The BMR Create SRT utility creates a shared resource tree. It runs on the BMR boot server.
126	bmrprep	The BMR Prepare to Restore utility prepares the BMR servers for a client restoration.
127	bmrsetup	The BMR Setup Commands utility sets up BMR installation, configuration, and upgrade processes.
128	bmrcommon	The BMR Libraries and Common Code catalog provides log messages to the BMR libraries.
129	bmrconfig	The BMR Edit Configuration utility modifies the client configuration.
130	bmrcreatepkg	The BMR Create Package utility adds Windows drivers, service packs, and hot fixes to the BMR master server for restore operations.
131	bmrrst	The BMR Restore utility restores Windows BMR clients. It runs on the restoring client for Windows systems only.

Table 4-2 Originator IDs for the server entities that use unified logging *(continued)*

Originator ID	Entity	Description
132	`nbsl`	The NetBackup Service Layer facilitates the communication between the NetBackup graphical user interface and NetBackup logic. `nbsl` is required to run Symantec NetBackup OpsCenter, an application that manages and monitors multiple NetBackup environments. This process runs only on the master server.
134	`ndmpagent`	The NDMP agent daemon manages NDMP backups and restores. It runs on the media server.
137	`libraries`	The libraries control the logging level in the NetBackup libraries. The application and diagnostic messages are for customer use; debug messages are intended for Symantec engineering.
140	`mmui`	The media server user interface is used for the Enterprise Media Manager (EMM).
142	`bmrepadm`	The BMR External Procedure process manages the BMR external procedures that are used during a restore operation.
143	`mds`	The EMM Media and Device Selection process manages the media selection component and device selection component of the Enterprise Media Manager (EMM).
144	`da`	The EMM Device Allocator is used for shared drives.
146	`NOMTRS`	TheSymantec OpsCenter reporting service is part of Symantec OpsCenter.
147	`NOMClient`	The Symantec OpsCenter Client is part of Symantec OpsCenter.
148	`NOMServer`	The Symantec OpsCenter Server is part of Symantec OpsCenter
151	`ndmp`	The NDMP message log (`ndmp`) handles NDMP protocol messages, `avrd`, and robotic processes.
154	`bmrovradm`	The BMR Override Table Admin Utility manages the custom override functions for Bare Metal Restore.

Table 4-2 Originator IDs for the server entities that use unified logging *(continued)*

Originator ID	Entity	Description
156	ace	The NBACE process controls the logging level in the (ACE/TAO) CORBA components for any process that uses a CORBA interface. The default level is 0 (only important messages are logged). This logging is intended for Symantec engineering. If Symantec Technical Support instructs you to increase the logging level, increase the level for originator ID 137 to 4 or higher. **Warning:** A debug logging level greater than 0 generates large amounts of data.
158	ncfrai	Remote access interface for NetBackup clients.
159	ncftfi	Transmater for NetBackup clients.
163	nbsvcmon	The NetBackup Service Monitor monitors the NetBackup services that run on the local computer and tries to restart a service that unexpectedly terminates.
166	nbvault	The NetBackup Vault Manager manages NetBackup Vault. nbvault must be running on the NetBackup Vault server during all NetBackup Vault operations.
178	dsm	The Disk Service Manager (DSM) performs set and get operations on disk storage and disk storage units.
199	nbftsrvr	The Fibre Transport (FT) server process runs on media servers that are configured for NetBackup Fibre Transport. On the server side of the FT connection, nbftsrvrcontrols data flow, processes SCSI commands, manages data buffers, and manages the target mode driver for the host bus adapters. nbftsrvr is part of SAN client.
200	nbftclnt	The Fibre Transport (FT) client process runs on the client and is part of SAN Client.
201	fsm	The FT Service Manager (FSM) is a component of the Enterprise Media Manager (EMM) and is part of SAN Client.
202	stssvc	The Storage service manages the storage server and runs on the media server.
210	ncfive	Exchange Firedrill Wizard for NetBackup clients.

Table 4-2 Originator IDs for the server entities that use unified logging *(continued)*

Originator ID	Entity	Description
219	rsrcevtmgr	The Resource Event Manager (REM) is a CORBA loadable service that runs inside nbemm. REM works with the Disk Polling Service to monitor free space and volume status, and to watch for disk-full conditions.
220	dps	Disk polling service for NetBackup clients.
221	mpms	The Media Performance Monitor Service (MPMS) runs on every media server within RMMS and gathers CPU load and free memory information for the host.
222	nbrmms	Remote monitoring and Management Service (RMMS) is the conduit through which EMM discovers and configures disk storage on media servers.
226	nbstserv	The Storage services controls the lifecycle image duplication operations.
230	rdsm	The Remote Disk Service Manager interface (RDSM) runs within the Remote Manager and Monitor Service. RDMS runs on media servers.
231	nbevtmgr	The Event Manager Service provides asynchronous event management services for cooperating participants.
248	bmrlauncher	The BMR Launcher Utility in the Windows BMR Fast Restore image configures the BMR environment.
254	SPSV2RecoveryAsst	Recovery Assistant for SharePoint Portal Server for NetBackup clients.
261	aggs	Artifact Generator Generated Source.
263	wingui	The NetBackup Administration Console for Windows
271	nbecmsg	Legacy error codes.
272	expmgr	The Expiration Manager handles the capacity management and the image expiration for storage lifecycle operations.
286	nbkms	The Encryption Key Management Service is a master server-based symmetric service that provides encryption keys to the media server NetBackup Tape Manager processes.
293	nbaudit	NetBackup Audit Manager.
294	nbauditmsgs	NetBackup Audit Messages.
309	ncf	NetBackup Client Framework.

Table 4-2 Originator IDs for the server entities that use unified logging *(continued)*

Originator ID	Entity	Description
311	ncfnbservercom	NetBackup Client/Server Communications.
317	ncfbedspi	NetBackup Client Beds Plug-in.
318	ncfwinpi	NetBackup Client Windows Plug-in.
321	dbaccess	NetBackup Relational Database access library.
348	ncforaclepi	NetBackup Client Oracle Plug-in.
351	ncflbc	Live Browse Client.
352	ncfgre	Granular restore.
355	ncftarpi	NetBackup TAR Plug-in.
356	ncfvxmspi	NetBackup Client VxMS Plug-in.
357	ncfnbrestore	NetBackup Restore.
359	ncfnbbrowse	NetBackup Browser.
360	ncforautil	NetBackup Client Oracle utility.
361	ncfdb2pi	NetBackup Client DB2 Plug-in.
362	nbars	NetBackup Agent Request Services.
363	dars	Database Agent Request Server process call
366	ncfnbcs	NetBackup Client Service.
369	importmgr	NetBackup ImportManager.
371	nbim	Image Manager.
372	nbhsm	Hold Service.
373	nbism	NetBackup Indexing service.
375	ncfnbusearchserverpi	NetBackup Client Search Server Plug-in.
377	ncfnbdiscover	NetBackup Client Component Discovery.
380	ncfnbquiescence	NetBackup Client Component Quiescence/Unquiescence.
381	ncfnbdboffline	NetBackup Client Component Offline/Online.

Table 4-2 Originator IDs for the server entities that use unified logging *(continued)*

Originator ID	Entity	Description
385	`ncfnbci`	NetBackup Content Indexer.
386	`ncfvmwarepi`	NetBackup NCF VMware Plug-in.
387	`nbrntd`	NetBackup Remote Network Transport. If multiple backup streams run concurrently, the Remote Network Transport Service writes a large amount of information to the log files. In such a scenario, set the logging level for OID 387 to 2 or less. See "Changing the logging level" on page 168.
395	`stsem`	STS Event Manager.
396	`nbutils`	NetBackup Utilities.
398	`nbevingest`	NetBackup Search Enterprise Vault Ingest.
400	`nbdisco`	NetBackup Discovery.
401	`ncfmssqlpi`	NetBackup Client MSSQL plug-in.
402	`ncfexchangepi`	NetBackup Client Exchange plug-in.
403	`ncfsharepointpi`	NetBackup Client SharePoint plug-in.
412	`ncffilesyspi`	NetBackup Client File System plug-in.

About changing the location of unified log files

The unified logging files can consume a lot of disk space. If necessary, enter the following to direct them to a different location.

UNIX

```
/usr/openv/netbackup/bin/vxlogcfg -a -p NB -o Default -s
LogDirectory=new_log_path
```

Where *new_log_path* is a full path, such as `/bigdisk/logs`.

Windows

```
install_path\NetBackup\bin\vxlogcfg -a -p NB -o Default
-s LogDirectory=new_log_path
```

Where *new_log_path* is a full path, such as `D:\logs`.

About rolling over unified log files

To prevent log files from becoming too large, or to control when or how often logs are created, you can set a log rollover option. When a file size or time setting is reached, the current log file is closed. New log messages for the logging process are written or “rolled over” to a new log file.

You can set log file rollover to occur based on file size, time of day, or elapsed time. Set the conditions by using the `vxlogcfg` command with the options described in Table 4-3.

Table 4-3 vxlogcfg options that control the rollover of unified log files

Option	Description
`MaxLogFileSizeKB`	Specifies the maximum size that is allowed for the log file (in kilobytes) before rollover occurs, if the `RolloverMode` is set to `FileSize`.
`RolloverAtLocalTime`	Specifies the time of day at which the log file is rolled over, if the `RolloverMode` is set to `LocalTime`.
`RolloverPeriodInSeconds`	Specifies a period of time in seconds after which the log file is rolled over, if the `RolloverMode` is set to `Periodic`.
`MaxLogFileSizeKB` or `RolloverAtLocalTime`	Specifies that the log file rollover occurs whenever the file size limit or the local time limit is reached, whichever is first. An example of the command: `vxlogcfg -a -p 51216 -g Default MaxLogFileSizeKB=256 RolloverAtLocalTime=22:00`
`MaxLogFileSizeKB` or `RolloverPeriodInSeconds`	Specifies that the log file rollover occurs whenever the file size limit or the periodic time limit is reached, whichever is first.

A complete description of `vxlogcfg` is in the NetBackup Commands Reference Guide.

By default, log file rollover is based on a file size of 51200 KB. When a log file reaches 51200 KB in size, the file closes and a new log file opens.

The following example sets the NetBackup (`prodid` 51216) rollover mode to `Periodic`.

```
# vxlogcfg -a --prodid 51216 --orgid 116 -s RolloverMode=Periodic
    RolloverPeriodInSeconds=86400
```

The previous example uses the `vxlogcfg` command with the `RolloverMode` option. It sets rollover mode for `nbpem` (originator ID 116) to `Periodic`. It also sets the interval until the next `nbpem` log file rollover to 24 hours (86400 seconds).

In the following example, the file names show the log file rollover with the rotation ID incremented:

```
/usr/openv/logs/nbpem/51216-116-2201360136-041029-0000000000.log
/usr/openv/logs/nbpem/51216-116-2201360136-041029-0000000001.log
/usr/openv/logs/nbpem/51216-116-2201360136-041029-0000000002.log
```

In addition, you can use log file rotation with the following:

- Logs for the server processes that use unified logging
  See "Originator IDs for the entities that use unified logging" on page 134.
- Certain legacy logs
- The unified logging files that the Bare Metal Restore process `bmrsavecfg` creates

About recycling unified log files

Deleting the oldest log files is referred to as recycling. You can recycle unified logging files in the following ways.

Limit the number of log files

Specify the maximum number of log files that NetBackup retains. When the number of log files exceeds the maximum, the oldest log files become eligible for deletion during log cleanup. The `NumberOfLogFiles` option for the `vxlogcfg` command defines that number.

The following example sets to 8000 the maximum number of log files that are allowed for all unified logging originators in the NetBackup (product ID 51216). When the number of log files exceeds 8000 for a particular originator, the oldest log files become eligible for deletion during log cleanup.

```
# vxlogcfg -a -p 51216 -o ALL -s
    NumberOfLogFiles=8000
```

See "Examples of using vxlogcfg to configure unified logs" on page 151.

Specify the number of days the log files are kept	Use the **Keep logs** property to specify the maximum number of days logs are kept. When the maximum number of days is reached, the unified logs and legacy logs are automatically deleted. In the NetBackup Administration Console, in the left pane, expand **NetBackup Management > Host Properties > Master Servers**. Double-click the server you want to change. A new dialog box appears. In the left pane, click **Clean-up > Keep logs**.
Explicitly delete the log files	To initiate recycling and delete the log files, run the following command: `# vxlogmgr -a -d` If you cannot manually delete or move files with `vxlogmgr`, the **Keep logs** property removes the old logs for both unified logging and legacy logging. See "Examples of using vxlogmgr to manage unified logs" on page 148.

If the `vxlogcfg LogRecycle` option is ON (true), the **Keep logs** setting is disabled for unified logs. In this case, unified logging files are deleted when their number (for a particular originator) exceeds the number that the `NumberOfLogFiles` option specifies on the `vxlogcfg` command.

About using the vxlogview command to view unified logs

Use the `vxlogview` command to view the logs that unified logging creates. These logs are stored in the following directory.

UNIX	`/usr/openv/logs`
Windows	*`install_path`*`\logs`

Unlike the files that are written in legacy logging, unified logging files cannot be easily viewed with a text editor. The unified logging files are in binary format, and some of the information is contained in an associated resource file. Only the `vxlogview` command can assemble and display the log information correctly.

You can use `vxlogview` to view NetBackup log files as well as PBX log files.

To view PBX logs using the `vxlogview` command, do the following:

- Ensure that you are an authorized user. For UNIX and Linux, you must have root privileges. For Windows, you must have administrator privileges.

- To specify the PBX product ID. enter `-p 50936` as a parameter on the `vxlogview` command line.

`vxlogview` searches all the files, which can be a slow process. Refer to the following topic for an example of how to display results faster by restricting the search to the files of a specific process.

About query strings used with the vxlogview command

Use the `vxlogview` command to display the logs that unified logging generates. The `vxlogview` command includes the following option: `-w` (`- -where`) *`QueryString`*.

`QueryString` represents a text expression similar to a database WHERE clause. The query string expression is used to retrieve log entries from the unified logging system. The expression is a combination of relational operators, constant integers, constant strings, and names of log fields that evaluate to a single value. Expressions are grouped by logical operators such as AND and OR.

The supported relational operators are as follows:

`<`	less than
`>`	greater than
`<=`	less than and equal to
`>=`	greater than and equal to
`=`	equal to
`!=`	not equal to

The supported logical operators are as follows:

`&&`	logical AND
`||`	logical OR

Table 4-4 shows data types for specific fields as well as description and an example. When more than one example is listed, both examples produce the same results.

Table 4-4 Data types for fields

Field name	Type	Description	Example
PRODID	Integer or string	Provide the product ID or the abbreviated name of product.	PRODID = 51216 PRODID = 'NBU'
ORGID	Integer or string	Provide the originator ID or the abbreviated name of the component.	ORGID = 116 ORGID = 'nbpem'
PID	Long Integer	Provide the process ID	PID = 1234567
TID	Long Integer	Provide the thread ID	TID = 2874950
STDATE	Long Integer or string	Provide the start date in seconds or in the locale-specific short date and time format. For example, a locale may have format 'mm/dd/yy hh:mm:ss AM/PM'	STDATE = 98736352 STDATE = '4/26/11 11:01:00 AM'
ENDATE	Long Integer or string	Provide the end date in seconds or in the locale-specific short date and time format. For example, a locale may have format 'mm/dd/yy hh:mm:ss AM/PM'	ENDATE = 99736352 ENDATE = '04/27/11 10:01:00 AM'
PREVTIME	String	Provide the hours in 'hh:mm:ss' format. This field should be used only with operators =, <, >, >=, and <=	PREVTIME = '2:34:00'
SEV	Integer	Provide one of the following possible severity types: 0 = INFO 1 = WARNING 2 = ERR 3 = CRIT 4 = EMERG	SEV = 0 SEV = INFO

Table 4-4 Data types for fields *(continued)*

Field name	Type	Description	Example
MSGTYPE	Integer	Provide one of the following possible message types: 0 = DEBUG (debug messages) 1 = DIAG (diagnostic messages) 2 = APP (application messages) 3 = CTX (context messages) 4 = AUDIT (audit messages)	MSGTYPE = 1 MSGTYPE = DIAG
CTX	Integer or string	Provide the context token as string identifier or 'ALL' to get all the context instances to be displayed. This field should be used only with the operators = and !=.	CTX = 78 CTX = 'ALL'

Consider the following when writing a query string.

Case sensitivity
: Field names, severity types, and message types are not case-sensitive. For example, the following are valid entries:
  - sev = info
  - msgtype = diag

String constants
: String constants should be given in single quotes. For example, PRODID = 'NBU'

Dates
: Start and end dates can be provided in the following formats:
  - A string constant that corresponds to the regional display short date format
  - A UNIX long value of number of seconds that elapsed since midnight January 1, 1970.

Table 4-5 provides examples of query strings.

Table 4-5 Examples of query strings

Example	Description
(PRODID == 51216) && ((PID == 178964) || ((STDATE == '2/5/09 00:00:00 AM') && (ENDATE == '2/5/03 12:00:00 PM'))	

Table 4-5 Examples of query strings *(continued)*

Example	Description
`((prodid = 'NBU') && ((stdate >= '11/18/09 0:0:0 AM') && (endate <= '12/13/09 13:0:0 AM'))) || ((prodid = 'BENT') && ((stdate >= '12/12/09 0:0:0 AM') && (endate <= '12/25/09 25:0:0 PM')))`	
`(STDATE <= '04/05/09 0:0:0 AM')`	Retrieves the log messages that were logged on or before 2009-05-04 for all the installed Symantec products.

Examples of using vxlogview to view unified logs

The following examples demonstrate how to use the `vxlogview` command to view unified logs.

Table 4-6 Example uses of the vxlogview command

Item	Example
Display all the attributes of the log messages	`vxlogview -p 51216 -d all`
Display specific attributes of the log messages	Display the log messages for NetBackup (51216) that show only the date, time, message type, and message text: `vxlogview --prodid 51216 --display D,T,m,x`
Display the latest log messages	Display the log messages for originator 116 (`nbpem`) that were issued during the last 20 minutes. Note that you can specify `-o nbpem` instead of `-o 116`: `# vxlogview -o 116 -t 00:20:00`
Display the log messages from a specific time period	Display the log messages for `nbpem` that were issued during the specified time period: `# vxlogview -o nbpem -b "05/03/05 06:51:48 AM" -e "05/03/05 06:52:48 AM"`

Table 4-6 Example uses of the vxlogview command *(continued)*

Item	Example
Display results faster	You can use the `-i` option to specify an originator for a process: `# vxlogview -i nbpem` The `vxlogview -i` option searches only the log files that the specified process (`nbpem`) creates. By limiting the log files that it has to search, `vxlogview` returns a result faster. By comparison, the `vxlogview -o` option searches all unified log files for the messages that the specified process has logged. **Note:** If you use the `-i` option with a process that is not a service, `vxlogview` returns the message "No log files found." A process that is not a service has no originator ID in the file name. In this case, use the `-o` option instead of the `-i` option. The -i option displays entries for all OIDs that are part of that process including libraries (137, 156, 309, etc.).
Search for a job ID	You can search the logs for a particular job ID: `# vxlogview -i nbpem | grep "jobid=`*`job_ID`*`"` The `jobid=` search key should contain no spaces and must be lowercase. When searching for a job ID, you can use any `vxlogview` command option. This example uses the `-i` option with the name of the process (`nbpem`). The command returns only the log entries that contain the job ID. It misses related entries for the job that do not explicitly contain the jobid=*job_ID*.

A complete description of `vxlogview` is in the NetBackup Commands Reference Guide.

Examples of using vxlogmgr to manage unified logs

The following examples show how to use the `vxlogmgr` command to manage unified logging files. Log file management includes actions such as deleting or moving the log files.

Table 4-7 Example uses of the vxlogmgr command

Item	Example

List the log files	List all unified log files for the `nbrb` service:
	
	`# vxlogmgr -s -o nbrb`
	`/usr/openv/logs/nbrb/51216-118-1342895976-050503-00.log`
	`/usr/openv/logs/nbrb/51216-118-1342895976-050504-00.log`
	`/usr/openv/logs/nbrb/51216-118-1342895976-050505-00.log`
	`Total 3 file(s)`

Delete the oldest log files	If the `vxlogcfg NumberOfLogFiles` option is set to 1, the following example deletes the two oldest log files for the `nbrb` service:
	
	`# vxlogcfg -a -p 51216 -o nbrb -s NumberOfLogFiles=1`
	`# vxlogmgr -d -o nbrb -a`
	`Following are the files that were found:`
	`/usr/openv/logs/nbrb/51216-118-1342895976-050504-00.log`
	`/usr/openv/logs/nbrb/51216-118-1342895976-050503-00.log`
	`Total 2 file(s)`
	`Are you sure you want to delete the file(s)? (Y/N):`
	`Y`
	`Deleting`
	`/usr/openv/logs/nbrb/51216-118-1342895976-050504-00.log ...`
	`Deleting`
	`/usr/openv/logs/nbrb/51216-118-1342895976-050503-00.log ...`

Delete the newest log files	Delete all the unified log files that NetBackup created in the last 15 days: `# vxlogmgr -d --prodid 51216 -n 15` Make sure that you roll over (rotate) the log files before you recycle them.
Delete the log files for a specific originator	Delete all unified log files for originator `nbrb`: `# vxlogmgr -d -o nbrb` Make sure that you roll over (rotate) the log files before you recycle them.
Delete all the log files	Delete all unified log files for NetBackup:. `# vxlogmgr -d -p NB` Make sure that you roll over (rotate) the log files before you recycle them.

Table 4-7 Example uses of the vxlogmgr command *(continued)*

Item	Example

Control the number of log files	You can use the `vxlogmgr` command with the `vxlogcfg` command's `NumberOfLogFiles` option to manually delete log files.
	
	For example, the `NumberOfLogFiles` option is set to 2, you have 10 unified logging files, and cleanup has not occurred. Enter the following to keep the two most recent log files and delete the rest for all originators:
	
	`# vxlogmgr -a -d`
	
	The following command keeps the two most recent log files of all PBX originators:
	
	`# vxlogmgr -a -d -p ics`
	
	The following deletes the older log files for the `nbrb` service only:
	
	`# vxlogmgr -a -d -o nbrb`

Control disk space usage	Periodically run the `vxlogmgr -a -d` command (such as through a `cron` job) to delete logs and monitor the disk space that unified logging uses. The disk space that a given originator uses can be calculated as follows: `NumberOfFiles` for originator * `MaxLogFileSizeKB` for originator The total disk space that unified logs consume is the sum of the disk space that each originator consumes. If none of the originators overrides the `NumberOfFiles` and `MaxLogFileSizeKB` settings, then the total disk space that unified logging consumes is as follows: Number of originators * default `MaxLogFileSizeKB` * default `NumberOfFiles` Use the `vxlogcfg` command to list the current unified logging settings. For example, assume the following: ■ `vxlogmgr -a -d -p NB` is configured as a `cron` job with a frequency of one hour. ■ No originators override default settings for `MaxLogFileSizeKB` or `NumberOfFiles`. ■ The number of active NetBackup originators on the host is 10. (Typical of a NetBackup master server that is not running BMR or NDMP.) ■ The default `MaxLogFileSizeKB` is equal to 5120. ■ The default `NumberOfFiles` is equal to 3. To calculate the total disk space that unified logging consumes, insert the values from the example into the previous formula. The results are as follows: 10 * 5120 * 3 KB = 15,360 KB of additional disk space used each hour.

A complete description of `vxlogmgr` is in the NetBackup Commands Reference Guide.

Examples of using vxlogcfg to configure unified logs

Use the `vxlogcfg` command to change logging levels and rollover settings.

The `vxlogcfg` command has the following characteristics:

- The `vxlogcfg` command is the only way to turn off diagnostic and debug messages in unified logging. In legacy logging, the writing of messages cannot be turned off, only minimized.
- The `vxlogcfg` options for robust file logging (`MaxLogFileSizeKB` and `NumberOfLogFiles`) also affect certain legacy logs.
  See "About limiting the size and the retention of legacy logs" on page 163.
- Absolute paths must be specified. Do not use relative paths.

The following examples show how to use the `vxlogcfg` command to configure unified logging settings.

Table 4-8 Example uses of the vxlogcfg command

Item	Example

Set the maximum log file size	By default, the maximum log file size in unified logging is 5120 KB. When a log file reaches 5120 KB, the file closes and a new log file opens.
	
	You can change the maximum file size with the `MaxLogFileSizeKB` option. The following command changes the default maximum log size to 2048 KB for the NetBackup product:
	
	`# vxlogcfg -a -p 51216 -o Default -s MaxLogFileSizeKB=100000`
	
	For `MaxLogFileSizeKB` to be effective, the `RolloverMode` option must be set to `FileSize` :
	
	`# vxlogcfg -a --prodid 51216 --orgid Default -s RolloverMode=FileSize`
	
	`MaxLogFileSizeKB` can be set per originator. An originator that is not configured uses the default value. The following example overrides the default value for service `nbrb` (originator 118).
	
	`# vxlogcfg -a -p 51216 -o nbrb -s MaxLogFileSizeKB=1024`

Table 4-8 Example uses of the vxlogcfg command *(continued)*

Item	Example
Set log recycling	The following example sets automatic log file deletion for `nbemm` logs (originator ID 111): `# vxlogcfg -a --prodid 51216 --orgid 111 -s RolloverMode=FileSize MaxLogFileSizeKB=512000 NumberOfLogFiles=999 LogRecycle=TRUE` This example sets `nbemm` rollover mode to file size, and turns on log recycling. When the number of log files exceeds 999, the oldest log file is deleted. EXAMPLE 5 shows how to control the number of log files.
Set debug level and diagnostic level	The following example sets the default debug level and diagnostic level of product ID NetBackup (51216): `# vxlogcfg -a --prodid 51216 --orgid Default -s DebugLevel=1 DiagnosticLevel=6`

List the unified logging settings	The following `vxlogcfg` example shows how to list the active unified logging settings for a given originator (the `nbrb` service). Note that `MaxLogFileSizeKB`, `NumberOfLogFiles`, and `RolloverMode` are included in the output.
	
	`# vxlogcfg -l -o nbrb -p NB`
	
	`Configuration settings for originator 118, of product 51,216...`
	`LogDirectory = /usr/openv/logs/`
	`DebugLevel = 5`
	`DiagnosticLevel = 5`
	`LogToStdout = False`
	`LogToStderr = False`
	`LogToOslog = False`
	`RolloverMode = FileSize`
	`MaxLogFileSizeKB = 5120`
	`RolloverPeriodInSeconds = 43200`
	`RolloverAtLocalTime = 0:00`
	`NumberOfLogFiles = 4`
	`...`

A complete description of `vxlogcfg` is in the NetBackup Commands Reference Guide.

About legacy logging

Legacy logging and unified logging are the two forms of debug logging used in NetBackup. In legacy debug logging, each process creates logs of debug activity in its own logging directory. All NetBackup processes use either unified logging or legacy logging.

See "About unified logging" on page 129.

To enable legacy debug logging on NetBackup servers, you must first create the appropriate directories for each process.

UNIX	`/usr/openv/netbackup/logs` `/usr/openv/volmgr/debug`
Windows	*`install_path`*`\NetBackup\logs` *`install_path`*`\Volmgr\debug`

After the directories are created, NetBackup creates log files in the directory that is associated with each process. A debug log file is created when the process begins.

To enable debug logging for the NetBackup Status Collection Daemon (`vmscd`), create the following directory before you start `nbemm`.

As an alternative, you can stop and restart `nbemm` after creating the following directory:

UNIX	`/usr/openv/volmgr/debug/reqlib`
Windows	*`install_path`*`\Volmgr\debug\reqlib\`

Tables are available that list the log directories that you must create.

See "Directory names for legacy debug logs for servers " on page 159.

See "Directory names for legacy debug logs for media and device management" on page 161.

Note: On a Windows server, you can create the debug log directories at once, under *`install_path`*`\NetBackup\Logs`, by running the following batch file: *`install_path`*`\NetBackup\Logs\mklogdir.bat`.

Media servers have only the `bpbrm`, `bpcd`, `bpdm`, and `bptm` debug logs.

UNIX client processes that use legacy logging

Most UNIX client processes use legacy logging. To enable legacy debug logging on UNIX clients, create the appropriate subdirectories in the following directory.

```
/usr/openv/netbackup/logs
```

Note: Create the directories with access modes of 777 so that user processes can write to the log files.

Table 4-9 describes the directories for the legacy debug logs that apply to UNIX clients.

Table 4-9 UNIX client processes that use legacy logging

Directory	Associated process
`bp`	Menu driven client-user interface program.
`bparchive`	Archive program. Also useful for debugging `bp`.
`bpbackup`	Backup program. Also useful for debugging `bp`.
`bpbkar`	Program that is used to generate backup images.
`bpcd`	NetBackup client daemon or manager.
`bphdb`	Program that starts a script to back up a database on a NetBackup database agent client. See the system administrator's guide for the appropriate NetBackup database agent for more information.
`bpjava-msvc`	The NetBackup-Java application server authentication service that `inetd` starts during startup of the NetBackup Java interface applications. This program authenticates the user that started the application.
`bpjava-usvc`	The NetBackup program that `bpjava-msvc` starts upon successful logon through the logon dialog box that is presented when a NetBackup-Java interface is started. This program services all requests from the Java administration and user interfaces on the host where `bpjava-msvc` is running.
`bplist`	Program that lists backed up and archived files. Also useful for debugging bp.
`bpmount`	Program that determines local mount points and wildcard expansion for multiple data streams.

Table 4-9 UNIX client processes that use legacy logging *(continued)*

Directory	Associated process
bporaexp	Command-line program on clients to export Oracle data in XML format. Communicates with bprd on server.
bporaexp64	64-bit command-line program on clients to export Oracle data in XML format. Communicates with bprd on server.
bporaimp	Command-line program on clients to import Oracle data in XML format. Communicates with bprd on server.
bporaimp64	64-bit command-line program on clients to import Oracle data in XML format. Communicates with bprd on server.
bprestore	Restore program. Also useful for debugging bp.
db_log	For more information on these logs, see the NetBackup guide for the database-extension product that you use.
mtfrd	These logs have information about the mtfrd process, which is used for phase 2 imports and restores of Backup Exec media.
tar	tar process during restores.
user_ops	The user_ops directory is created during the install of NetBackup on all servers and clients. The NetBackup Java interface programs use it for the following: temporary files and for job and progress log files that the **Backup, Archive, and Restore** program (jbpSA) generates. This directory must exist for successful operation of any of the Java programs and must have public read, write, and run permissions. This directory contains a directory for every user that uses the Java programs. In addition, on NetBackup-Java capable platforms, the NetBackup Java interface log files are written in a subdirectory that is called nbjlogs. All files in the user_ops directory hierarchy are removed according to the setting of the KEEP_LOGS_DAYS configuration option.

PC client processes that use legacy logging

Most PC client processes use legacy logging. To enable detailed legacy debug logging on Windows clients, create the directories in the following location. The directory names that you create correspond to the processes you want to create logs for.

```
C:\Program Files\VERITAS\NetBackup\Logs\
```

Note: These are the default locations in which to place these directories. You can specify another location during client installation.

Table 4-10 lists the legacy debug log directories that apply to these clients.

Table 4-10 PC client processes that use legacy logging

Directory	NetBackup client	Associated process
`bpinetd`	Windows2003	Client service logs. These logs have information on the `bpinetd32` process.
`bparchive`	Windows 2003	Archive program that is run from the command line.
`bpbackup`	Windows 2003	The backup program that is run from the command line.
`bpbkar`	Windows 2003	Backup and archive manager. These logs have information on the `bpbkar32` process.
`bpcd`	All Windows clients	NetBackup client daemon or manager. These logs have information on communications between the server and client.
`bpjava-msvc`	The NetBackup-Java application server authentication service that the `Client Services` service starts during startup of the NetBackup Java interface applications. This program authenticates the user that started the application. (On all Windows platforms.)	`bpjava-msvc`

Table 4-10 PC client processes that use legacy logging *(continued)*

Directory	NetBackup client	Associated process
bpjava-usvc	NetBackup program that bpjava-msvc starts upon successful logon through the logon dialog box that is presented when a NetBackup-Java interface is started. This program services all requests from the Java administration and user interfaces on the NetBackup host where bpjava-msvc is running. (On all Windows platforms.)	bpjava-usvc
bplist	Windows 2003	List program that is run from the command line.
bpmount	Windows 2003	The program that is used to collect drive names on the client for multistreaming clients.
bprestore	Windows 2003	The restore program that is run from the command line.
tar	Windows 2003	tar process. These logs have information about the tar32 process.

Table 4-10 PC client processes that use legacy logging *(continued)*

Directory	NetBackup client	Associated process
`user_ops`	Windows 2003	The `user_ops` directory is created during the install of NetBackup on all servers and clients. The NetBackup Java interface programs use it for the following: temporary files and for job and progress log files that the **Backup, Archive, and Restore** program (`jbpSA`) generates. This directory must exist for successful operation of any of the Java programs and must have public read, write, and run permissions. `user_ops` contains a directory for every user that uses the Java programs. In addition, on NetBackup-Java capable platforms, the NetBackup Java interface log files are written in a subdirectory that is called `nbjlogs`. All files in the `user_ops` directory hierarchy are removed according to the setting of the KEEP_LOGS_DAYS configuration option.

File name formats for legacy logging

In the standard legacy log system, a single NetBackup process creates one debug log file per day. In the legacy logging system with **Enable robust logging** enabled, a NetBackup process creates a certain number of log files. Each file grows to a certain size before it closes and a new one is created.

Legacy logging uses two formats for log file names. The format that is used depends on whether the log uses the standard system or file rotation (robust logging).

Table 4-11 File name formats for different types of legacy logging

Type	File name format
Standard legacy logging	■ On UNIX: `log.`*`mmddyy`* For example: `log.040805` ■ On Windows: *`mmddyy`*`.log` For example: `040105.log`

Table 4-11 File name formats for different types of legacy logging *(continued)*

Type	File name format
Legacy logging with robust logging enabled	*mmddyy_nnnnn*.log For example: 040105_00001.log Where *nnnnn* is a counter or a rotation number for the log file. When the counter exceeds the setting for number of log files, the oldest log file is deleted. The NumberOfLogFiles option on the vxlogcfg command sets the number of log files.

For compatibility with existing scripts, the debug log file naming format does not change. If you enable robust file logging after you create standard legacy logs, only the log files for the processes that robust logging governs use the file rotation naming format.

Any mixture of new and old log file names in a legacy debug log directory is managed according to the **Keep logs** setting and the robust logging settings.

Directory names for legacy debug logs for servers

Table 4-12 describes the directories you need to create to support legacy debug logs for servers. Each directory corresponds to a process. Unless it is noted, each directory should be created under the following directory.

UNIX	/usr/openv/netbackup/logs
Windows	*install_path*\NetBackup\logs

Table 4-12 Directory names for legacy debug logs

Directory	Associated process
admin	Administrative commands.
bpbrm	NetBackup backup and restore manager.
bpcd	NetBackup client daemon or manager. The NetBackup Client service starts this process
bpdbjobs	NetBackup jobs database manager program.
bpdm	NetBackup disk manager.
bpdbm	NetBackup Database Manager. This process runs only on master servers. On Windows systems, it is the NetBackup Database Manager service.

Table 4-12 Directory names for legacy debug logs *(continued)*

Directory	Associated process
bpjava-msvc	The NetBackup-Java application server authentication service that is started when the NetBackup Java interface applications start. On UNIX servers, inetd starts it. On Windows servers, the Client Services service starts it. This program authenticates the user that started the application.
bpjava-susvc	The NetBackup program that bpjava-msvc starts upon successful logon through the logon dialog box that is presented when a NetBackup-Java interface starts. This program services all requests from the Java user interfaces on the NetBackup master or media server host where the bpjava-msvc program runs (all Windows platforms).
bprd	NetBackup request daemon or manager. On Windows systems, this process is called the NetBackup Request Manager service.
bpsynth	The NetBackup process for synthetic backup. nbjm starts bpsynth. bpsynth runs on the master server.
bptm	NetBackup tape management process.
nbatd	Authentication daemon (UNIX and Linux) or service (Windows). nbatd authenticates access to interfaces of NetBackup services or daemons.
nbazd	Authorization daemon (UNIX and Linux) or service (Windows). nbazd authorizes access to interfaces of NetBackup services or daemons.
syslogs	System log. You must enable system logging to troubleshoot ltid or robotic software. See the syslogd man page.
user_ops	The user_ops directory is created during the install of NetBackup on all servers and clients. NetBackup Java interface programs use it for the following: temporary files and for job and progress log files that the **Backup, Archive, and Restore** program (jbpSA) generates. This directory must exist for successful operation of any of the Java programs and must have public read, write, and execute permissions. user_ops contains a directory for every user that uses the Java programs. In addition, on NetBackup-Java capable platforms, the NetBackup Java interface log files are written in the nbjlogs subdirectory. All files in the user_ops directory hierarchy are removed according to the setting of the KEEP_LOGS_DAYS configuration option.

Table 4-12 Directory names for legacy debug logs *(continued)*

Directory	Associated process
vnetd	The Symantec network daemon, used to create firewall-friendly socket connections. Started by the inetd(1M) process. **Note:** Logging occurs in either the /usr/openv/logs directory or the /usr/openv/netbackup/logs if the vnetd directory exists there. If the vnetd directory exists in both locations, logging occurs only in /usr/openv/netbackup/logs/vnetd.

More information is available on the programs and daemons that write the logs.

See "About backup and restore functional overview" on page 278.

On UNIX systems, also refer to the README file in the /usr/openv/netbackup/logs directory.

Directory names for legacy debug logs for media and device management

The debug log directories enable logging for the media management processes and device management processes. Table 4-13 describes the directories you need to create to support legacy debug logs for media and device management. Each directory corresponds to a process.

Table 4-13 Media and device management legacy debug logs

Directory	Associated process
acsssi	UNIX only. Debug information on transactions between NetBackup and the StorageTek ACSLS server.
daemon	Debug information for vmd (NetBackup Volume Manager service, Windows) and its associated processes (oprd and rdevmi). Stop and restart vmd after creating the directory.
ltid	Debug information on ltid, the Media Manager device daemon (UNIX), or on the NetBackup Device Manager service (Windows), and on avrd. Stop and restart ltid after creating the directory.
reqlib	Debug information on the processes that request media management services from vmd or EMM. Stop and restart vmd after creating the directory.
robots	Debug information on all robotic daemons, which includes tldcd, tl8cd, and tl4d daemons. Stop and restart robotic daemons.

Table 4-13 Media and device management legacy debug logs *(continued)*

Directory	Associated process
`tpcommand`	Debug information for device configuration, including the `tpconfig` and the `tpautoconf` commands and the **NetBackup Administration Console**.
`vmscd`	Debug information for the NetBackup Status Collection daemon. Stop and restart `vmscd` after creating the directory.

Unless it is noted, each directory should be created under the following directory.

UNIX /usr/openv/volmgr/debug

Windows *install_path*\Volmgr\debug

NetBackup creates one log per day in each of the debug directories.

You can disable debug logging by deleting or renaming the following directory:

UNIX: `vmd` command `/usr/openv/volmgr/debug/daemon`

Windows: NetBackup Volume Manager service *`install_path`*`\Volmgr\debug\daemon`

See "File name formats for legacy logging" on page 158.

See "About limiting the size and the retention of legacy logs" on page 163.

See "Directory names for legacy debug logs for media and device management" on page 161.

How to control the amount of information written to legacy logging files

You can set legacy logging levels to increase the amount of information that NetBackup processes write in the logs.

The following settings affect legacy logging, except media and device management.

- Increase the **Global logging level**.
  See "Changing the logging level" on page 168.

  Note: This setting also affects unified logging.

- On UNIX, add a `VERBOSE` entry in the `/usr/openv/netbackup/bp.conf` file.

If you enter VERBOSE without a value, the verbose value defaults to 1. For more log detail, enter VERBOSE = 2 or a higher value. This setting affects legacy logging only.

Warning: High verbose values can cause debug logs to become very large.

- Set the logging level for individual processes.
  In **Host Properties**, change logging levels for individual processes in the **Logging** dialog box. Or, specify the verbose flag (if available) when you start the program or daemon.
  Also, you can set the logging level of an individual process to a negative value in the bp.conf file as follows:
  <processname>_VERBOSE = -2 completely disables logs for the corresponding process.
  <processname>_VERBOSE = -3 the corresponding process only logs informational, warning, and error messages in the debug logs.
  See more about logging properties in the NetBackup Administrator's Guide, Volume I.

Media and device management legacy logging has two levels: not verbose (the default) and verbose. To set the verbose (higher) level, add the word VERBOSE to the vm.conf file. Create the file if necessary. Restart ltid and vmd after you add the VERBOSE entry. This entry affects logging levels in the **Event Viewer** Application and System log. The vm.conf file is located in the following directory:

UNIX	/usr/openv/volmgr/
Windows	*install_path*\Volmgr\

About limiting the size and the retention of legacy logs

Certain NetBackup processes write legacy debug logs. Because legacy debug logs can grow very large, enable them only if unexplained problems exist. Delete the logs and the associated directories when they are no longer needed.

To limit the time NetBackup retains legacy debug logs, specify the number of days in the **Keep logs** field. The default is 28 days. You can specify the number under **Host Properties** in the **Clean-up** dialog box.

See the NetBackup Administrator's Guide, Volume I for more information about clean-up properties.

To limit the amount of disk space that the logs consume, use robust logging. Robust logging involves file rotation, like that which is used in unified logging. Robust logging does not apply to media and device management logging.

See "About rolling over unified log files" on page 141.

Specify the maximum size for a log file and the maximum number of log files to keep in a logging directory. When a log file grows to its maximum size, it closes and a new file opens. If the number of log files exceeds the number that is allowed for the directory, the oldest file is deleted.

Logs created by the following NetBackup processes can use log rotation (robust logging):

- `bpbrm`
- `bpcd`
- `bpdbm`
- `bpdm`
- `bprd`
- `bptm`

For the legacy logs created by other NetBackup processes (except media and device management logs), use the **Keep logs** property.

The **Keep logs** property may override the robust file logging settings. If **Keep logs** is set to 10 days and robust file logging settings allow more than 10 days, the logs are deleted on day 11.

For media and device management legacy logs, use the `DAYS_TO_KEEP_LOGS` setting in the `vm.conf` file to control log file rotation. The default is infinite retention. The `vm.comf` file is located in the following directory:

UNIX	`/usr/openv/volmgr/`
Windows	*`install_path`*`\Volmgr\`

To retain logs for three days, enter the following in the `vm.conf` file:

See NetBackup Administrator's Guide, Volume II for instructions about how to use this entry.

```
DAYS_TO_KEEP_LOGS = 3
```

Configuring legacy log rotation

You can specify the maximum file size for a legacy log and the maximum number of log files to retain.

To configure the legacy log rotation

1. In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Host Properties > Master Servers**.
2. In the right pane, double-click the server you want to modify.
3. In the dialog box that appears, in the left pane, select **Logging** and check **Enable robust logging**.

   Robust logging applies only to legacy logs. Robust logging is also known as log rotation.

   By default, the maximum file size is 5120 KB and the maximum number of files that are kept per log directory is 3.

   If **Enable robust logging** is disabled, the standard behavior remains in effect. A single log file is created per log directory per day, and log deletion is based on the **Keep logs** property.
4. To change the maximum file size or the maximum number of log files per directory, use the `MaxLogFileSizeKB` and the `NumberOfLogFiles` options. These options are part of the `vxlogcfg` command, which is located in the following directory:

UNIX	`/usr/openv/netbackup/bin`
Windows	*`install_path`*`\NetBackup\bin`

   Use the following example to set the maximum file size to 2048 and the maximum number of log files per log directory to 10:

   ```
   vxlogcfg -a -p 51216 --orgid Default -s
   MaxLogFileSizeKB=2048,NumberOfLogFiles=10
   ```

   The example sets the default values for all unified logging processes and for all legacy processes for NetBackup (product ID 51216).

A complete description of `vxlogcfg` is in the NetBackup Commands Reference Guide.

Creating legacy log directories to accompany problem reports for synthetic backup

If the legacy log directories have not been created, you must create them. If the directories do not exist, the logs cannot be written to disk.

Table 4-14 Creating legacy log directories

Step	Action	Description
Step 1	Create directories on the master server.	Create the following directories: *install_path*/netbackup/logs/bpsynth *install_path*/netbackup/logs/bpdbm *install_path*/netbackup/logs/vnetd
Step 2	Create directories on the media server.	Create the following directories: *install_path*/netbackup/logs/bpcd *install_path*/netbackup/logs/bptm *install_path*/netbackup/logs/bpdm
Step 3	Change the **Global logging level**.	In **Host Properties**, select a master server and set the **Global logging level** to 5. See "Changing the logging level" on page 168. See "About global logging levels" on page 166. See "Using the Host Properties window to access configuration settings" on page 67.
Step 4	Rerun the job.	Rerun the job and gather the logs from the directories that you created. The bptm logs are required only if the images are read from or written to a tape device. The bpdm logs are needed only if the images are read from or written to disk. If the images are read from multiple media servers, the debug logs for bptm or bpdm must be collected from each media server.

See "Logs to accompany problem reports for synthetic backups" on page 170.

About global logging levels

Global logging levels refer to unified logging and legacy logging. The logging level determines how much information is included in the log message. The higher the level number, the greater the amount of detail is in the log messages.

Table 4-15 describes all logging levels and the detail that each level includes.

Table 4-15 Global logging levels

Logging level	Description
Minimum logging	Includes very important, low-volume diagnostic messages and debug messages. The Host Properties Logging page or Logging Assistant can set minimum logging. Legacy logs use the following values to represent minimum logging: ■ UNIX: The `bp.conf` file displays `VERBOSE=0` (global). `<processname>_VERBOSE = 0` represents using the global default for an individual process. ■ Windows: Registry displays the following hexadecimal value: 0xffffffff Unified logging uses the value 1 to represent minimum logging.
Disable logging	The Host Properties Logging page or Logging Assistant can set disable logging. Legacy logs use the following values to represent disabled logging: ■ UNIX: The `bp.conf` file displays `VERBOSE=-2` (global) or `<processname>_VERBOSE = -2` for an individual process. ■ Windows: Registry displays the following hexadecimal value: 0xfffffffe Unified logging uses the value 0 to represent disabled logging.
1	Adds verbose diagnostic messages and debug messages to the low-volume diagnostic messages that are associated with minimum logging.
2	Adds the progress messages.
3	Adds the informational dumps.
4	Adds the function entry and exits.
5	Includes everything. The finest detail of messages.

Unified logging is enabled by default to log debug messages at level 0 and application messages at level 5.

The following actions affect logging levels:

- In the **Global logging level** list, a zero (0) level specifies the minimum level of logging for both legacy and unified logging. However, for diagnostic and debug messages in unified logging, the logging level can be turned off completely. No

diagnostic messages or debug messages are logged. This level cannot be set with the **Global logging level** list in the **NetBackup Administration Console**. You can set it with the `vxlogcfg` command or Logging Assistant.

See "Changing the logging level" on page 168.
See "Examples of using vxlogcfg to configure unified logs" on page 151.

- A change to the **Global logging level** list affects the logging level of all NetBackup and Enterprise Media Manager (EMM) processes on the server or client. (The exceptions are PBX and media and device management logging.) This setting overrides any previous settings.
- If you make a change to the VERBOSE level in the `bp.conf` file or the `vm.conf` file, it only affects the legacy logging level.
  See "How to control the amount of information written to legacy logging files" on page 162.
- If you make a change with the `vxlogcfg` command, it only affects the unified logging level.

A change to the **Global logging level** list does not affect the level of the following logging processes:

- PBX logging
  See "Accessing the PBX logs" on page 76.
- Media and device management logging (`vmd`, `ltid`, `avrd`, robotic daemons, media manager commands)
  See "Directory names for legacy debug logs for media and device management" on page 161.
- Any unified logging process whose debug level has been changed from the default setting

Changing the logging level

The logging level determines how much information is included in the log message. The log range is 0-5. The higher the level number, the greater the amount of detail is in the log message.

To change the logging level

1. In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Host Properties**.
2. Select **Master Servers**, **Media Servers**, or **Clients**.
3. In the right pane, click the server or client to view the version and platform. Then, double-click to view the properties.

4 In the properties dialog box, in the left pane, click **Logging**.

5 In the **Global logging level** list, select a value from 0 to 5.

Changes affect the logging level of both unified logging and legacy logging.

See "About global logging levels" on page 166.

6 Click **OK**.

Changing the logging level on Windows clients

You can increase the amount of information that client processes write in the logs.

To change the logging level on Windows clients

1 In the **NetBackup Administraion Console**, on the **File** menu, click **Backup, Archive, and Restore**.

2 In the **Backup, Archive, and Restore** interface, on the **File** menu, click **NetBackup Client Properties**.

3 In the **NetBackup Client Properties** dialog box, select the **Troubleshooting** tab.

4 In the **Verbose** property field, enter a debug level from 0 to 5.

Use the default level of 0 unless advised otherwise by Technical Support. Higher levels can cause the logs to accumulate large amounts of information.

5 Click **OK**.

For the unified logging files that the Bare Metal Restore process `bmrsavecfg` creates, you also can control the logging level with the `vxlogcfg` command.

See "Examples of using vxlogcfg to configure unified logs" on page 151.

An increase in the log level can cause the logs to grow very large; increase the logging level only if unexplained problems exist.

Setting debug logging to a higher level

To solve many error conditions, set debug logging to a higher level. Then retry the operation and examine the debug logs.

To set debug logging to a higher level

1. Enable legacy debug logging by creating the necessary directories and folders.
2. Increase the level of verbosity for media and device management processes by adding the VERBOSE option in the `vm.conf` file. This file is located in `/usr/openv/volmgr/` (UNIX and Linux) or `install_path\Volmgr\` (Windows).
3. Restart the daemons and services or run the command verbose option, if available.

Logs to accompany problem reports for synthetic backups

To debug problems with synthetic backups, you must include a complete set of logs in the problem report and additional items. Send all the information to Symantec Technical Support.

Include the following log types:

- Log files that unified logging creates
  See "Gathering unified logs for NetBackup" on page 130.
- Log files that legacy logging creates
  See "Creating legacy log directories to accompany problem reports for synthetic backup" on page 166.

Include the following additional items:

Try file	The try file is located in the following directory: *install_path*/netbackup/db/jobs/trylogs/*jobid*.t If the job ID of the synthetic backup job was 110, the try file is named `110.t`.
Policy attributes	Use the following command to capture the policy attributes: *install_path*/netbackup/bin/admincmd/bppllist *policy_name* -L where *policy_name* is the name of the policy for which the synthetic backup job was run.
List of storage units	Capture the list of storage units from the following command: *install_path*/netbackup/bin/admincmd/bpstulist -L

See “Creating legacy log directories to accompany problem reports for synthetic backup” on page 166.

Setting retention limits for logs on clients

You can specify the numbers of days that NetBackup retains client logs on UNIX and Windows.

To set retention limits for logs on UNIX clients

1. In the **NetBackup Administration Console**, in the left pane, expand **Host Properties > Clients**.
2. In the right pane, double-click the client you want to modify.
3. In the properties dialog box, click **UNIX Client**.
4. In the **Client Settings** dialog box, find the **Keep status of user-directed backups, archives, and restores for** field.
5. Enter the number of days you want to retain the log files, and click **OK**.

To set the retention limits for logs on Windows clients

1. In the **NetBackup Adminsistration Console**, on the **File** menu, click **Backup, Archive, and Restore**.
2. In the **Backup, Archive, and Restore** interface, on the **File** menu, click **NetBackup Client Properties**.
3. In the **NetBackup Client Properties** dialog box, select the **General** tab.
4. In the **Keep status of user-directed backups, archives, and restores for** field, enter the number of days you want to retain the log files.
5. Click **OK**.

Logging options with the Windows Event Viewer

NetBackup Windows master servers can be configured so messages from NetBackup reports are written to the Windows **Event Viewer** Application log. You can see these messages in the Application log and also use third-party tools to monitor the Application log for these messages.

To route unified logging application and diagnostic messages for an originator to the Application log, set the `LogToOslog` value to true for that originator.

The following example routes the application and diagnostic messages for `nbrb` to the Windows event log:

```
# vxlogcfg -a -o nbrb -p NB -s "LogToOslog=true"
```

Note: For this setting to take effect, restart NetBackup services.

To enable the logging tool, do the following:

- Create the following file on the NetBackup master server.

  install_path\NetBackup\db\config\eventlog

- Optionally, add an entry to the `eventlog` file. The following is an example:

  ```
  56 255
  ```

The parameters in the `eventlog` represent severity and type. The parameters have the following characteristics:

Severity
- Listed as the first parameter.
- Controls the messages that NetBackup writes to the Application log.
- If the file is empty, the default severity is **Error** (16).
- If the file has only one parameter, it is used for the severity level.

Type
- Listed as the second parameter.
- Controls the type of messages that NetBackup writes to the Application log.
- If the file is empty, the default type is **Backup Status** (64).

Both parameters are specified as decimal numbers and equate to a bitmap that expresses the following values:

Severity

1 = Unknown

2 = Debug

4 = Info

8 = Warning

16 = Error

32 = Critical

Type	1 = Unknown
	2 = General
	4 = Backup
	8 = Archive
	16 = Retrieve
	32 = Security
	64 = Backup Status
	128 = Media Device

You can configure the `eventlog` file to log the messages that include several different severities and types. Consider the results that the following entry in the `eventlog` file produces:

```
56 255
```

Entry `56`	Produces a log with messages that have a severity of warning, error, and critical. (56 = 8 + 16 + 32)
Entry `255`	Produces a log with messages for all types. (255 = 1 + 2 + 4 + 8 + 16 + 32 + 64 +128)

Consider the following example message that is written in the Windows **Event Viewer** Application log:

```
16 4 10797 1 cacao bush nbpem backup of client bush exited with status 71
```

The definition of each value is as follows (left to right):

- Severity = `16` (Error)
- Type = `4` (Backup)
- Job ID = `10797`
- Job group ID = `1`
- Server = `cacao`
- Client = `bush`
- Process = `nbpem`
- Text = `backup of client bush exited with status 71`

Troubleshooting error messages in the NetBackup Administration Console for UNIX

Most error messages in the **NetBackup Administration Console** for UNIX appear in the following locations:

- An attention dialog box
- An error message pane in the lower right area of the console

If the errors appear elsewhere, they are Java exception errors. They may appear in the status line (bottom) of the **NetBackup Administration Console** window. They also may appear in the log file that contains the `stdout` or the `stderr` messages that the Java APIs or the **NetBackup Administration Console** write. Symantec does not document Java exception errors.

Four types of error messages appear in the **NetBackup Administration Console**.

Table 4-16 Error message types

Error type	Description
NetBackup status codes and messages	The operations that are performed in the **NetBackup Administration Console** can result in errors that are recognized in other parts of NetBackup. These errors usually appear exactly as documented in the NetBackup status codes and messages. **Note:** A status code does not always accompany the error message. To find the status code, look up the NetBackup message in the alphabetical listing and click the link to see a full description. See the Status Codes Reference Guide.
NetBackup Administration Console: application server status codes and messages	These messages have status codes in the 500 range. Messages with status codes 500, 501, 502, 503 and 504 begin with `"Unable to login, status:"`. Messages with status codes 511 and 512 may or may not begin with `"Unable to login, status:"`. **Note:** A status code does not always accompany the error message. See the Status Codes Reference Guide.

Table 4-16 Error message types *(continued)*

Error type	Description

Java exceptions	Either the Java APIs or NetBackup Administration APIs generate these exceptions. These messages begin with the name of the exception. For example:
	`java.lang.ClassCastException`
	or
	`vrts.nbu.NBUCommandExecutionException`
	Java exceptions usually appear in one of the following places:
	■ The status line (bottom) of the NetBackup Administration window
	■ The log file that the `jnbSA` or `jbpSA` commands generate
	■ The output file of the Windows Display Console `.bat` file if it is set up
	See "Troubleshooting error messages in the NetBackup Administration Console for UNIX" on page 174.

Operating system errors	Any messages that do not match those in the NetBackup documentation are most likely messages from the operating system.

About extra disk space required for logs and temporary files

For successful operation, the **NetBackup Administration Console** requires extra disk space to store logs and temporary files. The disk space should be available in the following locations.

- On the host that is specified in the logon dialog box
- In `/usr/openv/netbackup/logs/user_ops`
- On the host where the console was started
- In `/usr/openv/netbackup/logs/user_ops/nbjlogs`

If space is not available in the respective file systems, you may experience the following:

- Long waits for application response
- Incomplete data
- No response during logon
- Reduced functionality in the NetBackup interface, for example, only the Backup, Archive, and Restore and Files System Analyzer nodes appear in the tree

- Unexpected error messages:
  - "Cannot connect" socket errors during logon to the NBJava application server
  - "Unable to log in, status: 35 cannot make required directory"
  - "/bin/sh: null: not found (1) "
  - "An exception occurred: vrts.nbu.admin.bpmgmt.CommandOutputException: Invalid or unexpected class configuration data: <*the rest of the message will vary*>"
  - Empty warning dialog boxes

Enabling detailed debug logging

The **NetBackup Administration Console** is a distributed application that allows administration of remote NetBackup servers. All administration is accomplished through the application server of the **NetBackup Administration Console**. This application server is made up of an authentication service and a user service.

The logon request from the logon dialog box is sent to the authentication service for validation. The user name and password have to be valid in the Windows/UNIX authentication files and process.

After validation, the authentication service starts a user service under the user's account. Thereafter, all NetBackup administrative tasks are performed through an instance of the user service. Additional user service processes are initiated to process requests from the console.

On both UNIX and Windows, the authentication service is the `bpjava-msvc` application. The user service is the `bpjava-susvc` or `bpjava-usvc` application. To enable detailed debug logging, you must first create logging directories for these applications.

Table 4-17 Enabling detailed debug logging

Step	Action	Description
Step 1	Create logging directories	On the NetBackup client or server that is specified in the logon dialog box, create the following directories: ■ `bpjava-msvc` ■ `bpjava-susvc` (if a NetBackup server) ■ `bpjava-usvc` (if a NetBackup client) Create the directories in the following locations: ■ `/usr/openv/netbackup/logs` (UNIX) ■ *`install_path`*`\NetBackup\logs` (Windows) See "About unified logging" on page 129. See "About legacy logging" on page 153.
Step 2	Edit the `Debug.properties` file	Add the following line to the `Debug.properties` file: `debugMask=2` The `Debug.properties` file can be found in the following locations: ■ `/usr/openv/java` Change the file on the UNIX machine where you run the `jnbSA` or `jbpSA` commands. The log file name is displayed in the xterm window where you ran the `jnbSA` or `jbpSA` commands. ■ *`install_path`*`\VERITAS\java` Change the file at this location if you use the **NetBackup Java Windows Display Console**.
Step 3	Edit the `nbjava.bat` file	Perform this step if you use the **Windows Display Console** on a host where NetBackup is not installed. Edit the `nbjava.bat` file to redirect output to a file. The `nbjava.bat` file is located in *`install_path`*`\VERITAS\java` See the `nbjava.bat` file for details.

Chapter 5

Backup logging

This chapter includes the following topics:

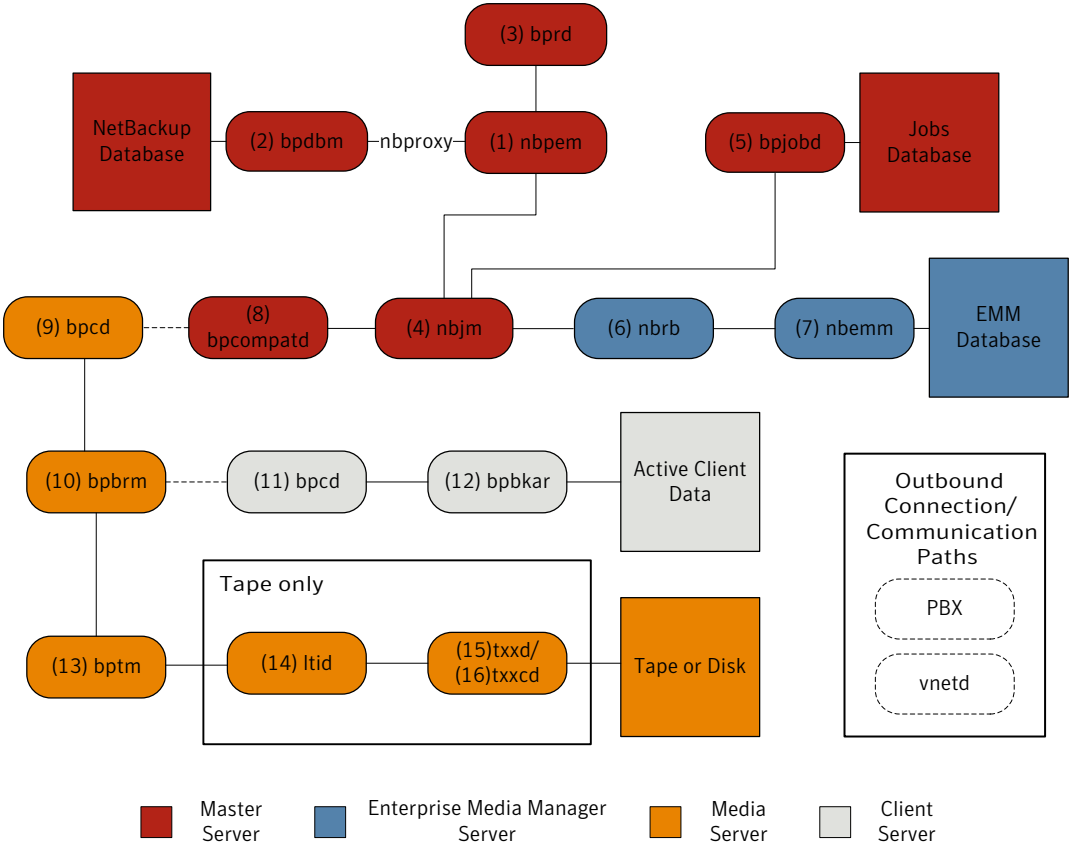
- About backup logging
- Sending backup logs to Symantec Technical Support

About backup logging

A variety of logs exist to help diagnose any issues that occur with backups. Understanding how the backup process works is a helpful first step in deciding which logs to gather for a particular issue.

Figure 5-1 illustrates the backup procedure and the processes involved.

Figure 5-1 Basic backup process flow



Basic backup procedure

1. The (1) NetBackup Policy Execution Manager (`nbpem`) initiates a backup when the job becomes due. To determine when the job is due, `nbpem` uses the proxy service `nbproxy` to get the backup policy information from the (2) NetBackup Database Manager (`bpdbm`).

   In the case of a user-initiated backup, the backup is started when `nbpem` receives a request from the (3) NetBackup request daemon (`bprd`).

2. When the job is due, `nbpem` issues a request to the (4) NetBackup Job Manager (`nbjm`) to submit the backup and get a `jobid`.

3. The nbjm service communicates with (5) bpjobd, and the job is added to the job list in the jobs database. The job is now visible in the Activity Monitor, in a queued state.
4. Once the job has been added to the jobs database, nbjm checks for resources through the (6) NetBackup Resource Broker (nbrb).
5. The nbrb process secures the required resources from the (7) Enterprise Media Manager (nbemm) and notifies nbjm that resources have been allocated.
6. After resource allocation, nbjm makes a call to the images database to create the image files in a temporary location. The required entries in the backup header tables are also created at this time. The job is now seen as “Active” in the Activity Monitor.
7. Once the job is active, nbjm uses (8) bpcompatd to open a connection to the (9) client service (bpcd) on the media server. The bpcompatd service creates the connection through Private Branch Exchange (PBX) and the NetBackup Legacy Network Service (vnetd).
8. The bpcd service starts the (10) NetBackup backup and restore manager (bpbrm).
9. The bpbrm service communicates with (11) bpcd on the client server (through PBX and vnetd) to start the (12) backup and archive manager (bpbkar). The bpbrm service also starts the (13) tape management process (bptm).
10. In the case of a tape backup, bptm reserves the drives and issues a mount request to the (14) logical tape interface daemon (ltid). The ltid service calls on the (15) robotic drive daemon (tx*xx*d, where *xx* varies based on the type of robot being used). The tx*xx*d daemon communicates the mount request to the (16) robotic control daemon (tx*xx*cd), which mounts the media.

    In the case of a disk backup, bptm communicates directly with the disk.
11. The bpbkar service sends the backup data through bptm to be written to the media storage or the disk storage.
12. When the backup is completed, nbjm is notified and sends a message to bpjobd. The job now appears as “Done” in the Activity Monitor. The nbjm service also reports the job exit status to nbpem, which recalculates the next due time of the job.

Each of the processes that is involved in a backup has an accompanying log file. These logs can be consulted to diagnose any issues that you encounter with your backups.

Some additional logs that are not included in the backup process flow but that may be of use in resolving backup problems include: `bpbackup`, `reqlib`, `daemon`, `robots`, and `acsssi`.

If you need assistance, send the logs to Symantec Technical Support.

See "Sending backup logs to Symantec Technical Support" on page 181.

See "nbpem logging" on page 198.

See "nbproxy logging" on page 199.

See "bpdbm logging" on page 194.

See "bprd logging" on page 195.

See "nbjm logging" on page 198.

See "bpjobd logging" on page 195.

See "nbrb logging" on page 199.

See "nbemm logging" on page 198.

See "bpcompatd logging" on page 194.

See "PBX logging" on page 200.

See "vnetd logging" on page 202.

See "bpcd logging" on page 194.

See "bpbrm logging" on page 193.

See "bpbkar logging" on page 193.

See "bptm logging" on page 196.

See "ltid logging" on page 197.

See "txxd and txxcd logging" on page 202.

See "bpbackup logging" on page 192.

See "reqlib logging" on page 200.

See "daemon logging" on page 197.

See "robots logging" on page 201.

See "acsssi logging" on page 192.

Sending backup logs to Symantec Technical Support

If you encounter a problem with a backup, you can send a problem report and the relevant logs to Symantec Technical Support for assistance.

See “Logs to accompany problem reports for synthetic backups” on page 170.

Table 5-1 provides a list of logs and the recommended logging levels that Symantec Technical Support may need to diagnose certain backup issues.

Note: Symantec recommends that the diagnostic level for unified logging be set at the default level of 6.

See “About global logging levels” on page 166.

Table 5-1 Logs to gather for specific backup issues

Type of problem	Logs to gather
Problems with backup scheduling	■ The `nbpem` log at debug level 5 ■ The `nbjm` log at debug level 5 ■ The `nbproxy` log at verbose 4 ■ The `bpdbm` log at verbose 2 ■ The `bprd` log at verbose 5 **Note:** The `bprd` log is only needed for problems with manual or user-initiated backups.
Problems with queued backup jobs that don't go active	■ The `nbpem` log at debug level 3 ■ The `nbjm` log at debug level 5 ■ The `nbrb` log at debug level 4 ■ The `nbproxy` log at verbose 4 ■ The `bpdbm` log at verbose 2 ■ The `nbemm` logs at the default levels ■ The `mds` log at debug level 2 **Note:** The `mds` log writes to the `nbemm` log.

Table 5-1 Logs to gather for specific backup issues *(continued)*

Type of problem	Logs to gather
Problems with active backup jobs that don't write	■ The `nbjm` log at debug level 5 ■ The `nbrb` log at debug level 4 ■ The `bpdbm` log at verbose 2 ■ The `bpbrm` log at verbose 5 ■ The `bptm` log at verbose 5 ■ The `bpcd` log at verbose 5 If the problem is a tape load or unload issue, Support may also need the following logs: ■ The `ltid` log ■ The `reqlib` log ■ The `daemon` log ■ The `robots` log ■ The `acsssi` log (UNIX only)

See "Setting debug logging to a higher level" on page 169.

See "About backup logging" on page 178.

Chapter 6

Restore logging

This chapter includes the following topics:

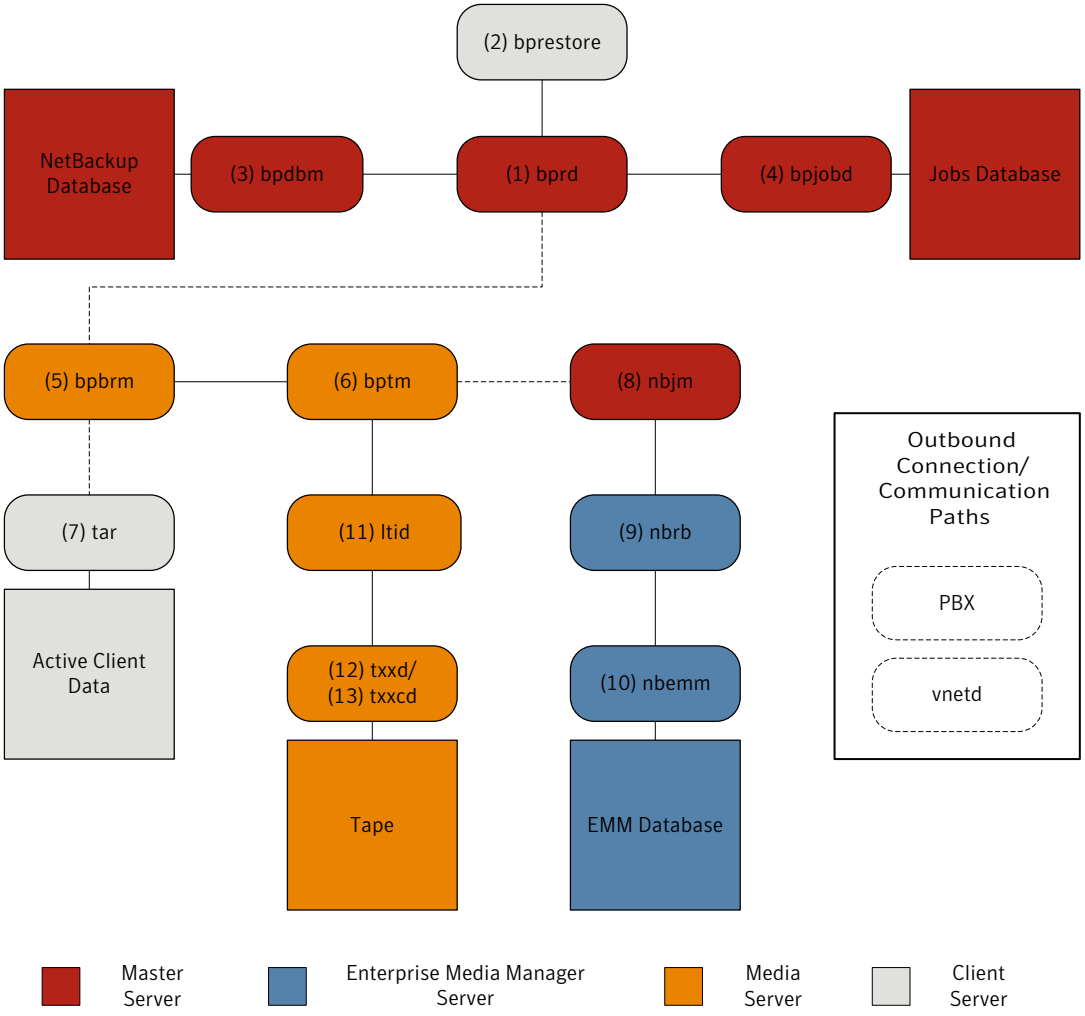
- About restore logging
- Sending restore logs to Symantec Technical Support

About restore logging

A variety of logs exist to help diagnose any issues that occur with restores. Understanding how the restore process works is a helpful first step in deciding which logs to gather for a particular issue. The process differs, depending on whether you restore an image from tape or from disk.

Figure 6-1 illustrates a restore from tape.

Figure 6-1 Restore from tape process flow

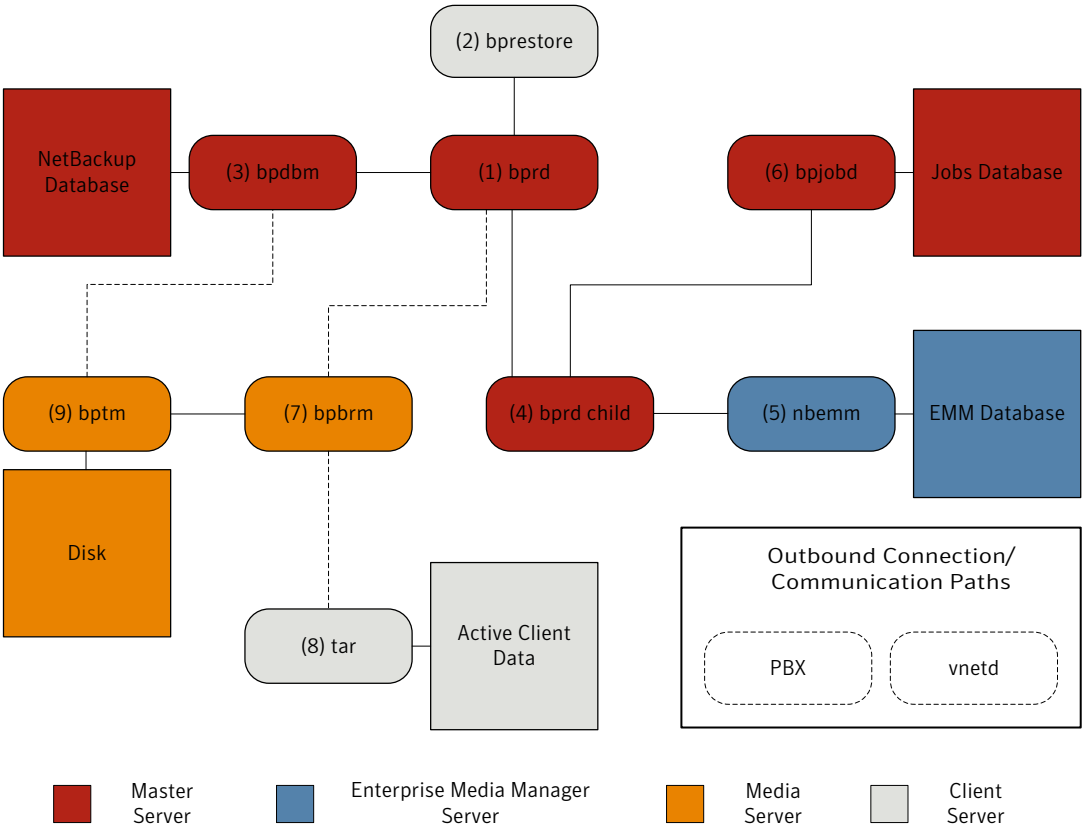


Restore procedure from tape

1. The (1) NetBackup request daemon (bprd) receives a restore request. This request can be initiated from the Backup, Archive, and Restore user interface or from the (2) command line (bprestore).
2. The bprd process launches two child processes: MAIN bprd and MPX-MAIN-bprd. The MAIN bprd process is used to identify images and media, while the MPX-MAIN-bprd process manages the restore operation. For simplicity's sake, these three processes are all referred to here as bprd.
3. The bprd service communicates with the (3) NetBackup Database Manager program (bpdbm) to get the information that is required to restore the files that have been requested.
4. Once it has the information it needs, bprd communicates with (4) bpjobd, and the job is added to the job list in the jobs database. The job is now visible in the Activity Monitor. It may show as "Active" even before resources are acquired.
5. The bprd service goes through Private Branch Exchange (PBX) and the NetBackup Legacy Network (vnetd) to start the (5) NetBackup backup and restore manager (bpbrm).
6. The bpbrm service starts the (6) tape management process (bptm) and provides the media information that is required for the restore. It also starts the (7) Tape Archive program (tar) on the client (through PBX and vnetd) and creates a connection between tar and bptm.
7. The bptm process sends a resource request to the (8) NetBackup Job Manager (nbjm) through PBX and vnetd.
8. The nbjm process sends the resource request to the (9) NetBackup Resource Broker (nbrb), which queries the (10) Enterprise Media Manager (nbemm). Once the resources have been allocated, nbrb notifies nbjm, which notifies bptm.
9. The bptm process makes a mount request to the (11) logical tape interface daemon (ltid). The ltid service calls on the (12) robotic drive daemon (tx*x*d, where *xx* varies based on the type of robot being used). The tx*x*d daemon communicates the mount request to the (13) robotic control daemon (tx*x*cd), which mounts the media.
10. The bptm process reads the data to be restored from the media and delivers it to tar.
11. The tar process writes the data to the client disk.
12. When the restore is completed, bptm unmounts the media and notifies nbjm. The job now appears as "Done" in the Activity Monitor.

Figure 6-2 illustrates a restore from disk.

Figure 6-2 Restore from disk process flow



Restore procedure from disk

1. The (1) NetBackup request daemon (`bprd`) receives a restore request. This request can be initiated from the Backup, Archive, and Restore user interface or from the (2) command line (`bprestore`).
2. The `bprd` process contacts the (3) NetBackup Database Manager program (`bpdbm`) to identify the files, the client, and the media information for the restore.
3. The `bprd` process initiates a (4) child `bprd` process. The child `bprd` process makes a call to the (5) Enterprise Media Manager (`nbemm`) to verify that the disk storage unit is available.

4 The child bprd process communicates with (6) bpjobd to allocate a jobid. The restore job is now visible in the Activity Monitor.

5 The bprd process starts the (7) NetBackup backup and restore manager (bpbrm) on the media server, through Private Branch Exchange (PBX) and the NetBackup Legacy Network Service (vnetd).

6 The bpbrm service uses PBX and vnetd to establish a connection with the (8) Tape Archive program (tar) on the client system. It also starts the (9) tape management process (bptm).

7 The bptm process makes a call to bpdbm (through PBX and vnetd) to get the fragment information and then mounts the disk.

8 The bptm process reads the backup image from the disk and streams the requested data to tar.

9 The tar process commits the data to the storage destination.

Each of the processes that is involved in a restore has an accompanying log file. These logs can be consulted to diagnose any issues that you encounter with your restore.

Some additional logs that are not included in the restore process flows but that may be of use in resolving restore problems include: reqlib, daemon, robots, and acsssi.

If you need assistance, send the logs to Symantec Technical Support.

See "Sending restore logs to Symantec Technical Support" on page 189.

See "bprd logging" on page 195.

See "bprestore logging" on page 196.

See "PBX logging" on page 200.

See "vnetd logging" on page 202.

See "bpdbm logging" on page 194.

See "bpjobd logging" on page 195.

See "bpbrm logging" on page 193.

See "bptm logging" on page 196.

See "tar logging" on page 201.

See "nbjm logging" on page 198.

See "nbrb logging" on page 199.

See "nbemm logging" on page 198.

See “ltid logging” on page 197.

See “reqlib logging” on page 200.

See “robots logging” on page 201.

See “acsssi logging” on page 192.

Sending restore logs to Symantec Technical Support

If you encounter a problem with a restore, you can send a problem report and the relevant logs to Symantec Technical Support for assistance.

See “Logs to accompany problem reports for synthetic backups” on page 170.

Table 6-1 provides a list of logs and the recommended logging levels that Symantec Technical Support may need to diagnose certain restore issues.

Note: Symantec recommends that the diagnostic level for unified logging be set at the default level of 6.

See “About global logging levels” on page 166.

Table 6-1 Log to gather for specific restore issues

Type of problem	Log to gather
Problems with restore jobs from tape	■ The `nbjm` log at debug level 5 ■ The `nbemm` log at debug level 1 ■ The `nbrb` log at debug level 4 ■ The `bpdbm` log at verbose 1 ■ The `bprd` log at verbose 5 ■ The `bpbrm` log at verbose 5 ■ The `bptm` log at verbose 5 ■ The `tar` log at verbose 5 ■ The `bpcd` log at verbose 5 If the problem is a media or a drive issue, Support may also need the following logs: ■ The `reqlib` log ■ The `daemon` log ■ The `robots` log ■ The `acsssi` log (UNIX only)

Table 6-1 Log to gather for specific restore issues *(continued)*

Type of problem	Log to gather
Problems with restore jobs from disk	■ The `bpdbm` log at verbose 1 ■ The `bprd` log at verbose 5 ■ The `bpbrm` log at verbose 5 ■ The `bptm` log at verbose 5 ■ The `bpdm` log at verbose 5 ■ The `tar` log at verbose 5 ■ The `bpcd` log at verbose 5

See "Setting debug logging to a higher level" on page 169.

See "About restore logging" on page 184.

Chapter 7

Locating logs

This chapter includes the following topics:

- acsssi logging
- bpbackup logging
- bpbkar logging
- bpbrm logging
- bpcd logging
- bpcompatd logging
- bpdbm logging
- bpjobd logging
- bprd logging
- bprestore logging
- bptm logging
- daemon logging
- ltid logging
- nbemm logging
- nbjm logging
- nbpem logging
- nbproxy logging
- nbrb logging

- PBX logging
- reqlib logging
- robots logging
- tar logging
- txxd and txxcd logging
- vnetd logging

acsssi logging

On UNIX systems, the NetBackup ACS storage server interface (`acsssi`) communicates with the ACS library software host.

Log location	UNIX: `/usr/openv/volmgr/debug/acsssi`
Server where it resides	media
How to access	The `acsssi` process uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See "About legacy logging" on page 153.

See "About backup logging" on page 178.

See "About restore logging" on page 184.

bpbackup logging

The `bpbackup` command-line executable is used to initiate user backups.

Log location	Windows: *`install_path`*`\NetBackup\logs\bpbackup` UNIX: `/usr/openv/netbackup/logs/bpbackup`
Server where it resides	client
How to access	The `bpbackup` process uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See "About legacy logging" on page 153.

See “About backup logging” on page 178.

bpbkar logging

The backup and archive manager (`bpbkar`) is used to read client data, which is sent to the media server to write to the storage media. It also collects metadata about the files that have been backed up to create the `files` file.

Log location	Windows: *`install_path`*`\NetBackup\logs\bpbkar` UNIX: `/usr/openv/netbackup/logs/bpbkar`
Server where it resides	client
How to access	The `bpbkar` process uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See “About legacy logging” on page 153.

See “About backup logging” on page 178.

bpbrm logging

The NetBackup backup and restore manager (`bpbrm`) manages the client and `bptm` process. It also uses the error status from the client and from `bptm` to determine the final status of backup and restore operations.

Log location	Windows: *`install_path`*`\NetBackup\logs\bpbrm` UNIX: `/usr/openv/netbackup/logs/bpbrm`
Server where it resides	media
How to access	The `bpbrm` process uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See “About legacy logging” on page 153.

See “About backup logging” on page 178.

See “About restore logging” on page 184.

bpcd logging

The NetBackup client service (bpcd) authenticates remote hosts and launches processes on local hosts.

Log location	Windows: *install_path*\NetBackup\logs\bpcd UNIX: /usr/openv/netbackup/logs/bpcd
Server where it resides	media and client
How to access	The bpcd process uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See "About legacy logging" on page 153.

See "About backup logging" on page 178.

bpcompatd logging

The NetBackup compatibility service (bpcompatd) creates connections between some multi-threaded processes and NetBackup legacy processes.

Log location	Windows: *install_path*\NetBackup\logs\bpcompatd UNIX: /usr/openv/netbackup/logs/bpcompatd
Server where it resides	master
How to access	The bpcompatd process uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See "About legacy logging" on page 153.

See "About backup logging" on page 178.

bpdbm logging

The NetBackup Database Manager (bpdbm) manages the configuration, error, and file databases.

Log location	Windows: *install_path*\NetBackup\logs\bpdbm UNIX: /usr/openv/netbackup/logs/bpdbm
Server where it resides	master
How to access	The bpdbm process uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See "About legacy logging" on page 153.

See "About backup logging" on page 178.

See "About restore logging" on page 184.

bpjobd logging

The bpjobd service manages the jobs database and relays job statuses to the Activity Monitor.

Log location	Windows: *install_path*\NetBackup\logs\bpjobd UNIX: /usr/openv/netbackup/logs/bpjobd
Server where it resides	master
How to access	The bpjobd process uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See "About legacy logging" on page 153.

See "About backup logging" on page 178.

See "About restore logging" on page 184.

bprd logging

The NetBackup request daemon (bprd) responds to client and administrative requests for backups, restores, and archives.

Log location	Windows: *install_path*\NetBackup\logs\bprd UNIX: /usr/openv/netbackup/logs/bprd
Server where it resides	master

How to access	The `bprd` process uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See "About legacy logging" on page 153.

See "About backup logging" on page 178.

See "About restore logging" on page 184.

bprestore logging

The `bprestore` command-line executable is used to initiate restores. It communicates with `bprd` on the master server.

Log location	Windows: *install_path*\NetBackup\logs\bprestore UNIX: `/usr/openv/netbackup/logs/bprestore`
Server where it resides	client
How to access	The `bprestore` process uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See "About legacy logging" on page 153.

See "About restore logging" on page 184.

bptm logging

The NetBackup tape management process (`bptm`) manages the transfer of backup images between the client and the storage device (tape or disk).

Log location	Windows: *`install_path`*`\NetBackup\logs\bptm` UNIX: `/usr/openv/netbackup/logs/bptm`
Server where it resides	media
How to access	The `bptm` process uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See "About legacy logging" on page 153.

See “About backup logging” on page 178.

See “About restore logging” on page 184.

daemon logging

The `daemon` log includes debug information for the Volume Manager service (`vmd`) and its associated processes.

Log location	Windows: *`install_path`*`\volmgr\debug\daemon` UNIX: `/usr/openv/volmgr/debug/daemon`
Server where it resides	master and media
How to access	The `daemon` log uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See “About legacy logging” on page 153.

See “About backup logging” on page 178.

See “About restore logging” on page 184.

ltid logging

The logical tape interface daemon (`ltid`), also called the NetBackup Device Manager, controls the reservation and assignment of tapes and optical disks.

Log location	Windows: *`install_path`*`\volmgr\debug\ltid` UNIX: `/usr/openv/volmgr/debug/ltid`
Server where it resides	media
How to access	The `ltid` process uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See “About legacy logging” on page 153.

See “About backup logging” on page 178.

See “About restore logging” on page 184.

nbemm logging

On the server that is defined as the EMM server, the NetBackup Enterprise Media Manager (nbemm) manages devices, media, and storage unit configuration. It also performs resource selection.

Log location	Windows: *install_path*\NetBackup\logs\nbemm UNIX: /usr/openv/logs/nbemm
Server where it resides	master
How to access	The nbemm process uses the unified logging method. Use the vxlogview and vxlogmgr commands to view and manage the unified log files. See "About unified logging" on page 129.

See "About backup logging" on page 178.

See "About restore logging" on page 184.

nbjm logging

The NetBackup Job Manager (nbjm) accepts job requests from nbpem and from media commands, and it acquires the necessary resources for the jobs.

Log location	Windows: *install_path*\NetBackup\logs\nbjm UNIX: /usr/openv/logs/nbjm
Server where it resides	master
How to access	The nbjm process uses the unified logging method. Use the vxlogview and vxlogmgr commands to view and manage the unified log files. See "About unified logging" on page 129.

See "About backup logging" on page 178.

See "About restore logging" on page 184.

nbpem logging

The NetBackup Policy Execution Manager (nbpem) creates policy and client tasks and determines when jobs are run.

Log location	Windows: *install_path*\NetBackup\logs\nbpem UNIX: /usr/openv/logs/nbpem
Server where it resides	master
How to access	The nbpem process uses the unified logging method. Use the vxlogview and vxlogmgr commands to view and manage the unified log files. See "About unified logging" on page 129.

See "About backup logging" on page 178.

nbproxy logging

The proxy service nbproxy enables nbpem and nbjm to query master server catalogs.

Log location	Windows: *install_path*\NetBackup\logs\nbproxy UNIX: /usr/openv/netbackup/logs/nbproxy
Server where it resides	master
How to access	The nbproxy process uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See "About legacy logging" on page 153.

See "About backup logging" on page 178.

nbrb logging

On the server that is defined as the EMM server, the NetBackup Resource Broker (nbrb) locates storage units, tape drives, and client reservations for jobs. Then it starts the jobs. It works with nbemm.

Log location	Windows: *install_path*\NetBackup\logs\nbrb UNIX: /usr/openv/logs/nbrb
Server where it resides	master

How to access	The `nbrb` process uses the unified logging method. Use the `vxlogview` and `vxlogmgr` commands to view and manage the unified log files. See "About unified logging" on page 129.

See "About backup logging" on page 178.

See "About restore logging" on page 184.

PBX logging

Private Branch Exchange (`PBX`) is the communication mechanism used by most NetBackup processes.

Log location	Windows: *install_path*`\VxPBX\log` UNIX: `/opt/VRTSpbx/log`
Server where it resides	master, media, and client
How to access	The `PBX` process uses the unified logging method. Use the `vxlogview` and `vxlogmgr` commands to view and manage the unified log files. Note that the `PBX` product ID used to access the unified log files differs from the NetBackup product ID. The `PBX` product ID is 50936. See "About unified logging" on page 129.

See "Accessing the PBX logs" on page 76.

See "About backup logging" on page 178.

See "About restore logging" on page 184.

reqlib logging

The `reqlib` log includes debug information on the processes that request media management services from EMM or the Volume Manager service (`vmd`).

Log location	Windows: *install_path*`\volmgr\debug\reqlib` UNIX: `/usr/openv/volmgr/debug/reqlib`
Server where it resides	master and media

How to access	The `reqlib` log uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See "About legacy logging" on page 153.

See "About backup logging" on page 178.

See "About restore logging" on page 184.

robots logging

The `robots` log includes debug information on all robotic daemons, including the `txxd` and `txxcd` daemons.

Log location	Windows: *`install_path`*`\volmgr\debug\robots` UNIX: `/usr/openv/volmgr/debug/robots`
Server where it resides	media
How to access	The `robots` log uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See "About legacy logging" on page 153.

See "txxd and txxcd logging" on page 202.

See "About backup logging" on page 178.

See "About restore logging" on page 184.

tar logging

The Tape Archive program (`tar`) writes restore data to the client disk.

Log location	Windows: *install_path*\NetBackup\logs\tar UNIX: `/usr/openv/netbackup/logs/tar`
Server where it resides	client
How to access	The `tar` process uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See "About legacy logging" on page 153.

See “About restore logging” on page 184.

txxd and txxcd logging

The robotic daemon (`txxd`, where *xx* varies based on the type of robot being used) provides the interface between `ltid` and the tape library. The robotic control daemon (`txxcd`) provides the robotic control for the robot and communicates mount and unmount requests.

Log location	The `txxd` and `txxcd` processes do not have their own log files. Instead, errors are logged in the `robots` debug log and the system log. The system log is managed by `syslog` on UNIX and by the Event Viewer on Windows. See “About UNIX system logs” on page 129. See “Logging options with the Windows Event Viewer” on page 171.
How to access	Debug information is included by adding the word `VERBOSE` to the `vm.conf` file. See “How to control the amount of information written to legacy logging files” on page 162. On UNIX, debug information is also included by starting the daemon with the `-v` option (either by itself or through `ltid`).

See “robots logging” on page 201.

See “About backup logging” on page 178.

See “About restore logging” on page 184.

vnetd logging

The NetBackup Legacy Network Service (`vnetd`) is a communication mechanism used to create firewall-friendly socket connections.

Log location	Windows: *`install_path`*`\NetBackup\logs\vnetd` UNIX: `/usr/openv/logs/vnetd` or `/usr/openv/netbackup/logs/vnetd` if the `vnetd` directory exists there. If the `vnetd` directory exists in both locations, logging occurs only in `/usr/openv/netbackup/logs/vnetd`.

Server where it resides	master, media, and client
How to access	The `vnetd` process uses the legacy logging method. If legacy debug logging is not enabled on your NetBackup servers, you must create the appropriate directories for each process. See "About legacy logging" on page 153.

See "About backup logging" on page 178.

See "About restore logging" on page 184.

Chapter 8

Disaster recovery

This chapter includes the following topics:

- About disaster recovery
- Recommended backup practices
- About disk recovery procedures for UNIX and Linux
- About clustered NBU server recovery for UNIX and Linux
- About disk recovery procedures for Windows
- About clustered NBU server recovery for Windows
- About recovering the NetBackup catalog

About disaster recovery

Data backup is essential to any data protection strategy, especially a strategy that is expected to assist in disaster recovery. Regularly backing up data and therefore being able to restore that data within a specified time frame are important components of recovery. Regardless of any other recovery provisions, backup protects against data loss from complete system failure. And off-site storage of backup images protects against damage to your on-site media or against a disaster that damages or destroys your facility or site.

To perform recovery successfully, the data must be tracked. Knowing at what point in time the data was backed up allows your organization to assess the information that cannot be recovered. Configure your data backup schedules to allow your organization to achieve its recovery point objective (RPO). The RPO is the point in time before which you cannot accept lost data. If your organization can accept one day's data loss, your backup schedule should be at least daily. That way you can achieve an RPO of one day before any disaster.

Your organization also may have a recovery time objective (RTO), which is the expected recovery time or how long it takes to recover. Recovery time is a function of the type of disaster and of the methods that are used for recovery. You may have multiple RTOs, depending on which services your organization must recover when.

High availability technologies can make the recovery point very close or even identical to the point of failure or disaster. They also can provide very short recovery times. However, the closer your RTO and RPO are to the failure point, the more expensive it is to build and maintain the systems that are required to achieve recovery. Your analysis of the costs and benefits of various recovery strategies should be part of your organization's recovery planning.

Effective disaster recovery requires procedures specific to an environment. These procedures provide detailed information regarding preparation for and recovering from a disaster. Use the disaster recovery information in this chapter as a model only; evaluate and then develop your own disaster recovery plans and procedures.

Warning: Before you try any of the disaster recovery procedures in this chapter, Symantec recommends that you contact technical support.

This topic provides information about NetBackup installation and (if necessary), catalog recovery after a system disk failure. Symantec assumes that you recover to the original system disk or one configured exactly like it.

Warning: NetBackup may not function properly if you reinstall and recover to a different partition or to one that is partitioned differently due to internal configuration information. Instead, configure a replacement disk with partitioning that is identical to the failed disk. Then reinstall NetBackup on the same partition on which it was originally installed.

The specific procedures that replace failed disks, build partitions and logical volumes, and reinstall operating systems can be complicated and time consuming. Such procedures are beyond the scope of this manual. Appropriate vendor-specific information should be referenced.

Recommended backup practices

The following backup practices are recommended:

Selecting files to back up	In addition to backing up files on a regular basis, it is important to select the correct files to back up. Include all files with records that are critical to users and the organization. Back up system and application files, so you can quickly and accurately restore a system to normal operation if a disaster occurs. Include all Windows system files in your backups. In addition to the other system software, the Windows system directories include the registry, which is needed to restore the client to its original configuration. If you use a NetBackup exclude list for a client, do not specify any Windows system files in that list. Do not omit executables and other application files. You may want to save tape by excluding these easy-to-reinstall files. However, backing up the entire application ensures that it is restored to its exact configuration. For example, if you have applied software updates and patches, restoring from a backup eliminates the need to reapply them.
Bare Metal Restore	NetBackup Bare Metal Restore (BMR) protects client systems by backing them up with a policy configured for BMR protection. A complete description of BMR backup and recovery procedures is available. See the *NetBackup Bare Metal Restore Administrator's Guide*.
Critical policies	When you configure a policy for online catalog backup, designate certain NetBackup policies as critical. Critical policies back up systems and data deemed critical to end-user operation. During a catalog recovery, NetBackup verifies that all of the media that is needed to restore critical policies are available.
Full backup after catalog recovery	If the configuration contains Windows clients that have incremental backup configurations set to **Perform Incrementals Based on Archive Bit**, run a full backup of these clients as soon as possible after a catalog recovery. The archive bit resets on the files that were incrementally backed up after the catalog backup that was used for the catalog recovery. If a full backup of these clients is not run after a catalog recovery, these files could be skipped and not backed up by subsequent incremental backups.
Online catalog backups	Online, hot catalog backup is a policy-driven backup that supports tape-spanning and incremental backups. It allows for restoring catalog files from the Backup, Archive, and Restore interface. Online catalog backups may be run while other NetBackup activity occurs, which provides improved support for environments in which continual backup activity is typical.
Online catalog backup disaster recovery files	Symantec recommends saving the disaster recovery files that are created by the online catalog backup to a network share or removable device. Do not save the disaster recovery files to the local computer. Catalog recovery from an online catalog backup without the disaster recovery image file is a more complex procedure and time-consuming procedure.

Automated recovery	The catalog disaster recovery file (created during an online catalog backup) is intended to automate the process of NetBackup recovery. If you recover a system other than the one that originally made the backups, it should be identical to the original system. For example, the system that performs the recovery should include NetBackup servers with identical names to those servers where the backups were made. If not, the automated recovery may not succeed.
Online catalog disaster recovery information email	Configure the online catalog backup policy to email a copy of the disaster recovery information to a NetBackup administrator in your organization. Configure this policy as part of every catalog backup. Do not save the disaster recovery information emails to the local computer. Catalog recovery without the disaster recovery image file or the disaster recovery information email available is exceedingly complex, time consuming, and requires assistance. You may tailor the disaster recovery email process by using the `mail_dr_info` notify scrpt. More details are available. Seethe *NetBackup Administrator's Guide, Volume II*.
Identifying the correct catalog backup	Ensure that you identify and use the appropriate catalog backup for your recovery. For example, if you recover from your most recent backups, use the catalog from your most recent backups. Similarly, if you recover from a specific point in time, use the catalog backup from that specific point in time.
Catalog recovery time	System environment, catalog size, location, and backup configuration (full and incremental policy schedules) all help determine the time that is required to recover the catalog. Carefully plan and test to determine the catalog backup methods that result in the desired catalog recovery time.
Master and media server backups	The NetBackup catalog backup protects your configuration data and catalog data. Set up backup schedules for the master servers and media servers in your NetBackup installation. These schedules protect the operating systems, device configurations, and other applications on the servers. Master or media server recovery procedures when the system disk has been lost assume that the servers are backed up separately from the catalog backup. Backups of master and media servers should not include NetBackup binaries, configuration or catalog files, or relational database data.

About disk recovery procedures for UNIX and Linux

The three different types of disk recovery for UNIX and Linux are as follows:

- Master server disk recovery procedures
  See "Recovering the master server disk for UNIX and Linux" on page 208.
- Media server disk recovery procedures
  See "About recovering the NetBackup media server disk for UNIX" on page 213.

- Client disk recovery procedures
  See "Recovering the system disk on a UNIX client workstation" on page 213.

The disk-based images that reside on AdvancedDisk or on OpenStorage disks cannot be recovered by means of the NetBackup catalog. These disk images must be recovered by means of the NetBackup import feature. For information on import,

See the topic on importing NetBackup images in the *NetBackup Administrator's Guide, Volume I*.

When the disk image is imported, NetBackup does not recover the original catalog entry for the image. Instead, a new catalog entry is created.

Recovering the master server disk for UNIX and Linux

Two procedures explain how to recover data if the system disk fails on a UNIX or Linux NetBackup master server, as follows:

- The root file system is intact. The operating system, NetBackup software and some (if not all) other files are assumed to be lost.
  See "Recovering the master server when root is intact" on page 208.
- The root file system is lost along with everything else on the disk. This situation requires a total recovery. This recovery reloads the operating system to an alternate boot disk and boots from this disk during recovery. This operation lets you recover the root partition without risking a crash that is caused by overwriting the files that the operating system uses during the restore.
  See "Recovering the master server when the root partition is lost" on page 210.

For NetBackup master and media servers, the directory locations of the NetBackup catalog become an integral part of NetBackup catalog backups. Any recovery of the NetBackup catalog requires identical directory paths or locations be created during the NetBackup software reinstallation. Disk partitioning, symbolic links, and NetBackup catalog relocation utilities may be needed.

NetBackup Bare Metal Restore (BMR) protects client systems by backing them up with a policy configured for BMR protection. Information is available that describes BMR backup and recovery procedures.

See the *NetBackup Bare Metal Restore System Administrator's Guide*.

Recovering the master server when root is intact

The following procedure recovers the master server by reloading the operating system, restoring NetBackup, and then restoring all other files.

To recover the master server when root is intact

1. Verify that the operating system works, that any require patches are installed, and that specific configuration settings are made. Take corrective action as needed.
2. Reinstall NetBackup software on the server you want to recover.

   See the *NetBackup Installation Guide for UNIX* for instructions.
3. Install any NetBackup patches that had been previously installed. See the documentation that was included with the patch software.

   Note: Symantec does not support the recovery of a catalog image that was backed up using an earlier version of NetBackup.
4. If any of the default catalog directories have changed that may be reflected in the NetBackup catalog backups, recreate those directories before the catalog recovery.

   The following are examples:

   - Use of symbolic links as part of the NetBackup catalog directory structure.
   - Use of the NetBackup `nbdb_move` command to relocate parts of the NetBackup relational database catalog.
5. If the recovery scenario involves restoring policy or catalog backups, the appropriate recovery device(s) must be configured, which may involve the following tasks:

   - Install and configure the robotic software for the devices that read backups of the NetBackup catalog and regular backups of the disk being restored. If a non-robotic drive is available that can read these backups, then no robot is required. Although manual intervention is required if multiple pieces of media are required.
     See the *NetBackup Device Configuration Guide*.
   - Use the NetBackup **Device Configuration** Wizard to discover and configure the recovery device in NetBackup.
     See the *NetBackup Administrator's Guide, Volume I*.
   - Use the NetBackup command `tpautoconf` to discover and configure the recovery device in NetBackup.
     See the *NetBackup Commands Reference Guide*.
   - Update the device mapping files.
     See the *NetBackup Administrator's Guide, Volume I*.

6 If you must restore from the policy backups or catalog backups that were done to media, the appropriate media may have to be configured in NetBackup.

See the *NetBackup Administrator's Guide, Volume I*.

Configuring the media may require some or all of the following tasks:

- Manually load the required media into a stand-alone recovery device.
- Use the NetBackup utilities such as `robtest` or vendor-specific robotic control software to load media into the required recovery device or devices.
- Use the NetBackup Volume Configuration Wizard to inventory the media contents of a robotic device.
- Use the vendor-specific robotic control software to load the media into the required recovery device(s).

7 Recover the NetBackup catalogs to the server you are recovering.

The NetBackup catalogs can be recovered only to the same directory structure from which they were backed up (alternate path recovery is not allowed).

8 Stop and restart all NetBackup daemons. Use the following NetBackup commands, or use the **Activity Monitor** in the NetBackup Administration Console.

```
/usr/openv/netbackup/bin/bp.kill_all
/usr/openv/netbackup/bin/bp.start_all
```

9 Start the NetBackup Backup, Archive, and Restore interface (or the `bp` command) and restore other files to the server as desired. When the files are restored, you are done.

Recovering the master server when the root partition is lost

The following procedure assumes that the root file system is lost along with everything else on the disk. This procedure reloads the operating system to an alternate boot disk and boots from that disk during recovery. This operation lets you recover the root partition without risking a crash that is caused by overwriting the files that the operating system uses during the restore.

To recover the master server when the root partition is lost

1 Load the operating system on an alternate boot disk, using the same procedure as you would normally use for the server type.

2 On the alternate disk, create the partition and directory where NetBackup, its catalogs (if applicable), and databases resided on the original disk. By default, they reside under the `/usr/openv` directory.

3 Verify that the operating system works, that any required patches are installed, and that specific configuration settings are made. Take corrective action as needed.

4 Install NetBackup on the alternate disk. Install only the robotic software for the devices that are required to read backups of the NetBackup catalogs and regular backups of the disk being restored. If a non-robotic drive can read these backups, no robot is required.

5 Install any NetBackup patches that had been previously installed. See the documentation that was included with the patch software.

6 If the catalog directories differ from those in the NetBackup catalog backups, recreate that directory structure on disk before you recover the catalog.

Examples of those directories are the following:

- Use of symbolic links as part of the NetBackup catalog directory structure.
- Use of the NetBackup `nbdb_move` command to relocate parts of the NetBackup relational database catalog.

7 If the recovery scenario involves restoring policy or catalog backups, the appropriate recovery device(s) must be configured.

Device configuration may include the following tasks:

- Install and configure the robotic software for the devices that read backups of the NetBackup catalog and regular backups of the disk being restored. If a non-robotic drive is available that can read these backups, then no robot is required. Although manual intervention is required if multiple pieces of media are required.
  See the *NetBackup Device Configuration Guide*.
- Use the NetBackup **Device Configuration** Wizard to discover and configure the recovery device in NetBackup.
  See the *NetBackup Administrator's Guide, Volume I*.
- Use the NetBackup command `tpautoconf` to discover and configure the recovery device in NetBackup.
  See the *NetBackup Commands Reference Guide* manual.
- Update the device mapping files.
  See the *NetBackup Administrator's Guide, Volume I*.

8 If you must restore from the policy backups or catalog backups that were done to media, the appropriate media may have to be configured in NetBackup.

See the *NetBackup Administrator's Guide, Volume I*.

Configuring the media may require some or all of the following tasks:

- Manually load the required media into a stand-alone recovery device.
- Use the NetBackup utilities such as `robtest` or vendor-specific robotic control software to load media into the required recovery device or devices.
- Use the NetBackup Volume Configuration Wizard to inventory the media contents of a robotic device.
- Use the vendor-specific robotic control software to load the media into the required recovery device(s).

9 Recover the NetBackup catalogs to the alternate disk.

See "About recovering the NetBackup catalog" on page 228.

The catalogs can be recovered only to the same directory structure from which they were backed up (alternate path recovery is not allowed).

10 Start the NetBackup Backup, Archive, and Restore interface (or the `bp` command). Restore the latest backed up version of all files.

You restore these files from the backup of the master server, not from the NetBackup catalog backup. Be sure to specify the disk that you recover as the alternate recovery location.

Warning: Do not restore files to the `/usr/openv/var`, `/usr/openv/db/data`, or `/usr/openv/volmgr/database` directories (or relocated locations) or the directories that contain NetBackup database data. This data was recovered to the alternate disk in step 9 and is copied back to the recovery disk in step 12.

---

11 Stop all NetBackup processes that you started from NetBackup on the alternate disk. Use the **Activity Monitor** in the NetBackup Administration Console or the following:

```
/usr/openv/netbackup/bin/bp.kill_all
```

12 Maintaining the same directory structure, copy the NetBackup catalogs from the alternate disk to the disk that you recover. These are the catalogs recovered in step 9.

13 Make the recovered disk the boot disk again and restart the system.

14 Start and test the copy of NetBackup on the disk that you have recovered.

```
/usr/openv/netbackup/bin/bp.start_all
```

Try the NetBackup Administration utilities. Also, try some backups and restores.

15 When you are satisfied that the recovery is complete, delete the NetBackup files from the alternate disk. Or, unhook that disk, if it is a spare.

About recovering the NetBackup media server disk for UNIX

NetBackup 6.0 and later media servers store information in the NetBackup relational database. If you need to recover the system disk on a NetBackup media server, the recommended procedure is similar to disk recovery for the client.

See "Recovering the system disk on a UNIX client workstation" on page 213.

Recovering the system disk on a UNIX client workstation

The following procedure recovers the client by reloading the operating system, installing NetBackup client software, and then restoring all other files. The procedure assumes that the host name does not change.

To recover the system disk on a client workstation

1 Install the operating system as you normally would for a client workstation of that type.

2 Install NetBackup client software and patches.

3 Use the NetBackup Backup, Archive, and Restore interface to select and restore user files.

About clustered NBU server recovery for UNIX and Linux

NetBackup server clusters do not protect against catalog corruption, loss of the shared disk, or loss of the whole cluster. Regular catalog backups must be performed. More information is available about configuring catalog backups and system backup policies in a clustered environment.

See the *NetBackup High Availability Guide*.

The following table describes the failure scenarios and points to the recovery procedures.

Warning: Before attempting any of the recovery procedures in this topic, contact technical support.

Table 8-1 Cluster failure and recovery scenarios

Scenario	Procedure
Node failure	See "Replacing a failed node on a UNIX or Linux cluster" on page 214.
Shared disk failure	See "Recovering the entire UNIX or Linux cluster" on page 215.
Cluster failure	See "Recovering the entire UNIX or Linux cluster" on page 215.

Replacing a failed node on a UNIX or Linux cluster

Cluster technology-specific information is available about how to bring the NetBackup resource group online and offline. Also, information about how to freeze and unfreeze (that is, disable and enable monitoring for) the NetBackup Resource group.

Refer to topics about configuring NetBackup in the *NetBackup High Availability Guide*.

The following procedure applies when the shared disk and at least one configured cluster node remain available.

To replace a failed node on a UNIX or Linux cluster

1. Configure the hardware, system software, and cluster environment on the replacement node.
2. Verify that the device configuration matches that of the surviving nodes.
3. Ensure that the NetBackup Resource group is offline on all nodes before installing NetBackup on the replacement node.
4. Ensure that the NetBackup shared disks are not mounted on the node on which NetBackup is to be installed.
5. Freeze the NetBackup service.
6. Reinstall NetBackup on the new mode or replacement node. Be sure to use the NetBackup Virtual Name as the name of the NetBackup server. Follow the instructions for installing the NetBackup server software.

   Refer to the *NetBackup Installation Guide*.
7. Install any Maintenance Packs and patches that are required to bring the newly installed node to the same patch level as the other cluster nodes.

8 Bring the NetBackup Resource group online on a node other than the freshly installed node.

9 Log onto the node on which the NetBackup resource group is online and run the following command:

```
/usr/openv/netbackup/bin/cluster/cluster_config -s nbu -o
add_node -n node_name
```

node_name is the name of the freshly installed node.

10 Switch the NetBackup resource group to the replacement node.

11 Freeze the NetBackup group.

12 Ensure that the appropriate low-level tape device and robotic control device configuration necessary for your operating system has been performed. Information is available for your operating system.

Refer to the *NetBackup Device Configuration Guide*.

13 Run the **Device Configuration Wizard** to configure the devices. You do not have to rerun the device configuration on the pre-existing nodes. Configuration information on your particular cluster is available.

See the *NetBackup Administrator's Guide, Volume I*.

14 Check that the robot numbers and robot drive numbers for each robot are consistent across all nodes of the cluster. Repeat for any other servers that are connected to that robot and correct if necessary.

See the *NetBackup Administrator's Guide , Volume 1*.

15 Test the ability of NetBackup to perform restores using the configured devices on the replacement node.

16 Unfreeze the NetBackup resource group.

Recovering the entire UNIX or Linux cluster

The following procedure applies to the clustered NetBackup server environment that must be re-created from scratch.

Before you proceed, ensure that you have valid online catalog backups.

To recover the entire UNIX or Linux cluster

1. Configure the hardware, system software, and cluster environment on the replacement cluster.
2. Ensure that the appropriate low-level tape device and robotic control device configuration necessary for your operating system has been performed.

   Refer to the *NetBackup Device Configuration Guide*.
3. Reinstall NetBackup on each of the cluster nodes. Be sure to use the NetBackup Virtual Name as the name of the NetBackup server. Follow the instructions for installing NetBackup server software.

   Refer to the *NetBackup Installation Guide*.
4. Configure the clustered NetBackup server.

   Refer to the *NetBackup High Availability Guide*.
5. Install any Maintenance Packs and patches that are required to bring the newly installed NetBackup server to the same patch level as the server being replaced.
6. Configure required devices and media and recover the NetBackup catalogs.

   See "Recovering the master server when root is intact" on page 208.
7. Bring the NetBackup resource group on each node in turn and run the **Device Configuration** Wizard to configure the devices.

   Configuration information on your particular cluster is available.

   Refer to the *NetBackup High Availability Guide*.

About disk recovery procedures for Windows

The three different types of disk recovery for Windows are as follows:

- Master server disk recovery procedures
  See "About recovering the master server disk for Windows" on page 217.
- Media server disk recovery procedures
  See "About recovering the NetBackup media server disk for Windows" on page 223.
- Client disk recovery procedures
  See "Recovering a Windows client disk" on page 223.

The disk-based images that reside on AdvancedDisk or on OpenStorage disks cannot be recovered by means of the NetBackup catalog. These disk images must be recovered by means of the NetBackup import feature. For information on import, refer to the section on importing NetBackup images in the following manual:

See *NetBackup Administrator's Guide, Volume I*.

Note: When the disk image is imported, NetBackup does not recover the original catalog entry for the image. Instead, a new catalog entry is created.

About recovering the master server disk for Windows

The procedure in this section explains how to recover data if one or more disk partitions are lost on a Windows NetBackup master server.

The following two scenarios are covered:

- Windows is intact and not corrupted. The system still starts Windows, but some or all other partitions are lost. NetBackup software is assumed to be lost.
  See "Recovering the master server with Windows intact" on page 217.
- All disk partitions are lost. Windows must be reinstalled, which is a total recovery. These procedures assume that the NetBackup master disk was running a supported version of Windows and that the defective hardware has been replaced.
  See "Recovering the master server and Windows" on page 220.

For NetBackup master and media servers, the directory locations of the NetBackup catalog become an integral part of NetBackup catalog backups. Any recovery of the NetBackup catalog requires the identical directory paths or locations be created before the catalog recovery.

Recovering the master server with Windows intact

This procedure shows how to recover the NetBackup master server with the Windows operating system intact.

To recover the master server with Windows intact

1. Determine the *install_path* in which NetBackup is installed. By default, NetBackup is installed in the `C:\Program Files\VERITAS` directory.
2. Determine if any directory paths or locations need to be created for NetBackup catalog recovery.
3. Partition any disks being recovered as they were before the failure (if partitioning is necessary). Then reformat each partition as it was before the failure.
4. Reinstall NetBackup software on the server.

   Refer to the *NetBackup Installation Guide for Windows*.
5. Install any NetBackup patches that had been previously installed. See the documentation that was included with the patch software.

6 If the catalog directories differ from those in the NetBackup catalog backups, recreate that directory structure on disk before you recover the catalog. For example, use the NetBackup `nbdb_move` command to relocate parts of the NetBackup relational database catalog.

7 If the recovery scenario involves restoring policy or catalog backups, the appropriate recovery devices must be configured.

You may have to do some or all of the following:

- Install and configure the robotic software for the devices that read backups of the NetBackup catalog and regular backups of the disk being restored. If a non-robotic drive is available that can read these backups, then no robot is required. Although manual intervention is required if multiple pieces of media are required.
  See the *NetBackup Device Configuration Guide*.
- Use the NetBackup **Device Configuration** Wizard to discover and configure the recovery device in NetBackup.
  See the *NetBackup Administrator's Guide, Volume I*.
- Use the NetBackup command `tpautoconf` to discover and configure the recovery device in NetBackup.
  See the *NetBackup Commands Reference Guide* manual.
- Update the device mapping files.
  See the *NetBackup Administrator's Guide, Volume I*.

8 If the recovery scenario involves restoring the policy backups or catalog backups that were done to media, the appropriate recovery device(s) must be configured.

Configuring the media may involve the following actions:

- Manually load the required media into a stand-alone recovery device.
- Use NetBackup utilities such as `robtest` or vendor-specific robotic control software to load media into the required recovery devices.
- Use the NetBackup Volume Configuration Wizard to inventory the media contents of a robotic device.
- Use the vendor-specific robotic control software to load the media into the required recovery device(s).

9 Recover the NetBackup catalogs.

See "About recovering the NetBackup catalog" on page 228.

10 When catalog recovery is complete, stop and restart the NetBackup services. Use the following `bpdown` and `bpup` commands, the **Activity Monitor** in the **NetBackup Administration Console**, or the Services application in the Windows Control Panel.

install_path\NetBackup\bin\bpdown
install_path\NetBackup\bin\bpup

Your configuration may include an EMM server that is separate from the master server. If so, start NetBackup on the EMM server before starting NetBackup on the master server.

Warning: In step 11, do not restore files to the *install_path*\NetBackup\db, *install_path*\NetBackupDB, *install_path*\NetBackup\var, or *install_path*\Volmgr\database directories. The catalogs were recovered in step 9 and overwriting them with regular backups leave them in an inconsistent state.

If the NetBackup relational database files were relocated using `nbdb_move` from *install_path*\NetBackupDB\data, they are recovered in step 9 and should not be restored in step 11.

11 To restore all other files, do the following actions in the order shown:

- Start the NetBackup Administration interface on the master server.
- Start the Backup, Archive, and Restore utility.
- Browse for restores and select only the partitions that were lost. Select the system directory (typically `C:\Winnt`), which ensures that all registry files are restored.
- Deselect the *install_path*\NetBackup\db, *install_path*\NetBackupDB, *install_path*\NetBackup\var, and *install_path*\Volmgr\database directories (see the caution in step 10).
- If you reinstall Windows, select the **Overwrite existing files** option, which ensures that existing files are replaced with the backups.
- Start the restore.

12 Reboot the system, which replaces any files that were busy during the restore. When the boot process is complete, the system is restored to the state it was in at the time of the last backup.

Recovering the master server and Windows

This procedure assumes that all disk partitions in Windows are lost.

To recover the master server and Windows

1. Install a minimal Windows operating system (perform the Express install).
   - Install the same type and version of Windows software that was used previously.
   - Install Windows in the same partition that was used before the failure.
   - Install any required patches. Take corrective action as needed.
   - Specify the default workgroup. Do not restore the domain.
   - Install and configure special drivers or other software that is required to get the hardware operational (for example, a special driver for the disk drive).
   - Install SCSI or other drivers as needed to communicate with the tape drives on the system.
   - Follow any hardware manufacturer's instructions that apply, such as loading SSD on a Compaq system.
   - Reboot the system when Windows installation is complete.
2. Determine the *install_path* in which NetBackup is installed. By default, NetBackup is installed in the `C:\Program Files\VERITAS` directory.
3. Determine if any directory paths or locations need to be created for NetBackup catalog recovery.
4. If necessary, partition any disks being recovered as they were before the failure. Then reformat each partition as it was before the failure.
5. Reinstall NetBackup software on the server being recovered. Do not configure any NetBackup policies or devices at this time.
6. Install any NetBackup patches that had been previously installed. See the documentation that was included with the patch software.
7. If the catalog directories differ from those in the NetBackup catalog backups, recreate that directory structure on disk before you recover the catalog. For example, use the NetBackup `nbdb_move` command to relocate parts of the NetBackup relational database catalog.
8. If the recovery scenario involves restoring policy or catalog backups, the appropriate recovery device or devices have to be configured.

   You may have to do all or some of the following tasks:

- Install and configure the robotic software for the devices that read backups of the NetBackup catalog and regular backups of the disk being restored. If a non-robotic drive is available that can read these backups, then no robot is required. Although manual intervention is required if multiple pieces of media are required.
  See the *NetBackup Device Configuration Guide*.
- Use the NetBackup **Device Configuration** Wizard to discover and configure the recovery device in NetBackup.
  See the *NetBackup Administrator's Guide, Volume I*.
- Use the NetBackup command `tpautoconf` to discover and configure the recovery device in NetBackup.
  See the *NetBackup Commands Reference Guide* manual.
- Update the device mapping files.
  See the *NetBackup Administrator's Guide, Volume I*.

9 If you must restore from the policy backups or catalog backups that were done to media, the appropriate media may have to be configured in NetBackup.

See the *NetBackup Administrator's Guide, Volume I*.

When you configure the media, you may have to do some or all of the following:

- Manually load the required media into a stand-alone recovery device.
- Use the NetBackup utilities such as `robtest` or vendor-specific robotic control software to load media into the required recovery devices.
- Use the NetBackup Volume Configuration Wizard to inventory the media contents of a robotic device.
- Use the vendor-specific robotic control software to load the media into the required recovery devices.

10 Recover the NetBackup catalogs.

See "About recovering the NetBackup catalog" on page 228.

11 When catalog recovery is complete, stop and restart the NetBackup services. Use the following `bpdown` and `bpup` commands, the **Activity Monitor** in the **NetBackup Administration Console**, or the Services application in the Windows Control Panel.

```
install_path\NetBackup\bin\bpdown
install_path\NetBackup\bin\bpup
```

Warning:

In step 12, do not restore files to the *install_path*`\NetBackup\db`, *install_path*`\NetBackupDB`, *install_path*`\NetBackup\var`, or *install_path*`\Volmgr\database` directories. These directories were recovered in step 10 and overwriting them with regular backups leaves the catalogs in an inconsistent state. If the relational database files were relocated using `nbdb_move` from *install_path*`\NetBackupDB\data`, they are recovered in step 10 and should not be restored in step 12.

---

12 To restore all other files, do the following steps in the order presented:

- Start the NetBackup Administration interface on the master server.
- Start the Backup, Archive, and Restore client interface.
- Browse for restores and select only the partitions that were lost. Select the system directory (typically `C:\Winnt`), which ensures that all registry files are restored.
- Deselect the *install_path*`\NetBackup\db`, *install_path*`\NetBackupDB` (or relocated NetBackup relational database path), *install_path*`\NetBackup\var`, or *install_path*`\Volmgr\database` directories.
  See the caution in this procedure.
- If you reinstall Windows, select the **Overwrite existing files** option, which ensures that existing files are replaced with the backups.
- Start the restore.

13 Restart the system, which replaces any files that were busy during the restore. When the boot process is complete, the system is restored to the state it was in at the time of the last backup.

About recovering the NetBackup media server disk for Windows

NetBackup media servers store their information in the NetBackup relational database. If you need to recover the system disk on a NetBackup media server, the recommended procedure is similar to disk recovery for the client.

See “Recovering a Windows client disk” on page 223.

Recovering a Windows client disk

The following procedure explains how to perform a total recovery of a Windows NetBackup client in the event of a system disk failure.

NetBackup Bare Metal Restore (BMR) protects client systems by backing them up with a policy configured for BMR protection. A complete description of BMR backup and recovery procedures is available.

See the *Bare Metal Restore System Administrator's Guide*.

This procedure assumes that the Windows operating system and NetBackup are reinstalled to boot the system and perform a restore.

The following are additional assumptions:

- The NetBackup client was running a supported Microsoft Windows version.
- The NetBackup client was backed up with a supported version of NetBackup client and server software.
- The NetBackup master server to which the client sent its backups is operational. You request the restore from this server.
- The backups included the directory where the operating system and its registry resided.
  If the backups excluded any files that resided in the directory, you may not be able to restore the system identically to the previous configuration.
- Defective hardware has been replaced.

Before starting, verify that you have the following:

- Windows system software to reinstall on the NetBackup client that being restored. Reinstall the same type and version of software that was previously used.
- NetBackup client software to install on the client that being restored.
- Special drivers or other software that is required to make the hardware operational (for example, a special driver for the disk drive).
- IP address and host name of the NetBackup client.
- IP address and host name of the NetBackup master server.

- The partitioning and formatting scheme that was used on the system to be restored. You must duplicate that scheme during Windows installation.

To recover a Windows client disk

1. Install a minimal Windows operating system (perform the Express install).

   During the installation, do the following tasks:

   - Partition the disk as it was before the failure (if partitioning is necessary). Then, reformat each partition as it was before the failure.
   - Install the operating system in the same partition that was used before the failure.
   - Specify the default workgroup. Do not restore to the domain.
   - Follow any hardware manufacturers' instructions that apply.

2. Reboot the system when the installation is complete.
3. Configure the NetBackup client system to re-establish network connectivity to the NetBackup master server.

   For example, if your network uses DNS, the configuration on the client must use the same IP address that was used before the failure. Also, it must specify the same name server (or another name server that recognizes both the NetBackup client and master server). On the client, configure DNS in the **Network** dialog, accessible from the Windows Control Panel.

4. Install NetBackup client software.

   Refer to the *NetBackup Installation Guide for Windows* for instructions. Ensure that you specify the correct names for the client server and master server.

   - To specify the client name, start the Backup, Archive, and Restore interface on the client and click **NetBackup Client Properties** on the **File** menu. Enter the client name on the **General** tab of the **NetBackup Client Properties** dialog.
   - To specify the server name, click **Specify NetBackup Machines and Policy Type** on the **File** menu.

5. Install any NetBackup patches that had previously been installed.
6. Enable debug logging by creating the following debug log directories on the client:

   ```
   install_path\NetBackup\Logs\tar
   install_path\NetBackup\Logs\bpinetd
   ```

   NetBackup creates logs in these directories.

7 Stop and restart the NetBackup Client service.

This action enables NetBackup to start logging to the `bpinetd` debug log.

8 Use the NetBackup Backup, Archive, and Restore interface to restore the system files and user files to the client system.

For example, if all files are on the `C` drive, restoring that drive restores the entire system.

To restore files, you do not need to be the administrator, but you must have restore privileges. For instructions, refer to the online Help or refer to the following:

See the *NetBackup Backup, Archive, and Restore Getting Started Guide*.

NetBackup restores the registry when it restores the Windows system files. For example, if the system files are in the `C:\Winnt` directory, NetBackup restores the registry when it restores that directory and its subordinate subdirectories and files.

9 Check for ERR or WRN messages in the log files that are in the directories you created in step 6.

If the logs indicate problems with the restore of Windows system files, resolve those problems before proceeding.

10 Stop the NetBackup Client service and verify that the `bpinetd` program is no longer running.

11 Restart the NetBackup client system.

When the boot process is complete, the system is restored to the state it was in at the time of the last backup.

About clustered NBU server recovery for Windows

NetBackup server clusters do not protect against catalog corruption, loss of the shared disk, or loss of the whole cluster. Regular catalog backups must be performed. More information is available about configuring catalog backups and system backup policies in a clustered environment.

Refer to topics about configuring NetBackup in the *NetBackup High Availability Guide*.

Warning: Contact technical support before you try these recovery procedures.

Replacing a failed node on a Windows VCS cluster

Cluster technology-specific information is available about how to bring the NetBackup resource group online and offline. Also, it is available on how to freeze and unfreeze (disable and enable the monitoring for) the resource group.

Refer to topics about configuring NetBackup in the *NetBackup High Availability Guide*.

Check the following conditions before you proceed with this procedure:

- The hardware, system software, and cluster environment on the replacement node have been configured.
- The reconfigured node or replacement node has been made a member of the cluster and has the same name as the failed node.

The following procedure applies when the shared disk and at least one configured cluster node remain available.

To replace a failed node on a Windows cluster using VCS

1. Freeze the NetBackup service.
2. Ensure that the NetBackup shared disks are not mounted on the node on which NetBackup is to be installed.
3. Reinstall NetBackup on the new node or replacement node. Be sure to use the NetBackup Virtual Name as the name of the NetBackup server. Follow the instructions for installing the NetBackup server software.

   Refer to the *NetBackup Installation Guide*.
4. Ensure that the node is a member of an existing cluster and that it performs the necessary configuration automatically.
5. Install any Maintenance Packs and patches that are required to bring the newly installed node to the same patch level as the other cluster nodes.
6. Unfreeze the NetBackup service and verify that it can be brought up on the replacement node.

Recovering the shared disk on a Windows VCS cluster

The following procedure is applicable in situations where the configured cluster nodes remain available but the NetBackup catalog, database files, or both on the shared disk have been corrupted or lost.

Check the following conditions before you proceed with this procedure:

- The shared storage hardware is restored to a working state, so that the shared disk resource can be brought online with an empty shared directory.

- Valid online catalog backups exist.

To recover the shared disk on a Windows cluster that uses VCS

1. Clear the faulted NetBackup resource group, disable monitoring, and bring up the shared disk and virtual name resources on a functioning node.
2. Ensure that all NetBackup shared disks are assigned the same drive letters that were used when NetBackup was originally installed and configured.
3. To reconfigure NetBackup for the cluster, initialize the database by running the following commands in sequence on the active node:

   ```
   bpclusterutil -ci
   tpext
   bpclusterutil -online
   ```

4. Use the appropriate NetBackup catalog recovery procedure to restore the NetBackup catalog information on the shared disk.

   See "Recovering the master server and Windows" on page 220.
5. If the clustered NetBackup server is a media server, verify that the restored vm.conf file contains the correct host-specific MM_SERVER_NAME configuration entry for the active node. If MM_SERVER_NAME is different from the local host name, edit the file and change the server name to the local host name:

   MM_SERVER_NAME=<local host name>
6. Use NetBackup to restore any data on the shared disks. Details are available on how to perform a restore.

   Refer to the *NetBackup Backup, Archive, and Restore Getting Started Guide*.
7. Configure required devices and media and recover the NetBackup catalogs.
8. Manually shut down and restart NetBackup on the active node.
9. Re-enable monitoring of the NetBackup resource group.
10. Verify that the NetBackup server can now be brought online on all configured nodes.

Recovering the entire Windows VCS cluster

The following procedure applies to the clustered NetBackup server environment that must be re-created from scratch.

Before you proceed, ensure that you have valid online catalog backups.

To recover the entire Windows VCS cluster

1. Configure the hardware, system software, and cluster environment on the replacement cluster.
2. Ensure that the appropriate low-level tape device and robotic control device configuration necessary for your operating system has been performed.

   Refer to the *NetBackup Device Configuration Guide*.
3. Reinstall NetBackup on each of the cluster nodes. Be sure to use the NetBackup Virtual Name as the name of the NetBackup server. Follow the instructions for installing NetBackup server software.

   Refer to the *NetBackup Installation Guide*.
4. Configure the clustered NetBackup server.

   Refer to the *NetBackup High Availability Guide*.
5. Install any Maintenance Packs and patches that are required to bring the newly installed NetBackup server to the same patch level as the server that is being replaced.
6. Configure required devices and media and recover the NetBackup catalogs.

   See "Recovering the master server and Windows" on page 220.
7. Bring the NetBackup resource group on each node in turn and run the **Device Configuration** Wizard to configure the devices.

   Configuration information on your cluster (MSCS or VCS) is available.

   Refer to the *NetBackup High Availability Guide*.

About recovering the NetBackup catalog

The NetBackup catalog consists of the following parts:

Image files	Information about the backups. It is the largest part of the catalog.
NetBackup configuration files	The `databases.conf` and `server.conf` configuration files are the flat files that contain instructions for the SQL Anywhere services.
Relational database files	Information about media and the storage devices that are in NetBackup storage units. Also, the NetBackup catalog images files.

Several options to recover the catalog exist, as follows:

Table 8-2 Catalog recovery options

Recovery option	Description
Recover the entire catalog	Symantec recommends that you recover the entire catalog. Doing so helps ensure consistency among the various parts of the catalog. This method is most useful for recovering a catalog to the same environment from which it was backed up. See "About recovering the entire NetBackup catalog" on page 232.
Recover the catalog image files and configuration files	The image database contains information about the data that has been backed up. The configuration files (databases.conf and server.conf) are the flat files that contain instructions for the SQL Anywhere daemon. This type of restore also restores the NetBackup relational database (NBDB) to the staging directory so that it is available for further processing if required. See "About recovering the NetBackup catalog image files" on page 243.
Recover the relational database files	The NetBackup database (NBDB) is also known as the Enterprise Media Manager (EMM) database. It contains information about volumes and the robots and drives that are in NetBackup storage units. The NetBackup relational database also contains the NetBackup catalog images files. The images files contain the metadata that describes the backups. Recover the relational database if it is corrupt or lost but the catalog image files exist and are valid. See "About recovering the NetBackup relational database" on page 257.

Recovery of the entire catalog or the catalog image files relies on the disaster recovery information. That information is saved in a file during the catalog backup. The location of the disaster recovery file is configured in the catalog backup policy.

See "Recovering the NetBackup catalog without the disaster recovery file" on page 266.

Note: After a catalog recovery, NetBackup freezes the removeable media that contains the catalog backup. This operation prevents a subsequent accidental overwrite action on the final catalog backup image on the media. This final image pertains to the actual catalog backup itself, and its recovery is not part of the catalog recovery. You can unfreeze the media.

Catalog recovery may be part of a larger recovery procedure.

See "About disk recovery procedures for UNIX and Linux" on page 207.

See "About disk recovery procedures for Windows" on page 216.

Other procedures exist for special use cases.

See “Recovering the NetBackup catalog when NetBackup Access Control is configured” on page 264.

Other topics provide more information about catalog recovery.

See “About NetBackup catalog recovery on Windows computers” on page 230.

See “About NetBackup catalog recovery from disk devices” on page 230.

See “About NetBackup catalog recovery and OpsCenter” on page 231.

About NetBackup catalog recovery on Windows computers

On Windows computers, the NetBackup media server host names are stored in the Windows registry. (They also are stored in the NetBackup catalog.)

If you install NetBackup during a catalog recovery scenario, ensure that you enter your media server names during the installation. Doing so adds them to the registry. Your catalog recovery and any subsequent backups that use the existing media servers and storage devices then function correctly.

About NetBackup catalog recovery from disk devices

In a catalog recovery, the disk media IDs in the recovery environment may differ from the disk media IDs in the backup environment. They may differ in the following uses cases:

- The storage devices are the same but the NetBackup master server installation is new. A master server host or disk failure may require that you install NetBackup. Configuring the devices in NetBackup may assign different disk media IDs to the disk volumes than were assigned originally.
- The disk storage devices are different than those to which the catalog backups were written. It may be in the same environment after storage hardware failure or replacement. It may be at another site to which you replicate the catalog backups and the client backups. Regardless, the catalog backups and the client backups reside on different hardware. Therefore, the disk media IDs may be different .

In these scenarios, NetBackup processes the disk media IDs so that the catalog may be recovered. The processing maps the disk media IDs from the backup environment to the disk media IDs in the recovery environment.

This processing occurs when the catalog backup resides on one of the following storage types:

- An AdvancedDisk disk pool
- A **Media Server Deduplication Pool** (MSDP)

- An OpenStorage device

About NetBackup catalog recovery and symbolic links

When you recover the NetBackup catalog, you must account for any symbolic links the NetBackup catalog directory structure, as follows:

`db/images` directory	If the NetBackup `db/images` directory resides on the storage that is the target of a symbolic link, that symbolic link must exist in the recovery environment. The symbolic link also must have the same target in the recovery environment.
`db/images/`*`client`* directories	If any of the client subdirectories under the `db/images` directory are symbolic links, they also must exist in the recovery environment. The symbolic links also must have the same targets in the recovery environment.

Catalog recovery of clustered master server	To recover the NetBackup catalog from a clustered master server to a single master server at a disaster recovery site, you must create the following symbolic links on the recovery host before you recover the catalog:
	`/usr/openv/netbackup/db -> /opt/VRTSnbu/netbackup/db`
	`/usr/openv/db/staging -> /opt/VRTSnbu/db/staging`
	On Solaris systems only, you also must create the following symbolic links before you recover the catalog:
	`/usr/openv -> /opt/openv`

If the symbolic links and their targets do not exist, catalog recovery fails.

About NetBackup catalog recovery and OpsCenter

When the NetBackup catalog is recovered, NetBackup resets the job ID to 1. NetBackup starts assigning job numbers beginning with 1.

If you use NetBackup OpsCenter to monitor NetBackup activity, you may see duplicate job IDs in OpsCenter after a catalog recovery. To prevent duplicate job IDs, you can specify the job ID number in NetBackup. Specify a number that is one higher than the highest job number in OpsCenter.

See "Specifying the NetBackup job ID number after a catalog recovery" on page 232.

Specifying the NetBackup job ID number after a catalog recovery

You can specify the NetBackup job ID number after a catalog recovery. If you use OpsCenter to monitor NetBackup activity, doing so prevents duplicate job ID numbers in OpsCenter.

See "About NetBackup catalog recovery and OpsCenter" on page 231.

To specify the NetBackup job ID number after a catalog recovery

1. If necessary, restore the OpsCenter database from a backup.
2. Determine the last job ID number that is recorded in OpsCenter.
3. Edit the NetBackup `jobid` file and set the value to one higher than the number from step 2. The following is the pathname to the `jobid` file:
   - UNIX: `/usr/openv/netbackup/db/jobs/jobid`
   - Windows: *`install_path`*`\Veritas\NetBackup\db\jobs\jobid`

   Because the recovery consumes job numbers, you must specify the number before the catalog recovery.
4. Recover the NetBackup catalog.

About recovering the entire NetBackup catalog

Symantec recommends that you recover the entire catalog. Doing so helps ensure consistency among the various parts of the catalog.

Recovery includes the catalog image files and configuration files that are in the catalog backups that are identified by the disaster recovery file, as follows:

Full backup	The NetBackup relational database files identified by the DR file are restored. The images and configuration files that are identified by the disaster recovery file are restored.
Incremental backup	The NetBackup relational database files identified by the DR file are restored. All catalog backup image files back to the last full catalog backup are automatically included in an incremental catalog backup. Therefore, only catalog images and configuration files that changed since the last full backup are restored. You can then use the Backup, Archive, and Restore user interface to restore all backup images.

You can use either of the following methods to recover the entire catalog:

- The **Catalog Recovery Wizard** in the **NetBackup Administration Console**.

See “Recovering the entire NetBackup catalog using the Catalog Recovery Wizard” on page 233.

- The text-based wizard launched by the `bprecover -wizard` command and option.
  See “Recovering the entire NetBackup catalog using bprecover -wizard” on page 239.

The relational database transaction log is not applied during full catalog recovery.

Recovering the entire NetBackup catalog using the Catalog Recovery Wizard

This procedure describes how to recover the entire catalog using the **Catalog Recovery Wizard**. You must have root (administrative) privileges.

The relational database transaction log is not applied during full catalog recovery.

You must have root (administrative) privileges to perform these procedures.

You must be logged on to the master server on which you want to recover the catalog. The **Catalog Recovery Wizard** does not work after you perform a change server operation.

Note: During the catalog recovery process, services may be shut down and restarted. If NetBackup is configured as a highly available application (cluster or global cluster), freeze the cluster before starting the recovery process to prevent a failover. Then unfreeze the cluster after the recovery process is complete.

Note: Full catalog recovery restores the device and media configuration information in the catalog backup. If you must configure storage devices during the recovery, Symantec recommends that you recover only the NetBackup image files.

See “About recovering the NetBackup catalog image files” on page 243.

Warning: Do not run any client backups before you recover the NetBackup catalog.

To recover the entire catalog by using the Catalog Recovery Wizard

1. If recovering the catalog to a new NetBackup installation, such as at a disaster recovery site, go to step 3.
2. Start all of the NetBackup services by entering the following:
   - On UNIX and Linux:
     `/usr/openv/netbackup/bin/bp.start_all`

- On Windows:

  install_path\NetBackup\bin\bpup

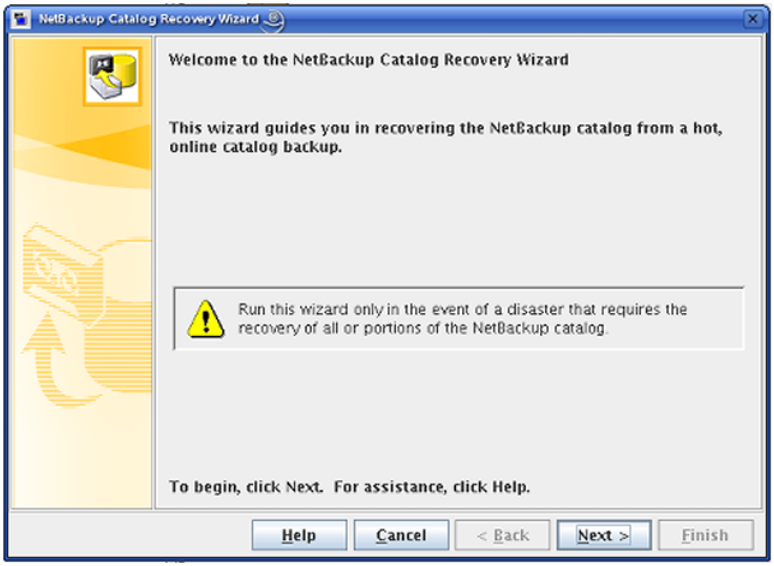
3 Start the **NetBackup Administration Console**.

4 If the necessary devices are not already configured, configure them in NetBackup.

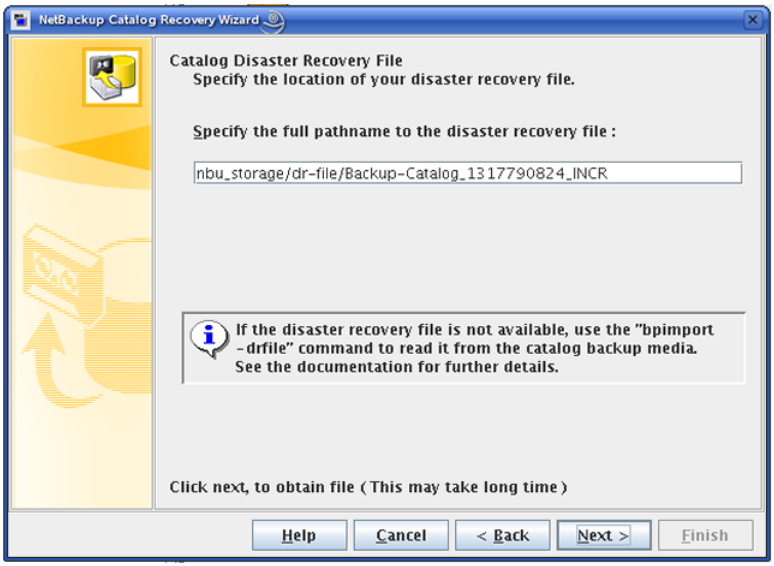
5 Make available to NetBackup the media that contains the catalog backup.

6 Click **Recover the catalogs** on the **NetBackup Administration Console** to start the **Catalog Recovery Wizard**.

The **Welcome** panel appears.



7 Click **Next** on the **Welcome** panel to display the **Catalog Disaster Recovery File** panel.

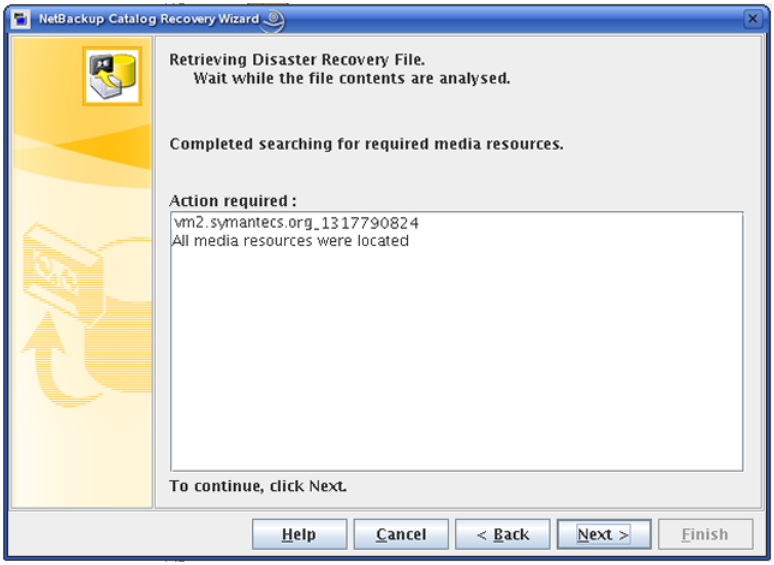


Specify where the disaster recovery file is stored by entering the fully qualified path to the disaster recovery file.

In most cases, you specify the most recent disaster recovery information file available. If the most recent catalog backup is an incremental backup, use the disaster recovery file from the incremental backup. (There is no need to first restore the full backup and then follow with the incremental backup.)

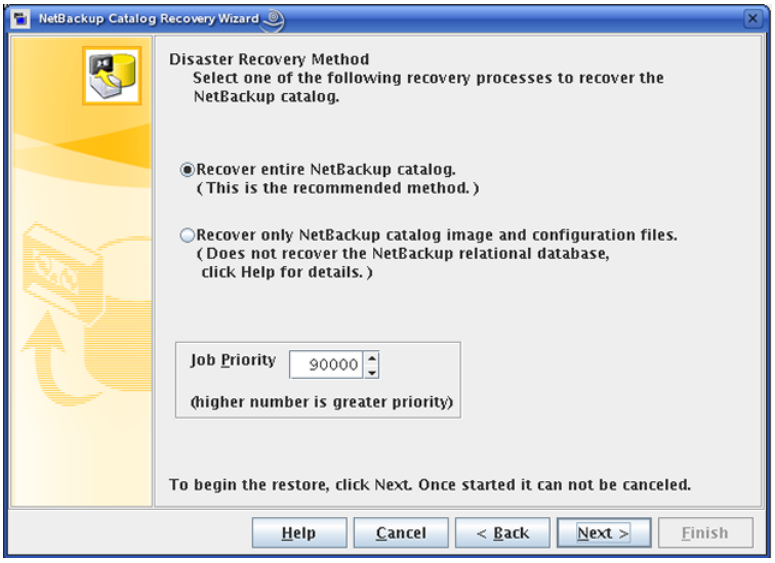
If some form of corruption has occurred, you may want to restore to an earlier state of the catalog.

8 The wizard waits while NetBackup searches for the necessary media sources. The wizard then informs you if the necessary backup ID of the disaster recovery image is located. If the media is not located, the wizard lists which media is needed to update the database.



If necessary, follow the wizard instructions to insert the media that is indicated and run an inventory to update the NetBackup database. The information that is displayed on this panel depends on whether the recovery is from a full backup or an incremental backup.

9 When the required media sources are all found, click **Next** to display the **Disaster Recovery Method** panel. The **Recover entire NetBackup catalog** option is selected.



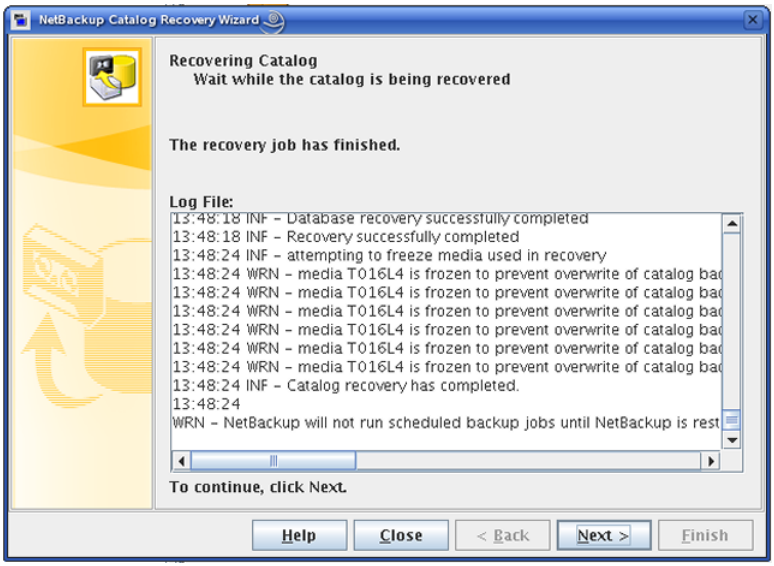
10 If desired, select a **Job Priority** then click **Next** to initiate the recovery of the entire NetBackup catalog.

NetBackup restores the entire NetBackup relational database, which includes the following:

- NBDB database (including the EMM database)
- BMR database (if applicable)
- NetBackup policy files
- Backup image files
- Other configuration files

If the EMM server is located on a remote computer, the NBDB database is recovered on the remote computer.

11 The wizard displays the recovery progress and announces when the catalog has been recovered.



If the recovery is not successful, consult the log file messages for an indication of the problem. Fix the problem and then continue.

Click **Next** to continue to the final panel

12 Click **Finish** in the final panel

When the recovery job is finished, each image file is restored to the proper image directory, and the NetBackup relational databases (NBDB and optionally BMRDB) have been restored and recovered.

13 Before you continue, be aware of the following points:

- If you recovered the catalog from removable media, NetBackup freezes the catalog media.
  See "Unfreezing the NetBackup online catalog recovery media" on page 274.
- Before you restart NetBackup, Symantec recommends that you freeze the media that contains the backups more recent than the date of the catalog from which you recovered.
- NetBackup does not run scheduled backup jobs until you stop and then restart NetBackup.
  You can submit backup jobs manually before you stop and restart NetBackup. However, if you do not freeze the media that contains the

backups more recent than the date of the catalog from which you recovered, NetBackup may overwrite that media.

- Because this operation is a partial recovery, you must recover the relational database portion of the catalog.
  See "About recovering the NetBackup relational database" on page 257.

14 Stop and restart NetBackup on all the servers.

The following are the commands to stop and restart NetBackup.

- On UNIX and Linux:

```
/usr/openv/netbackup/bin/bp.kill_all
/usr/openv/netbackup/bin/bp.start_all
```

- On Windows:

```
install_path\NetBackup\bin\bpdown
install_path\NetBackup\bin\bpup
```

15 If the catalog recovery is part of a server recovery procedure, complete the remaining steps in the appropriate recovery procedure.

Recovery can include the following:

- Importing the backups from the backup media into the catalog.
- Write protecting the media.
- Ejecting the media and setting it aside.
- Freezing the media.

Recovering the entire NetBackup catalog using bprecover -wizard

The `bprecover -wizard` command is an alternative to using the **NetBackup Administration Console** wizard. You must have root (administrative) privileges to perform this procedure.

The relational database transaction log is not applied during full catalog recovery.

You must have root (administrative) privileges to perform these procedures.

You must be logged on to the master server on which you want to recover the catalog.

Note: During the catalog recovery process, services may be shut down and restarted. If NetBackup is configured as a highly available application (cluster or global cluster), freeze the cluster before starting the recovery process to prevent a failover. Then unfreeze the cluster after the recovery process is complete.

Note: Full catalog recovery restores the device and media configuration information in the catalog backup. If you must configure storage devices during the recovery, Symantec recommends that you recover only the NetBackup image files.

See "About recovering the NetBackup catalog image files" on page 243.

Warning: Do not run any client backups before you recover the NetBackup catalog.

To recover the entire catalog by using bprecover -wizard

1. If recovering the catalog to a new NetBackup installation, such as at a disaster recovery site, do the following:
   - Install NetBackup.
   - Configure the devices that are required for the recovery.
   - Add the media that are required for the recovery to the devices.
2. Start NetBackup.

   The following are the commands to start NetBackup:
   - UNIX and Linux:

     `/usr/openv/netbackup/bin/bp.start_all`
   - Windows:

     install_path`\NetBackup\bin\bpup.exe`
3. Start the `bprecover` wizard by entering the following command:
   - UNIX and Linux:

     `/usr/openv/netBbckup/bin/admincmd/bprecover -wizard`
   - Windows:

     install_path`\Veritas\NetBackup\bin\admincmd\bprecover.exe -wizard`

   The following is displayed:

```
Welcome to the NetBackup Catalog Recovery Wizard!

Please make sure the devices and media that contain catalog
```

```
disaster recovery data are available
Are you ready to continue?(Y/N)
```

4 Enter **Y** to continue. The following prompt appears:

```
Please specify the full pathname to the catalog disaster recovery
file:
```

5 Enter the fully qualified pathname to the disaster recovery file for the backup that you want to restore. For example:

```
/mnt/hdd2/netbackup/dr-file/Backup-Catalog_1318222845_FULL
```

If the most recent catalog backup was an incremental backup, use the disaster recovery file from the incremental backup. (There is no need to first restore the full backup and then follow with the incremental backup.) Alternately, you can recover from earlier version of the catalog.

If the pathname is to a valid DR file, a message similar to the following is displayed:

```
vm2.symantecs.org_1318222845
All media resources were located
Do you want to recover the entire NetBackup catalog? (Y/N)
```

If the DR file or the pathname is not valid, the command-line wizard exits.

6 Enter **Y** to continue. The following is displayed:

```
Do you want to startup the NetBackup relational database (NBDB)
after the recovery?(Y/N)
```

The image file is restored to the proper image directory and the NetBackup relational databases (NBDB and optionally BMRDB) are restored and recovered.

7 Enter **Y** or **N** to continue.

The following is displayed while the restore is in progress:

```
Catalog recovery is in progress. Please wait...

Beginning recovery of NBDB.  Please wait...
Completed successful recovery of NBDB on vm2.symantecs.org
INF - Catalog recovery has completed.

WRN - NetBackup will not run scheduled backup jobs until NetBackup
is restarted.

For more information, please review the log file:
/usr/openv/netbackup/logs/user_ops/root/logs/Recover1318344410.log
```

When the recovery job is finished, each image file is restored to the proper image directory, and the NetBackup relational databases (NBDB and optionally BMRDB) have been restored and recovered.

8 Before you continue, be aware of the following points:

- If you recovered the catalog from removable media, NetBackup freezes the catalog media.
  See "Unfreezing the NetBackup online catalog recovery media" on page 274.
- Before you restart NetBackup, Symantec recommends that you freeze the media that contains the backups more recent than the date of the catalog from which you recovered.
- NetBackup does not run scheduled backup jobs until you stop and then restart NetBackup.
  You can submit backup jobs manually before you stop and restart NetBackup. However, if you do not freeze the media that contains the backups more recent than the date of the catalog from which you recovered, NetBackup may overwrite that media.
- Because this operation is a partial recovery, you must recover the relational database portion of the catalog.
  See "About recovering the NetBackup relational database" on page 257.

9 Stop and restart NetBackup.

The following are the commands to stop and restart NetBackup:

- On UNIX and Linux:

```
/usr/openv/netbackup/bin/bp.kill_all
/usr/openv/netbackup/bin/bp.start_all
```

- On Windows:

```
install_path\NetBackup\bin\bpdown
install_path\NetBackup\bin\bpup
```

10 If the catalog recovery is part of a server recovery procedure, complete the remaining steps in the appropriate recovery procedure.

This procedure can include the following tasks:

- Importing the backups from the backup media into the catalog
- Write protecting the media
- Ejecting the media and setting it aside
- Freezing the media

About recovering the NetBackup catalog image files

The catalog image files contain information about all the data that has been backed up. This information constitutes the largest part of the NetBackup catalog. This type of catalog recovery does the following:

- Recovers the image `.f` files.
- Recovers the configuration files (`databases.conf` and `server.conf`).
- Restores the NetBackup relational database (NBDB) to the staging directory so that it is available for further processing if required.
  See "About processing the relational database in staging" on page 263.
- Optionally, recovers the policy and the licensing data.

Table 8-3 is a list of the files that are included in a partial recovery.

Note: Beginning with the NetBackup 7.5 release, the images files are now stored in the NetBackup relational database. The images files contain the metadata that describes the backups.

NetBackup supports recovery of the catalog image files and configuration files from a clustered environment to a non-clustered master server at a disaster recovery.

Recovery recommendations

See "About NetBackup catalog recovery and symbolic links" on page 231.

Symantec recommends that you recover the catalog images files in the following scenarios:

- The NetBackup relational database is valid, but NetBackup policy, backup image, or configuration files are lost or corrupt.
- You want to restore part of the NetBackup catalog before you restore the entire catalog. This procedure recovers only the catalog images and configuration files.
  After you recover the image files, you can recover the relational database.
  See "About recovering the NetBackup relational database" on page 257.
- You recover the catalog using different storage devices. It may be to the same environment after storage hardware failure or replacement. It may be another site to which you replicate the catalog backups and the client backups. Regardless, the catalog backups and the client backups reside on different hardware.
  This recovery does not overwrite the new storage device configuration with the old, no longer valid storage device information from the catalog backup.

Catalog recovery and backup types

Recovery includes the catalog image files and configuration files that are in the catalog backups listed in the disaster recovery file, as follows:

Full backup	The image files and configuration files that are listed in the disaster recovery file are recovered.
Incremental backup	Two recover scenarios exist, as follows: ■ The catalog contains *no* information about the corresponding full backup and other incremental backups. NetBackup restores only the backup image `.f` files, configuration files, and NetBackup policy files that are backed up in that incremental backup. However, all of the catalog backup image `.f` files up to the last full catalog backup are restored. Therefore, you can restore the rest of the policy, image `.f` files, and configuration files by using the Backup, Archive and Restore interface. ■ The catalog *contains* information about the corresponding full backup and other incremental backups. NetBackup restores all of the backup image `.f` files and the configuration files that were included in the related set of catalog backups.

Catalog image files

Table 8-3 lists the files that comprise a partial catalog recovery.

Table 8-3 Catalog image files

UNIX and Linux	Windows
`/usr/openv/netbackup/bp.conf`	Not applicable
`/usr/openv/netbackup/db/*`	*install_path*`\NetBackup\db\*`
`/usr/openv/netbackup/db/class/*` (optional)	*install_path*`\NetBackup\db\class\*` (optional)
`/usr/openv/netbackup/vault/sessions*`	*install_path*`\NetBackup\vault\sessions\*`
`/usr/openv/var/*` (optional)	*install_path*`\NetBackup\var\*` (optional)
`/usr/openv/volmgr/database/*`	*install_path*`\Volmgr\database\*`
`/usr/openv/volmgr/vm.conf`	*install_path*`\Volmgr\vm.conf`

Recovery methods

You can use either of the following methods to recover the catalog image files:

- The **Catalog Recovery Wizard** in the **NetBackup Administration Console**.
  See "Recovering the NetBackup catalog image files using the Catalog Recovery Wizard" on page 245.
- The text-based recovery wizard. The `bprecover -wizard` command and option start the text-based recovery wizard.
  See "Recovering the NetBackup catalog image files using bprecover -wizard" on page 252.

Recovering the NetBackup catalog image files using the Catalog Recovery Wizard

You must have root (administrative) privileges to perform this procedure.

You must be logged on to the master server on which you want to recover the catalog. The **Catalog Recovery Wizard** does not work after you perform a change server operation.

Note: This wizard relies on the disaster recovery file that was generated during the catalog backup. The path to the disaster recovery file is specified in the catalog backup policy.

Note: During the catalog recovery process, services may be shut down and restarted. If NetBackup is configured as a highly available application (cluster or global cluster), freeze the cluster before starting the recovery process to prevent a failover. Then unfreeze the cluster after the recovery process is complete.

Warning: Do not run any client backups before you recover the NetBackup catalog.

See "About recovering the NetBackup catalog image files" on page 243.

To recover the catalog image files using the Catalog Recovery Wizard

1. If recovering the catalog to a new NetBackup installation, such as at a disaster recovery site, do the following:
   - Install NetBackup.
   - Configure the devices that are required for the recovery.
   - Add the media that are required for the recovery to the devices.
   - Create symlinks to match those in the original environment.
     See "About NetBackup catalog recovery and symbolic links" on page 231.
2. If the EMM server is on a different host than the master server, start the NetBackup services on that host by entering the following command:
   - On UNIX and Linux:
     `/usr/openv/netbackup/bin/bp.start_all`
   - On Windows:
     install_path`\NetBackup\bin\bpup`
3. Start the NetBackup services on the master server by entering the following command:
   - On UNIX and Linux:
     `/usr/openv/netbackup/bin/bp.start_all`
   - On Windows:
     install_path`\NetBackup\bin\bpup`
4. Click **Recover the Catalogs** in the **NetBackup Administration Console** to start the **Catalog Recovery Wizard**.

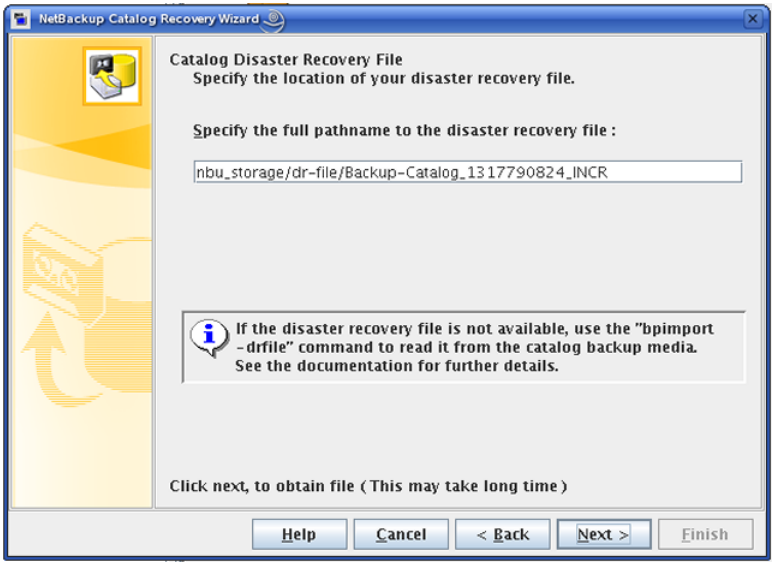
   The **Welcome to the NetBackup Disaster Recovery Wizard** panel appears.
5. Click **Next** in the wizard welcome panel.

   The **Catalog Disaster Recovery File** panel appears.

6 On the **Catalog Disaster Recovery File** panel, enter or browse to select the full pathname to the most recent disaster recovery information file available.

If the most recent catalog backup was an incremental backup, use the disaster recovery file from the incremental backup. (There is no need to first restore the full backup and then follow with the incremental backup.) Alternately, you can recover from earlier version of the catalog.

The following is an example of the wizard panel:

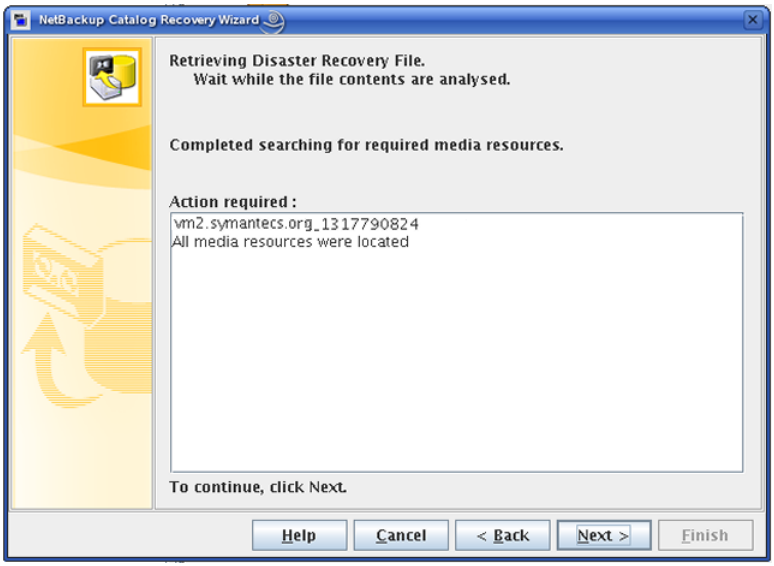


After you enter the fully qualified pathname to the disaster recovery file, click **Next**.

The **Retrieving Disaster Recovery File** panel appears.

7 The wizard searches for the media sources that are identified in the disaster recovery file. This wizard panel also displays the result of the media search.

The following is an example of the wizard panel.



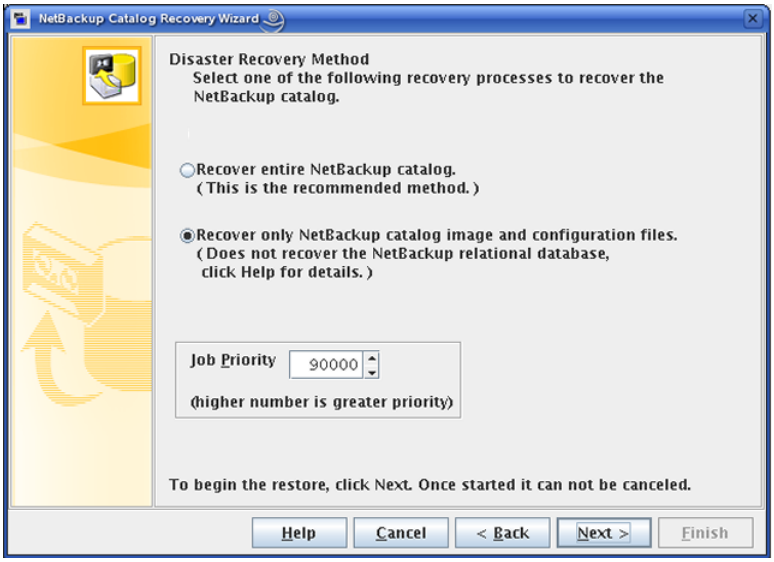
If the wizard finds the media, click **Next**.

If the wizard does not find the media, follow the wizard instructions to insert the required media and update the NetBackup database. After you insert the media and update the database, click **Next**.

The **Disaster Recovery Method** panel appears.

8 On the **Disaster Recovery Method** panel, select **Recover only NetBackup catalog image and configuration files** and specify a job priority.

The following is an example of the wizard panel.

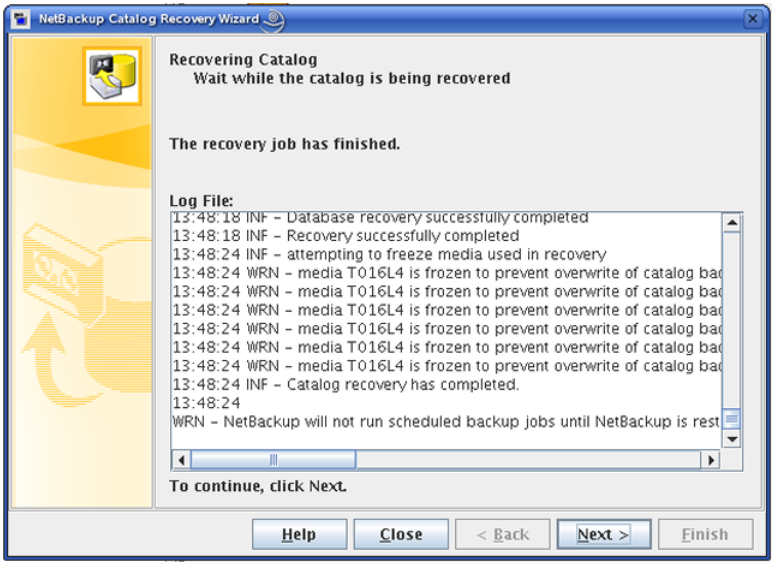


To continue, click **Next**.

The **Recovering Catalog** panel appears.

9 The **Recovering Catalog** panel displays the recovery progress.

The following is an example of the wizard panel.



If the recovery is not successful, consult the log file messages for an indication of the problem.

Click **Next** to continue to the final wizard panel.

10 On the final wizard panel, click **Finish**

11 When the recovery job is finished, each image file is restored to the proper image directory and the configuration files are restored. If you chose to recover the policy data and licensing data, it is restored also.

12 Export the image metadata from the relational database in the staging directory, as follows:

```
cat_export -all -staging -source_master source-master-server-name
```

The export is required so that the image metadata can be imported into the relational database. A catalog image file recovery does not recover the relational database.

13 Import the image metadata into the relational database, as follows:

```
cat_import -all -replace_destination
```

14 If you recovered the catalog from a disk device, you may have to fix the disk media ID references in the image headers. The image headers were recovered from the catalog backup.

To fix the disk media IDs in the image headers, run the following command:

```
nbcatsync -backupid image_id -dryrun
```

Replace *image_id* with the ID of the catalog backup. You can find the image ID of the catalog backup by examining the DR file.

15 Before you continue, be aware of the following points:

- If you recovered the catalog from removable media, NetBackup freezes the catalog media.
  See "Unfreezing the NetBackup online catalog recovery media" on page 274.
- Before you restart NetBackup, Symantec recommends that you freeze the media that contains the backups more recent than the date of the catalog from which you recovered.
- NetBackup does not run scheduled backup jobs until you stop and then restart NetBackup.
  You can submit backup jobs manually before you stop and restart NetBackup. However, if you do not freeze the media that contains the backups more recent than the date of the catalog from which you recovered, NetBackup may overwrite that media.
- Because this operation is a partial recovery, you must recover the relational database portion of the catalog.
  See "About recovering the NetBackup relational database" on page 257.

16 Stop and restart NetBackup on all the servers, as follows:

- On UNIX and Linux:

  ```
  /usr/openv/netbackup/bin/bp.kill_all
  /usr/openv/netbackup/bin/bp.start_all
  ```

- On Windows:

  ```
  install_path\NetBackup\bin\bpdown
  install_path\NetBackup\bin\bpup
  ```

17 If the catalog recovery is part of a server recovery procedure, complete the remaining steps in the appropriate recovery procedure.

Recovery can include the following:

- Importing the backups from the backup media into the catalog.

- Write protecting the media.
- Ejecting the media and setting it aside.
- Freezing the media.

Recovering the NetBackup catalog image files using bprecover -wizard

You must have root (administrative) privileges to perform this procedure.

You must be logged on to the master server on which you want to recover the catalog. The **Catalog Recovery Wizard** does not work after you perform a change server operation.

Note: This wizard relies on the disaster recovery file that was generated during the catalog backup. The path to the disaster recovery file is specified in the catalog backup policy.

Note: During the catalog recovery process, services may be shut down and restarted. If NetBackup is configured as a highly available application (cluster or global cluster), freeze the cluster before starting the recovery process to prevent a failover. Then unfreeze the cluster after the recovery process is complete.

Warning: Do not run any client backups before you recover the NetBackup catalog.

See "About recovering the NetBackup catalog image files" on page 243.

To recover the catalog image files using bprecover -wizard

1. If recovering the catalog to a new NetBackup installation, such as at a disaster recovery site, do the following:
   - Install NetBackup.
   - Configure the devices that are required for the recovery.
   - Add the media that are required for the recovery to the devices.
   - Create symlinks to match those in the original environment.
     See "About NetBackup catalog recovery and symbolic links" on page 231.
2. If the EMM server is on a different host than the master server, start the NetBackup services on that host by entering the following command:
   - On UNIX and Linux:
     ```
     /usr/openv/netbackup/bin/bp.start_all
     ```

- On Windows:

  install_path\NetBackup\bin\bpup

3 Start the NetBackup services on the master server by entering the following command:

- On UNIX and Linux:

  /usr/openv/netbackup/bin/bp.start_all

- On Windows:

  install_path\NetBackup\bin\bpup

4 Start the `bprecover` wizard by entering the following command:

```
bprecover -wizard
```

The following is displayed:

```
Welcome to the NetBackup Catalog Recovery Wizard!
Please make sure the devices and media that contain catalog
disaster recovery data are available
Are you ready to continue?(Y/N)
```

5 Enter **Y** to continue. You are prompted to enter the full path name of the disaster recovery file, as follows:

```
Please specify the full pathname to the catalog disaster recovery
file:
```

6 Enter the fully qualified path name to the disaster recovery file for the backup that you want to restore. For example:

```
/mnt/hdd2/netbackup/dr-file/Backup-Catalog_1318222845_FULL
```

If the most recent catalog backup was an incremental backup, use the disaster recovery file from the incremental backup. (There is no need to first restore the full backup and then follow with the incremental backup.) Alternately, you can recover from earlier version of the catalog.

If you specified a DR file for a full backup, a message similar to the following appears:

```
vm2.symantecs.org_1318222845
All media resources were located

Do you want to recover the entire NetBackup catalog? (Y/N)
```

If you specified a DR file for an incremental backup, a message similar to the following is displayed:

```
vm2.symantec.org_1318309224
All media resources were located

The last catalog backup in the catalog disaster recovery file is
an incremental.
If no catalog backup images exist in the catalog,
a PARTIAL catalog recovery will only restore the NetBackup catalog
files backed up in that incremental backup.

However, all of the catalog backup images up to the last full catalog
backup are restored.  Then you can restore the remaining NetBackup
catalog files from the Backup, Archive, and Restore user interface.
If catalog backup images already exist, all files that were included
in the related set of catalog backups are restored.

Do you want to recover the entire NetBackup catalog? (Y/N)
```

7 Enter **N** to continue. The following is displayed:

```
A PARTIAL catalog recovery includes the images directory
containing the dotf files and staging of the NetBackup relational
database (NBDB) for further processing.

Do you also want to include policy data?(Y/N)
```

8 Enter **Y** or **N** to continue. The following is displayed:

```
Do you also want to include licensing data?(Y/N)
```

9 Enter **Y** or **N** to continue. The following is displayed:

```
Catalog recovery is in progress. Please wait...

Completed successful recovery of NBDB in staging directory on
vm2.symantecs.org

This portion of the catalog recovery has completed.
Because this was a PARTIAL recovery of the NetBackup catalog,
any remaining files included in the catalog backup can be restored
using the the Backup, Archive, and Restore user interface.

The image metadata that is stored in NBDB in the staging directory
can be exported using "cat_export -staging", and, imported using
"cat_import".

The "nbdb_unload -staging" command can be used to unload one or more
database tables from NBDB in the staging directory.

The "nbdb_restore -recover -staging" command can be used to replace
NBDB in the data directory with the contents from the staging
directory.

WRN - NetBackup will not run scheduled backup jobs until NetBackup
is restarted.

For more information, please review the log file:
/usr/openv/netbackup/logs/user_ops/root/logs/Recover1318357550.log
```

10 When the recovery job is finished, each image file is restored to the proper image directory and the configuration files are restored. If you chose to recover the policy data and licensing data, it is restored also.

11 Export the image metadata from the relational database in the staging directory, as follows:

```
cat_export -all -staging -source_master source-master-server-name
```

The export is required so that the image metadata can be imported into the relational database. A catalog image file recovery does not recover the relational database.

12 Import the image metadata into the relational database, as follows:

```
cat_import -all -replace_destination
```

13 If you recovered the catalog from a disk device, you may have to fix the disk media ID references in the image headers. The image headers were recovered from the catalog backup.

See "About NetBackup catalog recovery from disk devices" on page 230.

To fix the disk media IDs in the image headers, run the following command:

```
nbcatsync -backupid image_id -prune_catalog
```

Replace *image_id* with the ID of the catalog backup. The `bprecover` output contains the image ID of the catalog backup being restored. Alternatively, you can find the image ID of the catalog backup by examining the DR file.

14 Before you continue, be aware of the following points:

- If you recovered the catalog from removable media, NetBackup freezes the catalog media.
  See "Unfreezing the NetBackup online catalog recovery media" on page 274.
- Before you restart NetBackup, Symantec recommends that you freeze the media that contains the backups more recent than the date of the catalog from which you recovered.
- NetBackup does not run scheduled backup jobs until you stop and then restart NetBackup.
  You can submit backup jobs manually before you stop and restart NetBackup. However, if you do not freeze the media that contains the backups more recent than the date of the catalog from which you recovered, NetBackup may overwrite that media.
- Because this operation is a partial recovery, you must recover the relational database portion of the catalog.
  See "About recovering the NetBackup relational database" on page 257.

15 Stop and restart NetBackup on all the servers, as follows:

- On UNIX and Linux:

  ```
  /usr/openv/netbackup/bin/bp.kill_all
  /usr/openv/netbackup/bin/bp.start_all
  ```

- On Windows:

```
install_path\NetBackup\bin\bpdown
install_path\NetBackup\bin\bpup
```

16 If the catalog recovery is part of a server recovery procedure, complete the remaining steps in the appropriate recovery procedure.

This procedure can include the following tasks:

- Importing the backups from the backup media into the catalog
- Write protecting the media
- Ejecting the media and setting it aside
- Freezing the media

About recovering the NetBackup relational database

The NetBackup database (NBDB) is also known as the Enterprise Media Manager (EMM) database. It contains information about volumes and the robots and drives that are in NetBackup storage units. The NetBackup relational database also contains the NetBackup catalog images files. The images files contain the metadata that describes the backups.

You can recover the NetBackup relational databases independently of an entire catalog backup.

Recover from a backup	See "Recovering NetBackup relational database files from a backup" on page 257.
Recover from the staging directory	See "Recovering the NetBackup relational database files from staging" on page 260.

Recovering NetBackup relational database files from a backup

You can recover the NetBackup (NBDB) or Bare Metal Restore (BMRDB) relational database files from a backup. Two recovery procedures exist, as follow:

The database is not corrupted	See "To recover relational database files from an online catalog backup if the database is corrupted" on page 258.
The database is corrupted	See "To recover relational database files from an online catalog backup if the database is not corrupted" on page 258.

To recover relational database files from an online catalog backup if the database is not corrupted

1. For online catalog recovery, run the following command on the master server:

   UNIX: `/usr/openv/netbackup/bin/admincmd/bprecover -r -nbdb`

   Windows: *`install_path`*`\NetBackup\bin\admincmd\bprecover -r -nbdb`

2. Stop and restart NetBackup, as follows:

   UNIX and Linux:

   ```
   /usr/openv/netbackup/bin/bp.kill_all
   /usr/openv/netbackup/bin/bp.start_all
   ```

   Windows:

   ```
   install_path\NetBackup\bin\bpdown
   install_path\NetBackup\bin\bpup
   ```

To recover relational database files from an online catalog backup if the database is corrupted

1. If the NetBackup services are running, stop them as follows:

   UNIX: `/usr/openv/netbackup/bin/bp.kill_all`

   Windows: *`install_path`*`\NetBackup\bin\bpdown`

2. Move the `*.db` and `*.log` files from the following database file directories to a temporary directory:

   UNIX: `/usr/openv/db/data`

   Windows: `C:\Program Files\Veritas\NetBackupDB\data`

3. Configure SQL Anywhere so that it does not try to start automatically when the host is started, as follows:

   Linux: `/usr/openv/db/bin/nbdb_admin -auto_start NONE`

   Windows: *`install_path`*`\NetBackup\bin\nbdb_admin -auto_start NONE`

4. Start the SQL Anywhere server, as follows:

   UNIX: `/usr/openv/netbackup/bin/nbdbms_start_stop start`

   Windows: *`install_path`*`\NetBackup\bin\bpup -e SQLANYs_VERITAS_NB`

5 Create the database. The command that you run depends on your scenario, as follows:

Normal scenario	UNIX: `/usr/openv/db/bin/create_nbdb -drop` Windows: *`install_path`*`\NetBackup\bin\create_nbdb -drop`
The database was relocated or the environment is clustered	UNIX: `/usr/openv/db/bin/create_nbdb -drop -staging` *`VXDBMS_NB_STAGING`* Windows: *`install_path`*`\NetBackup\bin\create_nbdb -drop -staging` *`VXDBMS_NB_STAGING`* Obtain the value for the staging directory (*`VXDBMS_NB_STAGING`*) from the `vxdbms.conf` file in the `data` directory that was identified in step 2.
The database was relocated or the environment is clustered, and space constraints force you to create this temporary database in the final location	UNIX: `/usr/openv/db/bin/create_nbdb -drop -data` *`VXDBMS_NB_DATA`* `-index` *`VXDBMS_NB_INDEX`* `-tlog` *`VXDBMS_NB_TLOG`* `-staging` *`VXDBMS_NB_STAGING`* Windows: *`install_path`*`\NetBackup\bin\create_nbdb -drop -data` *`VXDBMS_NB_DATA`* `-index` *`VXDBMS_NB_INDEX`* `-tlog` *`VXDBMS_NB_TLOG`* `-staging` *`VXDBMS_NB_STAGING`* Obtain the values for the option arguments from the `vxdbms.conf` file in the `data` directory that was identified in step 2.

6 Stop and restart NetBackup, as follows:

UNIX:

```
/usr/openv/netbackup/bin/bp.kill_all
/usr/openv/netbackup/bin/bp.start_all
```

Windows:

```
install_path\NetBackup\bin\bpdown
install_path\NetBackup\bin\bpup
```

7 Run the NetBackup `tpext` command to update the device mapping files, as follows:

UNIX: `/usr/openv/volmgr/bin/tpext -loadEMM`

Windows: *`install_path`*`\Volmgr\bin\tpext -loadEMM`

8 If you relocated the database files, re-create the directories where the files were located when you backed up the catalog.

9 Start the device manager, as follows:

UNIX: `/usr/openv/volmgr/bin/ltid -v`

Windows: Start the device manager service.

10 Configure the necessary recovery device in NetBackup.

11 Make available to NetBackup the media that contains the catalog backup. Inventory the robot, add the media for standalone drives, configure the storage server and disk pool, or so on.

12 Import the catalog backup from the media on which it resides. Perform both a Phase I and Phase II import.

See "Importing backup images, Phase I" on page 274.

See "Importing backup images, Phase II" on page 276.

13 Recover the catalog by running the following command on the master server:

UNIX: `/usr/openv/netbackup/bin/admincmd/bprecover -r -nbdb`

Windows: *`install_path`*`\NetBackup\bin\admincmd\bprecover -r -nbdb`

14 Stop and restart NetBackup, as follows:

UNIX and Linux:

```
/usr/openv/netbackup/bin/bp.kill_all
/usr/openv/netbackup/bin/bp.start_all
```

Windows:

```
install_path\NetBackup\bin\bpdown
install_path\NetBackup\bin\bpup
```

Recovering the NetBackup relational database files from staging

During a catalog backup, NetBackup copies the relational database files to the staging directory. The recovery option that restores the image files and the configuration files also restores the relational database files to the staging directory.

See "About recovering the NetBackup catalog image files" on page 243.

You can recover the NetBackup NBDB relational database files from the staging directory. You can also use NetBackup commands process the NBDB relational database files further.

See "About processing the relational database in staging" on page 263.

When the relational database is recovered from staging, NetBackup also applies the current online transaction log during the recovery. Applying the transaction log ensures that the database as consistent as possible with the current `db/images` directory.

To recover relational database files from staging if the database is not corrupted

1. Run the following command on the master server to recover NBDB from staging:

   UNIX: `/usr/openv/netbackup/bin/nbdb_restore -dbn NBDB -recover -staging`

   Windows: *`install_path`*`\NetBackup\bin\nbdb_restore -dbn NBDB -recover -staging`

2. Stop and restart NetBackup, as follows:

   UNIX:

   ```
   /usr/openv/netbackup/bin/bp.kill_all
   /usr/openv/netbackup/bin/bp.start_all
   ```

   Windows:

   ```
   install_path\NetBackup\bin\bpdown
   install_path\NetBackup\bin\bpup
   ```

To recover relational database files from staging if the database is corrupted

1. If the NetBackup services are running, stop them as follows:

   UNIX: `/usr/openv/netbackup/bin/bp.kill_all`

   Windows: *`install_path`*`\NetBackup\bin\bpdown`

2. Move the `*.db` and `*.log` files from the following database file directories to a temporary directory:

   UNIX: `/usr/openv/db/data`

   Windows: `C:\Program Files\Veritas\NetBackupDB\data`

3. Configure SQL Anywhere so that it does not try to start automatically when the host is started, as follows:

   Linux: `/usr/openv/db/bin/nbdb_admin -auto_start NONE`

   Windows: *`install_path`*`\NetBackup\bin\nbdb_admin -auto_start NONE`

4. Start the SQL Anywhere server, as follows:

   UNIX: `/usr/openv/netbackup/bin/nbdbms_start_stop start`

   Windows: *`install_path`*`\NetBackup\bin\bpup -e SQLANYs_VERITAS_NB`

5 Create an empty database, as follows:

UNIX: `/usr/openv/db/bin/create_nbdb -drop`

Windows: *`install_path`*`\NetBackup\bin\create_nbdb -drop`

6 Stop and restart NetBackup, as follows:.

UNIX and Linux:

```
/usr/openv/netbackup/bin/bp.kill_all
/usr/openv/netbackup/bin/bp.start_all
```

Windows:

```
install_path\NetBackup\bin\bpdown
install_path\NetBackup\bin\bpup
```

7 Run the NetBackup `tpext` command to update the device mapping files, as follows:

UNIX: `/usr/openv/volmgr/bin/tpext -loadEMM`

Windows: *`install_path`*`\Volmgr\bin\tpext -loadEMM`

8 If you used the `nbdb_move` command to relocate NetBackup database files, re-create the directories where the files were located when you backed up the catalog.

9 Start the device manager, as follows:

UNIX: `/usr/openv/volmgr/bin/ltid -v`

Windows: Start the device manager service.

10 Run the following command on the master server to recover NBDB from staging:

UNIX: `/usr/openv/netbackup/bin/nbdb_restore -dbn NBDB -recover -staging`

Windows: *install_path*`\NetBackup\bin\nbdb_restore -dbn NBDB -recover -staging`

11 Stop and restart NetBackup, as follows:

UNIX:

```
/usr/openv/netbackup/bin/bp.kill_all
/usr/openv/netbackup/bin/bp.start_all
```

Windows:

```
install_path\NetBackup\bin\bpdown
install_path\NetBackup\bin\bpup
```

About processing the relational database in staging

A recovery of the NetBackup image files and configuration files also restores the NetBackup relational database (NBDB) to the staging directory. You can use the following NetBackup commands to further process the NBDB database if required:

`cat_import`	Use `cat_import` to import the image metadata that is in the legacy flat file format into an NBDB relational database. The NBDB database can be the actual production DB or an NBDB in a different NetBackup domain.
`cat_export`	Use `cat_export -staging` to extract the image metadata from the relational database. It writes the data to the `db.export` directory in the legacy flat file format. You can export all of the image metadata or a subset of the image metadata by client or backup ID. Then, you can use the `cat_import` command to insert the data into another NBDB database. *Another NBDB* can be the actual production DB or an NBDB in a different NetBackup domain.
`nbdb_restore -staging`	Use `nbdb_restore -staging` to recover the relational database from the staging directory. See "Recovering the NetBackup relational database files from staging" on page 260.

`nbdb_unload -staging` Use `nbdb_unload -staging` to unload the media table and related tables to a set of flat files. Then, you can use SQL tools to insert the subset of data into another NBDB. *Another NBDB* can be the actual production DB or an NBDB in a different NetBackup domain.

Warning: Symantec recommends that you do not manipulate or process the NetBackup relational database unless directed to do so by a Symantec Support Representative. For help with NetBackup domain merges and splits, contact the Symantec Information Management Consulting Services.

More information about the commands is available.

See the *NetBackup Commands Reference Guide*.

Recovering the NetBackup catalog when NetBackup Access Control is configured

If you have configured NetBackup Access Control (NBAC), the online, hot catalog backup automatically backs up your authentication information and authorization configuration information.

Both the Operate and Configure permission sets are required on the catalog object to successfully back up and recover NBAC authentication and authorization data.

Separate recovery procedures exist based on operating system, as follows:

- UNIX: See Table 8-4 on page 264.
- Windows: See Table 8-5 on page 265.

Table 8-4 To recover the NetBackup catalog on UNIX when NetBackup Access Control is configured

Step	Task	Procedure
Step 1	If recovering to a master server on which NBAC is configured and operational, disable NBAC (that is, set it to PROHIBITED mode).	See the *NetBackup Security and Encryption Guide*.
Step 2	Recover the NetBackup catalog from the online catalog backup using the Catalog Recovery Wizard or the `bprecover` command.	See "About recovering the entire NetBackup catalog" on page 232.
Step 3	Configure NetBackup to use NBAC by setting it to AUTOMATIC or REQUIRED as per the security level desired.	See the *NetBackup Security and Encryption Guide*.

Table 8-4 To recover the NetBackup catalog on UNIX when NetBackup Access Control is configured *(continued)*

Step	Task	Procedure
Step 4	Restart NetBackup.	`/usr/openv/netbackup/bin/bp.kill_all` `/usr/openv/netbackup/bin/bp.start_all`

Table 8-5 To recover the NetBackup catalog on Windows when NetBackup Access Control is configured

Step	Task	Procedure
Step 1	If recovering to a master server on which NBAC is configured and operational, disable NBAC (that is, set it to PROHIBITED mode).	See the *NetBackup Security and Encryption Guide*.
Step 2	Stop the NetBackup services.	*install_path*`\Veritas\NetBackup\bin\bpdown.exe`
Step 3	In Windows, change the start-up type of the NetBackup Authentication Service and NetBackup Authorization Service to Disabled.	See the Microsoft documentation.
Step 4	Start the NetBackup services.	*install_path*`\Veritas\NetBackup\bin\bpup.exe`
Step 5	Recover the NetBackup catalog from the online catalog backup using the Catalog Recovery Wizard or the `bprecover` command.	See "About recovering the entire NetBackup catalog" on page 232.
Step 6	In Windows, change the start-up type of the NetBackup Authentication Service and NetBackup Authorization Service to Automatic.	See the Microsoft documentation.
Step 7	Configure NetBackup to use NBAC.	The procedure depends on the environment, as follows: ■ For recovery in an existing environment, set NBAC to AUTOMATIC or REQUIRED as per the security level desired. ■ For recovery to a new installation, configure NBAC by using the `bpnbaz -setupmaster` command and option. See the *NetBackup Security and Encryption Guide*.
Step 8	Restart NetBackup.	*install_path*`\Veritas\NetBackup\bin\bpdown.exe` *install_path*`\Veritas\NetBackup\bin\bpup.exe`

See "About recovering the NetBackup catalog" on page 228.

Recovering the NetBackup catalog from a nonprimary copy of a catalog backup

By default, catalog backup can have multiple copies, and the catalog is recovered from the primary backup copy. The primary copy is the first or the original copy. However, you can recover from a copy other than the primary.

Note: You must be logged on to the master server on which you want to recover the catalog. You cannot change server while running the **NetBackup Administration Console** on a different host and then run the wizard.

Note: You must have root (administrative) privileges to perform these procedures.

To recover the catalog from a non-primary copy

1. If the copy of the catalog backup is on a medium other than tape, do the following:

   BasicDisk — Make sure that the disk that contains the backup is mounted against the correct mount path (as displayed in the disaster recovery file).

   Disk pool — For a catalog backup file in a disk pool, do the following:

   - Create the disk storage server for the storage by using the **Storage Server Configuration Wizard**.
   - Create the disk pool for the storage by using the **Disk Pool Configuration Wizard**.
   - Run the following command to synchronize the disaster recovery file to the new disk pool.

     ```
     nbcatsync -sync_dr_file disaster_recovery_file
     ```

2. Run the following NetBackup command to recover the catalog:

   ```
   bprecover –wizard –copy N
   ```

   N is the number of the copy from which you want to recover.

Recovering the NetBackup catalog without the disaster recovery file

If the disaster recovery file has been lost, consult the email that was sent to the administrator when the catalog was backed up. The disaster recovery file is written to the location you specify in the catalog backup policy and is appended to the backup stream itself.

To recover the catalog without the disaster recovery file

1. The email identifies the media that contains the disaster recovery file, and the media that was used to back up critical policies. Ensure that this media is available.
2. Follow the normal catalog recovery steps until the point where the **Catalog Recovery Wizard** or `bprecover` command is called for.
3. Run the following command to retrieve all disaster recovery files from the catalog backup media:

   ```
   bpimport -drfile -id media_id -drfile_dest
   fully_qualified_dir_name
   ```

   This command recovers all disaster recovery files from the specified media ID and places them in the specified directory. The ID can be either a tape media ID or the fully qualified location of a disk storage unit.
4. Verify that the correct disaster recovery file is available in the specified directory and that it is available from the NetBackup master server.
5. Continue with the normal catalog recovery procedure by running the **Catalog Recovery Wizard** or `bprecover` command, providing the disaster recovery file location when prompted.

   Refer to the email as your primary source for recovery instructions, because they are the most current instructions for recovering your catalog. The instructions are sent when the catalog backup is completed, or when a catalog backup image is duplicated.

   Note: If you restore catalog files directly by using `bprestore` on a Solaris system, use the following path: `/opt/openv/netbackup/bin/bprestore`.

   The name of the online catalog backup policy is **CatalogBackup**. The email is written to the following file:

   ```
   /storage/DR/CatalogBackup_1123605764_FULL.
   ```

   The file name itself indicates if the backup was full or not.

   See “NetBackup disaster recovery email example” on page 267.

NetBackup disaster recovery email example

The following is an example of a disaster recovery email after a successful catalog backup:

```
From: Netbackup.HostName@HostName
Sent: Monday, January 2, 2012 1:26 PM
To: NetBackup Administrator
Subject: NetBackup Catalog Backup successful on host HostName

status 0

Server
HostName

Date
 Sun Jan 1 13:05:44 2012

Policy
 hot

Catalog Backup Status
 the requested operation was successfully completed (status 0).

DR image file:
 /backup/dr/hot_1305655567_FULL

To ensure that the NetBackup catalog data is protected through Tue
May 17 13:05:44 2011 , retain a copy of the attached file, and the
media  or files listed below:

Catalog Recovery Media
 Media Server  Disk Image Path                      Image File Required
 * HostName  /backup/nb/HostName_1305655547_C1_F1  hot_1305655547_FULL
 * HostName  /backup/nb/HostName_1305655567_C1_F1  hot_1305655567_FULL
 * HostName  /backup/nb/HostName_1305655567_C1_TIR hot_1305655567_FULL

DR file written to
 /backup/dr/hot_1305655567_FULL

* - Primary Media


Catalog Recovery Procedure for the Loss of an Entire Catalog

You should create a detailed disaster recovery plan to follow should it
become necessary to restore your organization's data in the event of
a disaster.  A checklist of required tasks can be a tremendous tool in
```

assisting associates in triage. For example, after the facility is safe for data to be restored, the power and data infrastructure need to be verified. When these tasks are completed, the following scenarios will elp to quickly restore the NetBackup environment, and in turn, restore applications and data.

Disaster Recovery Procedure using the DR Image File

In the event of a catastrophic failure, use the following procedure to rebuild the previous NetBackup environment.

Note: If new hardware is required, make sure that the devices contain drives capable of reading the media and that the drive controllers are capable of mounting the drives.

1. Install NetBackup.
2. Configure the devices necessary to read the media listed above.
3. Inventory the media.
4. Make sure that the master server can access the attached DR image file. Start the NetBackup Recovery Wizard from the NetBackup Administration Console. Or, start the wizard from a command line by entering bprecover -wizard.

Disaster Recovery Procedure without the DR Image File

NOTE: ONLY ATTEMPT THIS AS A LAST RESORT If you do not have the attachment included with this email, use the following instructions to recover your catalog (If using OpenStorage disk pools, refer to the Shared Storage Guide to configure the disk pools instead of step 2 and 3 below):

1. Install NetBackup.
2. Configure the devices necessary to read the media listed above.
3. Inventory the media.
4. Run:
   bpimport -create_db_info [-server name] -id /backup/nb
5. Run:
   cat_export -client *HostName*
6. Go to the following directory to find the DR image file hot_1305655567_FULL:
   /usr/openv/netbackup/db.export/images/*HostName*/1305000000
7. Open hot_1305655567_FULL file and find the BACKUP_ID (for example: *HostName*_1305655567).

8. Run:
   bpimport [-server name] -backupid *HostName*_1305655567
9. Run:
   bprestore -T -w [-L progress_log] -C *HostName* -t 35
    -p hot -X -s 1305655567 -e 1305655567 /
10. Run the BAR user interface to restore the remaining image database if the DR image is a result of an incremental backup.
11. To recover the NetBackup relational database, run:
    bprecover -r -nbdb
12. Stop and Start NetBackup
13. Configure the devices if any device has changed since the last backup.
14. To make sure the volume information is updated, inventory the media to update the NetBackup database.

Recovering a NetBackup user-directed online catalog from the command line

This procedure recovers the catalog manually through the command line interface (CLI) without a Phase 1 import when the disaster recovery (DR) file is available. You must have root (administrative) privileges to perform this procedure.

Note: Use this procedure only if you want to restore the minimal NetBackup catalog information that lets you begin to recover critical data.

To recover the user-directed online catalog from the command line interface

1. Verify the location of the disaster recovery files that are created from Full and Incremental Hot Catalog backups. These files can be stored in a specified path of the file system on the master server and in email attachments to the NetBackup administrator.
2. Set up each master server and media server in the same configuration as the configuration that is used during the last catalog backup. The master server and media servers have the following same properties as the backed up catalog configuration: name, NetBackup version, operating system patch level, and path to storage devices.

   Configure any devices and volumes you may need for the recovery.

3 Locate the latest DR image file corresponding to the backup that are used for recovery. Open the file in an editor and find values for the following:

`master_server`	Use the exact name that is specified in NetBackup configuration for the master server .
`media_server`	The location of the robot or disk storage unit that is used for catalog backup.
`timestamp`	The four most significant digits in the DR file name and six zeroes attached.
`media`	The location of the catalog backup media as specified by the disaster recovery file under the FRAGMENT keyword.
`backup_id`	Found in the DR file under BACKUP_ID.

Example:

file: Hot_Backup_1122502016_INCR

timestamp: 1122000000

4 Create the DR recovery directory on the master server.

UNIX and Linux:

`/usr/openv/netbackup/db/images/`*`master_server`*`/`*`timestamp`*`/tmp`

Windows:

`C:\Program Files\VERITAS\NetBackup\db\images\`*`master_server`*
`\`*`timestamp`*`\tmp`

Copy the DR file to the newly created directory.

5 Edit the DR file in `netbackup/db/images/`*`master_server`*`/`*`timestamp`*`/tmp` as follows:

- Change the value of IMAGE_TYPE to 1.
- Change the value of TIR_INFO to 0.
- Change the value of NUM_DR_MEDIAS to 0.
- Remove ALL lines containing DR_MEDIA_REC.

6 If your catalog recover media is on tape, run the `vmquery` command to assign the media to the media server.

```
vmquery -assigntohost media timestamp master_server
```

Example:

```
vmquery -assigntohost DL005L 1122000000 klingon
```

7 To recover the catalog .f file from the hot catalog backup, run a Phase II import on the media that is specified by the disaster recovery file .

```
bpimport -server master_server -backupid backup_id
```

8 If your catalog backup was incremental, recover all the other catalog backup images up to and including the most recent Full Catalog backup.

- Open the Backup, Archive, and Restore client interface for NetBackup. Select NBU-Catalog as the policy type. Set the source clients and destination clients to your master server.
- Search the backups and restore all files that are located in the following directory:

  install_path/netbackup/db/images/*master_server*

- Verify that all files are restored successfully on the master server.

9 Restore your critical data by using the Backup, Archive, and Restore client interface or the command line.

- Restore the catalog backup images for each media server which requires data recovery.
- To restore the backup images, select NBU-Catalog as the policy type. Source and destination clients should be your master server. Refresh your view in the BAR GUI. Traverse the file system for the master server to the following:

  install_path/netbackup/db/images

  Restore the images for each configured media server. Verify that your images are present by searching for them in the catalog.

10 Recover backup data from each media server in the previous step. Change the Policy Type, Source, and Destination client to match the client that is used to back up the desired data. Select the desired files from the Backup, Archive, and Restore client interface and restore them.

11 To recover the NetBackup relational database, run the following:

```
bprecover -r -nbdb
```

This command restores NetBackup media usage information, ensure that media containing backups are not overwritten, and restore the storage unit configuration.

You cannot recover the NetBackup relational database to a configuration that is not identical to the configuration on which the catalog was backed up. Instead, you must import each piece of backup media.

12 If your catalog recovery media is on tape, freeze the media that contains the catalog backup that is used for recovery. This action protects the media from being reused:

```
bpmedia -freeze -m media -h master_server
```

Run `bpmedialist` to verify that the media is frozen.

13 Recover your policies and configuration data on each master server and media server.

Before recovering NetBackup policy files, ensure that you have recovered all of your critical data, or protected the media that contains your critical data. When policy information is recovered, NetBackup starts to run the scheduled jobs that may overwrite the media that was written after the last catalog backup.

Open the Backup, Archive, and Restore client interface for NetBackup and select NBU-Catalog as the policy type.

For each server to be restored, set the source clients and destination clients to your server, starting with the master server.

Restore all files that are backed up by the hot catalog backup on each server.

14 Stop and restart the NetBackup services.

Restoring files from a NetBackup online catalog backup

Because the online catalog backup uses the standard backup format, you may recover specific files using the NetBackup Backup, Archive, and Restore user interface. Restoring catalog files directly to their original location may cause inconsistencies in the NetBackup catalog or cause NetBackup to fail. Instead, you should restore catalog files to an alternate location.

To restore files from an online catalog backup

1. From the **Specify NetBackup Machines and Policy Type** menu, select the **NBU-Catalog** policy type.
2. Specify the master server as the source client for the restore.
3. Select the catalog files to restore.

Unfreezing the NetBackup online catalog recovery media

This procedure shows how to unfreeze your online catalog recovery media.

To unfreeze the online catalog recovery media

1. On the master server, go to the image database. In the master server's portion of the image catalog, locate the catalog backup image file from which the recovery was made, as follows:

   a. Identify the associated catalog backup parent image file by viewing the `PARENT_IMAGE_ID` value.

   b. Identify the media that the catalog backup was written to by viewing the second to last field in the `DR_MEDIA_REC` line(s).

   c. Save the catalog backup parent image file that was identified in the first substep.

   d. Relocate or remove all other image files that relate to the catalog backup policy.

2. On the master server, for each media that is identified in step 1b, run the following command:

   ```
   bpimport -create_db_info -server server_name -id media_id
   ```

3. On the master server, run the following command:

   ```
   bpimport
   ```

4. On the master server, for each media that is identified in step 1b, run the following command:

   ```
   bpmedia -unfreeze -m media_id -h server_name
   ```

Importing backup images, Phase I

Phase I of the import process creates a list of images from which to select to import in Phase II. No import occurs in Phase I.

Initiate an import by using either the Import Images Wizard or initiate it manually.

If tape is used, each tape must be mounted and read. It may take some time to read the catalog and build the list of images.

To import a catalog backup, import all of the child jobs that were used to create the catalog backup.

To import backup images by using the Import Images Wizard, Phase I (Windows only)

1. If you import Backup Exec media, run the NetBackup `vmphyinv` physical inventory utility to update the Backup Exec media GUID in the NetBackup Media Manager database. Run the command only once after creating the media IDs in the NetBackup Media Manager database.
2. Add the media IDs that contain the Media Manager backups to the server where the backups are to be imported.
3. In the **NetBackup Administration Console** left pane, select **NetBackup Management**.
4. Select **Import Images** in the right pane to launch the wizard. **Import Images** is available when **Master Server** or **NetBackup Management** is selected.
5. The wizard explains the two-step import process and takes you through Phase I. Click **Next**.
6. In the **Media Host** field, type the name of the host that contains the volume to import. Click **Next**.

   This media server becomes the media owner.
7. In the **Image Type** field, select whether the images to import are on tape or disk.
8. Depending on whether the import is from tape or disk do one of the following:
   - Type the Media ID for the volume that contains the backups to import.
   - For disk storage, select the **Disk Type**. If **BasicDisk** type, enter the path from which the images are to be imported.

     Click **Next**.

   If the Backup Exec media is password-protected , the job fails without a correct password. The logs indicate that either no password or an incorrect password was provided. If the media is not password-protected and the user provides a password, the password is ignored.

   To import Backup Exec media if the password contains non-ASCII characters do the following:

- Use the **NetBackup Administration Console** on Windows. (You cannot use the **NetBackup-Java Administration Console**.)
- Use the `bpimport` command.

9 For disk pool storage only, select the disk pool and the disk volume ID and then click **Next**.

10 Click **Finish**. The wizard explains how to check the progress as the media host reads the media.

11 Continue to Phase II to complete the import.

See "Importing backup images, Phase II" on page 276.

To initiate an import (UNIX only)

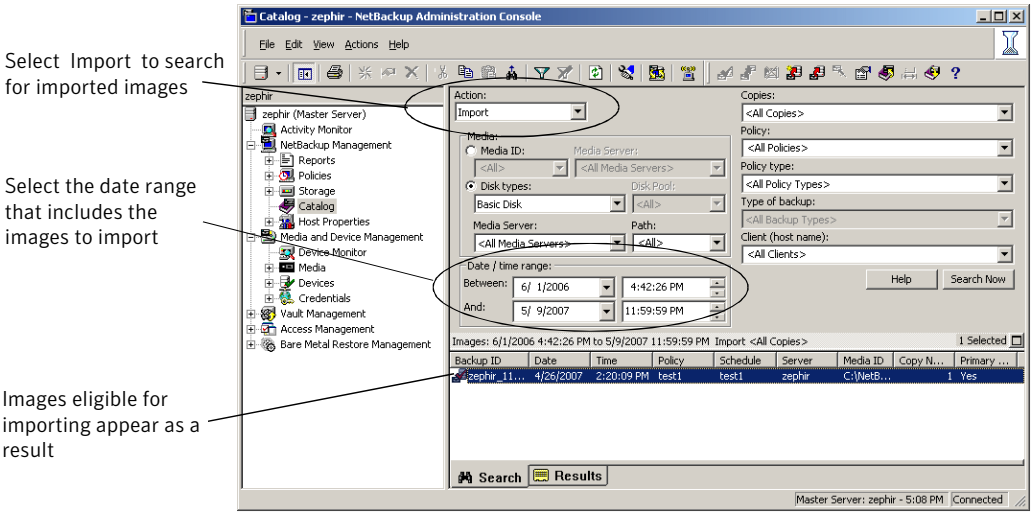
- To import Backup Exec media, run the `vmphyinv` physical inventory utility to update the Backup Exec media GUID in the NetBackup Media Manager database. Run the command only once after creating the media IDs in the NetBackup Media Manager database.

Importing backup images, Phase II

To import the backups, first run the Initiate Import (Import Phase I). The first phase reads the catalog to determine all of the media that contain the catalog backup images. After Phase I, start the Import (Phase II). If Phase II is run before Phase I, the import fails with a message. For example, Unexpected EOF or Import of backup ID failed, fragments are not consecutive.

To import backup images, Phase II

1. In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Catalog**.
2. In the right pane, set up the search criteria to find images available to import by setting the search action to **Import**. Be sure to select a date range that includes the images you want to import.



3. Select the image(s) you want to import and on the **Actions** menu, select **Actions > Initiate Import**.

   The **Initialize Import** dialog box appears.
4. Ensure that the **Use Import Images Wizard** check box is clear. Complete the **Initialize Import** dialog box and then click **OK**.
5. To view the log, click the **Results** tab, then select the import job log.

Appendix A

Backup and restore functional overview

This appendix includes the following topics:

- About backup and restore functional overview
- Backup and restore startup process
- Backup and archive processes
- Backups and archives - UNIX clients
- About UNIX client restoration
- About SAN client restoration
- About Windows client restoration
- About catalog backup restoration
- NetBackup directories and files
- NetBackup programs and daemons
- NetBackup catalogs

About backup and restore functional overview

This appendix provides a functional overview of NetBackup backup and restore operations for both UNIX and Windows. The discussions include descriptions of important services or daemons and programs, and the sequence in which they execute during backup and restore operations. The databases and the directory structure of the installed software are also described.

Backup and restore startup process

When the NetBackup master server starts up, a script automatically starts all services, daemons, and programs that are required by NetBackup. (The start-up commands that are used by the script vary according to the platform.)

The same is true on a media server. NetBackup automatically starts additional programs as required, including robotic daemons.

For more information about SAN client and Fibre Transport startup processes, see the NetBackup SAN Client and Fibre Transport Guide.

Note: No daemons or programs need to be explicitly started. The necessary programs are started automatically during the backup or restore operation.

A daemon that executes on all servers and clients is the NetBackup client daemon, `bpcd`. On UNIX clients, `inetd` starts `bpcd` automatically so no special actions are required. On Windows clients, `bpinetd` performs the same functions as `inetd`. Netware clients do not use `inetd` or `bpinetd` but are configured to start the `bpcd` NLM (`bpcd.nlm`) automatically. An NLM (NetWare Loadable Module) is similar to a service.

Note that all NetBackup processes on UNIX can be started manually by running the following:

```
/usr/openv/netbackup/bin/bp.start_all
```

Backup and archive processes

The backup processes and archive processes vary depending on the type of client. The following explains the various NetBackup processes involved in backups and restores including snapshot, SAN client, synthetic backup, and NetBackup catalog backup.

The job scheduler processes consist of the following:

- The `nbpem` service (Policy Execution Manager) creates policy-client tasks and determines when jobs are due to run. It starts the job and upon job completion, determines when the next job should run for the policy-client combination.
- The `nbjm` service (Job Manager) does the following:
  - Accepts requests from `nbpem` to run backup jobs or media jobs from commands such as `bplabel` and `tpreq`

- Requests resources for each job, such as storage units, drives, media, and client and policy resources.
- Executes the job and starts the media server processes.
- Fields updates from the media server `bpbrm` process and routes them to the jobs database and the images database.
- Receives preprocessing requests from `nbpem` and initiates `bpmount` on the client.

- The `nbrb` service (Resource Broker) does the following:
  - Allocates resources in response to requests from `nbjm`.
  - Acquires physical resources from the Enterprise Media Manager service (`nbemm`).
  - Manages logical resources such as multiplex groups, maximum jobs per client, and maximum jobs per policy.
  - Initiates drive unloads and manages pending request queues.
  - Queries media servers periodically for current drive state.

The NetBackup master server and the Enterprise media manager (EMM) server are on the same physical host.

The master server is responsible for running jobs as configured in NetBackup policies by using the `nbpem` and `nbjm` services.

The EMM server allocates resources for a single master server. It is the repository for all device configuration information. The EMM server uses the `nbemm` service and the `nbrb` service for device and resource allocation.

Backups and archives - UNIX clients

For UNIX clients, NetBackup supports scheduled, immediate manual, and user-directed backups of both files and raw partitions. User-directed archives of files are also supported; raw partition archives are not supported. When the operations start, they are all similar to the extent that the same daemons and programs execute on the server.

Each type of backup is started differently as follows:

- Scheduled backups begin when the `nbpem` service detects that a job is due. It checks the policy configurations for the scheduled client backups that are due.
- Immediate manual backups begin if the administrator chooses this option in the NetBackup Administration Console or runs the `bpbackup -i` command. This

action causes bprd to contact nbpem, which then processes the policy, client, and schedule that the administrator selects.

- User-directed backups or archives begin when a user on a client starts a backup or archive through the user interface on the client. The user can also enter the bpbackup or bparchive command on the command line. This action invokes the client's bpbackup or bparchive program, which sends a request to the request daemon bprd on the master server. When bprd receives the user request, it contacts nbpem, which checks the policy configurations for schedules. By default nbpem chooses the first user-directed schedule that it finds in a policy that includes the requesting client.
  For user-directed backups or archives, it is also possible to specify a policy and schedule. A description is available of the UNIX BPBACKUP_POLICY and BPBACKUP_SCHED options in bp.conf and the Windows equivalents.
  For more information, see the NetBackup Administrator's Guide, Volume I.

Backup process

This topic uses a diagram and a table to describe each step of a backup process. PBX (not shown in the diagram) must be running for NetBackup to operate.

See "Resolving PBX problems" on page 73.

The process for a multiplexed backup is essentially the same as a non-multiplexed backup. An exception is that a separate bpbrm process and bptm process is created for each backup image being multiplexed onto the media. NetBackup also allocates a separate set of shared memory blocks for each image. The other client and server processes for multiplexed backups are the same.

Figure A-1 illustrates the various operations that comprise the backup process.

Figure A-1 Backup or archive to tape or disk

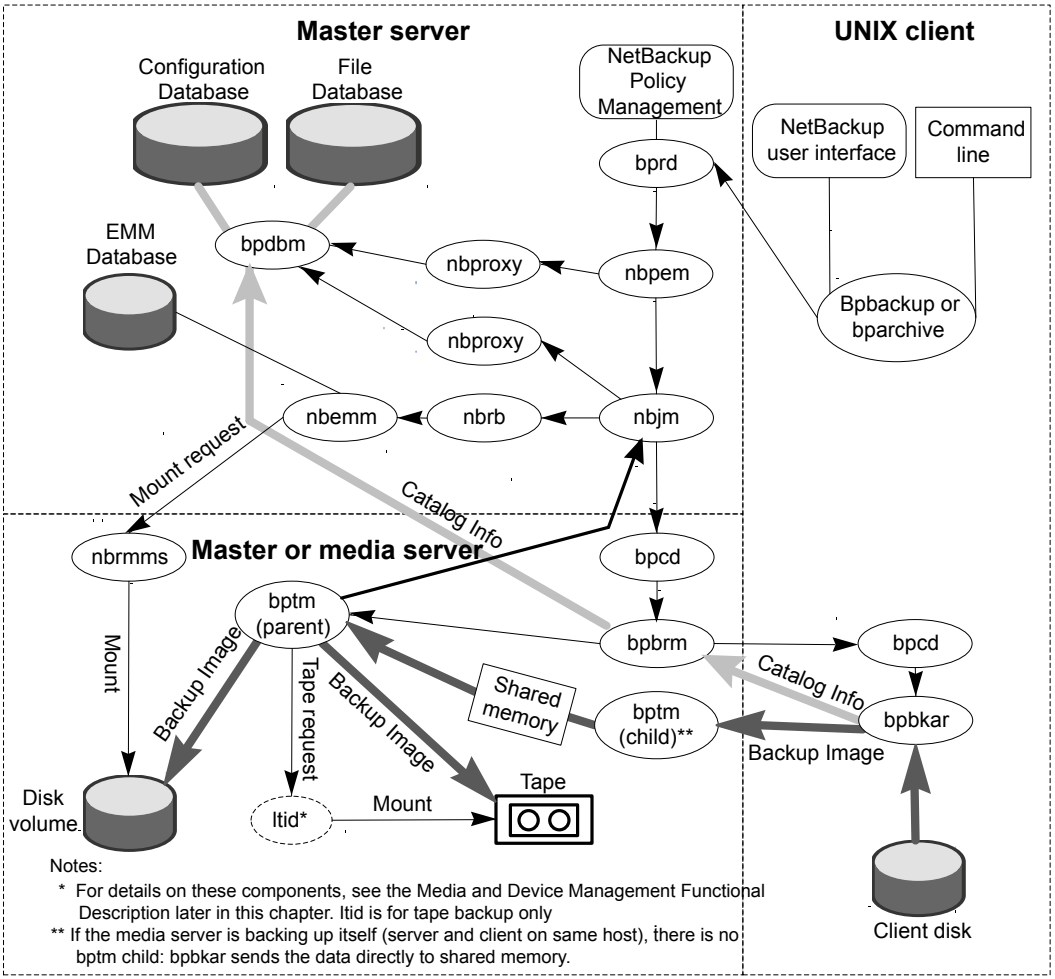


Table A-1 shows the sequence of operation of a backup process.

Table A-1 Backup to tape or disk sequence of operation

Agent	Action
Start-up script	Launches `bprd` on the master server and `ltid` on the master server and all media servers. All other daemons and programs are started as necessary including `nbpem`, `nbjm`, `nbrb`, and `nbemm`.

Table A-1 Backup to tape or disk sequence of operation *(continued)*

Agent	Action
Policy execution manager service (nbpem)	Gets the policy list from bpdbm. Creates a policy-client task for all policy-client combinations specified in the policy list. Computes the due time for each policy-client task (policy priority is honored for internal processing). Submits to nbjm all jobs as policy-client tasks become due. When a job finishes, it recomputes the due time of that policy-client task.
Job manager service (nbjm)	Issues a single request (with a request ID) to `nbrb`, for all resources that are required by a job. `nbrb` gets the storage unit, tape drive, and media ID information from `nbemm` and allocates client and policy resources. `nbrb` returns to `nbjm` an allocation sequence that contains one allocation for each resource (each allocation contains a unique ID). `nbrb` also returns allocation data for the specific resource type. `nbrb` also returns the request ID along with the allocations so that `nbjm` can correlate the response with the right request (and job). Note that `nbrb` allocates all resources that are included in a request. If the resources are temporarily unavailable the request is queued in `nbrb`. If the resource cannot be allocated, `nbrb` fails the request. `nbjm` starts the backup by using the client daemon `bpcd` to start the backup and restore manager `bpbrm`. For normal backup (not snapshots), `nbjm` starts `bpbrm` on the media server, which may or may not be the same system as the master server.
Backup and restore manager (bpbrm)	Starts `bptm`. Starts the actual backup (or archive) by using the client daemon `bpcd` to start the backup program and archive program `bpbkar` on the client.

Table A-1 Backup to tape or disk sequence of operation *(continued)*

Agent	Action
Backup and archive manager (bpbkar)	Sends the information about files within the image to `bpbrm`, which directs the file information to the NetBackup image database and the jobs database. The information is sent by means of `bpbrm` to `nbjm`. Transmits the backup image to `bptm` depending on one of the following: whether the media server backs up itself (`bptm` and `bpbkar` are on the same host) or back ups a client that resides on a different host. If the media server backs up itself, `bpbkar` stores the image block-by-block in shared memory on the media server. If the media server backs up a client on a different host, the `bptm` process on the server creates a child process of itself. The child receives the image from the client by means of socket communications and then stores the image block-by-block in shared memory on the server. Use the NOSHM file to force a media server that backs up itself to do the following: create a child process and use socket communications, as though the client is on a different host. More information on the NOSHM file is available. See the NetBackup Backup Planning and Performance Tuning Guide.

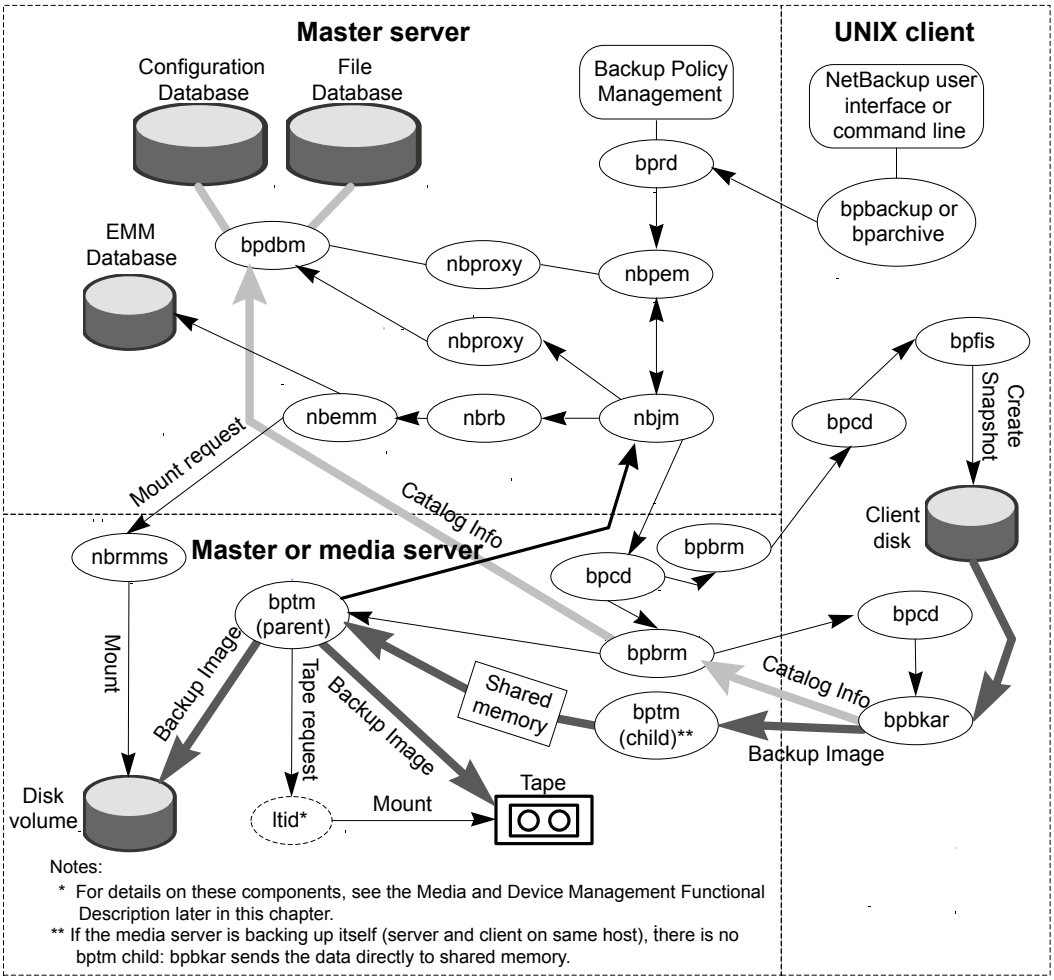
Table A-1 Backup to tape or disk sequence of operation *(continued)*

Agent	Action
backup manager for tape (bptm) or disk (bpdm)	The `bptm` process on the server takes the image from shared memory and directs it to the storage media, which can be disk, tape, or both disk and tape. The `bpdm` process manages and cleans up the disk images. If the storage media is tape, `bptm` requests information for the first media and drive to use, by exchanging information with `nbjm`. `bptm` sends mount requests for specific media and drives to the NetBackup Device Manager (`ltid`). This action causes the media to be mounted on the appropriate devices. If, during the backup, a tape span is required, `bptm` again exchanges information with `nbjm` to release the correct tape and to get another one. nbjm exchanges information with `nbrb` to accomplish this function. For AdvancedDisk and OpenStorage, `bptm` requests the volume from `nbjm`. `nbjm` then passes the request to `nbemm` to choose the volume server and media server to use. The `nbemm`service calls `nbrmms` on the media server that was chosen to mount the volume. For BasicDisk, `bptm` writes the images to the path that is configured in the disk storage unit. The system disk manager controls the actual writing of data. In the case of an archive, `bpbrm` deletes the files from the client disk after the files are successfully backed up.
Job manager service (nbjm)	Receives the completion status of the job from `bpbrm`. Releases the resources to `nbrb` and returns the status to `nbpem`.

Snapshot backup and Windows open file backups

Figure A-2 shows the overall snapshot backup process. PBX (not shown in the diagram) must be running for NetBackup to operate.

Figure A-2 Snapshot backup and Windows open file backup using multiple data streams



A separate parent job creates all snapshots followed by a child job that backs up the snapshot. An exception is when Windows opens file backups that do not use multiple data streams.

The following sequence of operation is for snapshot creation and backup that includes Windows open file backups that employ multiple data streams:

- The NetBackup master server or primary client initiates the backup. This action causes the NetBackup request daemon `bprd` to submit a backup request to the Policy Execution Manager `nbpem`. `nbpem` processes the policy configurations.

- nbpem (through nbjm) starts a parent job to create the snapshot. This job is separate from the job that backs up the snapshot.
- nbjm starts an instance of bpbrm through bpcd on the media server, and bpbrm starts bpfis through bpcd on the client.
- bpfis creates a snapshot of the client's data by means of a snapshot method.
- When bpfis is finished, it sends snapshot information and completion status to bpbrm and exits. bpbrm, in turn, reports the snapshot information and status to nbjm and exits. nbjm relays the information and status to nbpem.
- nbpem submits a child job for the backup to nbjm, with a file list derived from the snapshot information. nbjm starts bpbrm to back up the snapshot.
- bpbrm starts bpbkar on the client. bpbkar sends the file catalog information to bpbrm, which relays it to the NetBackup file database bpdbm on the master server.
- bpbrm starts the process bptm (parent) on the media server.
- The next step depends on whether the media server backs up itself (bptm and bpbkar are on the same host) or the media server backs up a client that resides on a different host. If the media server backs up itself, bpbkar stores the snapshot-based image block by block in shared memory on the media server. If the media server backs up a client that resides on a different host, bptm on the server creates a child process of itself. The child receives the snapshot-based image from the client by means of socket communications and then stores the image block-by-block in shared memory.
- The original bptm process then takes the backup image from shared memory and sends it to the storage device (disk or tape).
  Information is available on how the tape request is issued.
  See "Media and device management process" on page 326.
- bptm sends backup completion status to bpbrm, which passes it to nbjm.
- When nbpem receives backup completion status from nbjm, nbpem tells nbjm to delete the snapshot. nbjm starts a new instance of bpbrm on the media server, and bpbrm starts a new instance of bpfis on the client. bpfis deletes the snapshot on the client, unless the snapshot is of the Instant Recovery type, in which case it is not automatically deleted. bpfis and bpbrm report their status and exit.
  For more information, see the NetBackup Snapshot Client Administrator's Guide.
  Note that Windows open file backups do not require Snapshot Client.

SAN client

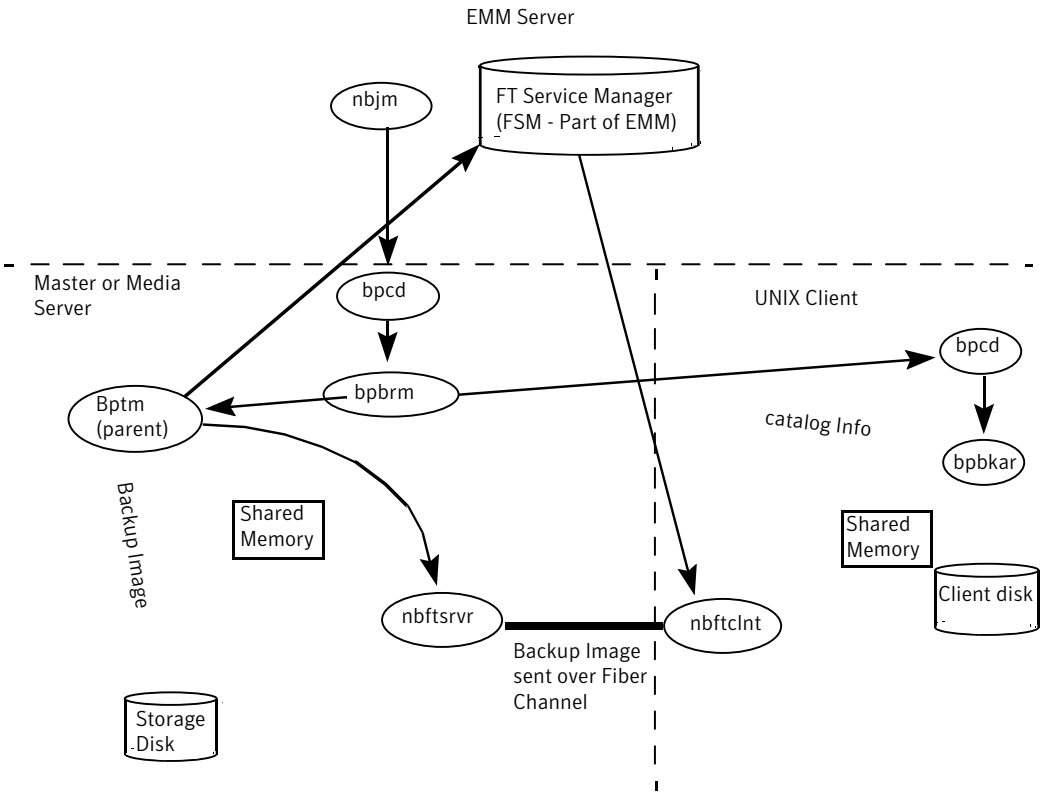
For backups to disk, the SAN Client feature provides high-speed data movement between NetBackup media servers and NetBackup SAN-attached clients. SAN-attached clients send backup data to the media server by means of fibre channel connections.

As part of SAN Client, the FT Service Manager (FSM) is a domain layer service that resides on the EMM server. The FSM provides discovery, configuration, and event monitoring of SAN Client resources. The FSM collects fibre channel information from the client and from the media server; FSM then populates the NetBackup relational database (NBDB) with the information. FSM runs as a sub-process of NBDB and writes log messages to the NBDB log. FSM interacts with the `nbftclnt` process on NetBackup clients and with the `nbftsrvr` process on media servers.

The initial stages of a backup are the same as shown in Figure A-1

Figure A-3 shows the server and client components that are unique to SAN client backup over Fibre Channel.

Figure A-3 SAN client backup over Fibre Transport



The process flow for a SAN Client backup is as follows (in the order presented):

- A start-up script launches `bprd` on the master server and `ltid` on the master server and all media servers.
  All other daemons and programs are started as necessary including `nbpem`, `nbjm`, `nbrb`, and `nbemm`.
- The policy execution manager service (nbpem) does the following:
  - Gets the policy list from bpdbm.
  - Builds a work list of all scheduled jobs.
  - Computes the due time for each job.
  - Sorts the work list in order of due time.
  - Submits to nbjm all jobs that are currently due.
  - Sets a wakeup timer for the next due job.

    - When the job finishes, re-computes the due time of the next job and submits to nbjm all jobs that are currently due.
- The job manager service (nbjm) requests backup resources from the resource broker (nbrb), which returns information on the use of shared memory for SAN Client.
- The nbjm service starts the backup by means of the client daemon bpcd, which starts the backup and restore manager bpbrm.
- The bpbrm service starts bptm, which does the following:
    - Requests SAN Client information from nbjm.
    - Sends a backup request to the FT server process (nbftsrvr).
    - Sends a backup request to the FT Client process on the client (nbftclnt), which does the following: opens a fibre channel connection to nbftsrvr on the media server, allocates shared memory, and writes shared memory information to the backup ID file.
- The bpbrm service uses bpcd to start bpbkar, which does the following:
    - Reads the shared memory information from the BID file (waits for the file to exist and become valid).
    - Sends the information about files in the image to bpbrm.
    - Writes the file data to tar, optionally compresses it, then writes the data to the shared buffer.
    - Sets the buffer flag when the buffer is full or the job is done.
- FT Client process nbftclnt waits for the shared memory buffer flag to be set. It then transfers the image data to the FT Server (nbftsrvr) shared memory buffer, and clears the buffer flag.
- The nbftsrvr service waits for data from nbftclnt; and writes the data is written to the shared memory buffer. When the transfer completes, nbftsrvr sets the buffer flag.
- bptm waits for the shared memory buffer flag to be set, writes data from the buffer to the storage device, and clears the buffer flag.
- At the end of the job:
    - bpbkar informs bpbrm and bptm that the job is complete.
    - bptm sends bpbrm the final status of the data write.
    - bptm directs nbftclnt to close the fibre channel connection.
    - nbftclnt closes the fibre channel connection and deletes the BID file.

Backups and archives - Windows

NetBackup supports the same types of operations on Windows clients as it does on UNIX clients.

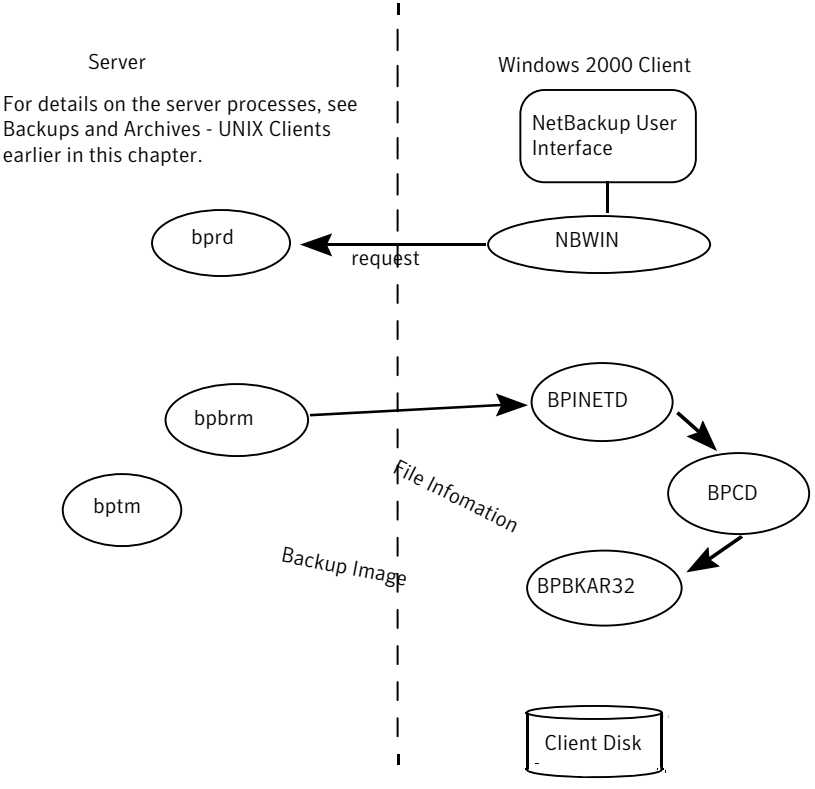
Figure A-4 shows the Windows client processes.

In this figure, the following items apply:

- NBWIN is the user interface program on the client. The bpbackup function and the bparchive function are merged into NBWIN.
- BPINETD serves the same purpose as inetd on UNIX clients.
- The NetBackup client daemon is called BPCD.
- BPBKAR32 serves the same purpose as bpbkar on UNIX clients.

The server processes are the same as described for UNIX.

Figure A-4 Backup and archive - Windows clients



Synthetic backups

The typical NetBackup backup process accesses the client to create a backup. A synthetic backup is a backup image created without using the client. Instead, a synthetic backup process creates a full or a cumulative incremental image by using only previously created backup images, called component images.

Note: Synthetic archives do not exist.

For example, an existing full image and subsequent differential incremental images may be synthesized to create a new full image. The previous full image and the incrementals are the component images. The new synthetic full image behaves like a backup that is created through the traditional process. The new synthetic full image is a backup of the client that is as current as the last incremental. The synthetic image is created by copying the most current version of each file from the most recent component image that contains the file. A synthetic backup must be created in a policy with the **True Image Restore with Move Detection** option selected. This option enables the synthetic backup to exclude the files that have been deleted from the client file system from appearing in the synthetic backup.

Like a traditional backup, `nbpem` initiates a synthetic backup. It submits a request to `nbjm` to start the synthetic backup process and `nbjm` then starts `bpsynth`, which executes on the master server. It controls the creation of the synthetic backup image and the reading of the files that are needed from the component images. If directory `bpsynth` exists in the debug log directory, additional debug log messages are written to a log file in that directory.

`bpsynth` makes a synthetic image in several phases:

Table A-2

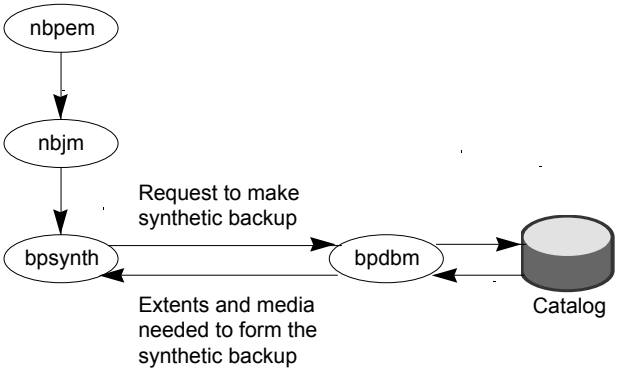
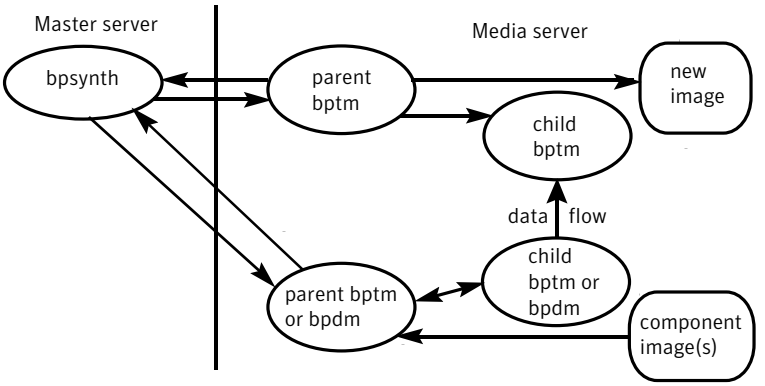
Phase	Description
1 - Prepare catalog information and extents	In phase 1, `bpsynth` makes a synthetic backup request to the database manager, `bpdbm`. It uses the entries and the TIR information from the catalogs of the component images to build the catalog for the new synthetic image. It also builds the extents to be copied from the component images to the synthetic image. The `bpdbm` service returns the list of extents to `bpsynth`. (An extent is the starting block number and the number of contiguous blocks within a specific component image.) A set of extents is typically copied from each component image onto the new synthetic image. The following figure shows how phase 1 operates: 
2 - Obtain resources	In phase 2, `bpsynth` obtains write resources (storage unit, drive, and media) for the new image. It also reserves all the read media containing component images and obtains the drive for the first media to be read. When the component images reside on BasicDisk, no resource reservation is done.

Table A-2 *(continued)*

Phase	Description
3 - Copy data	In phase 3, `bpsynth` starts the writer `bptm` (for tape and disk) on the media server to write the new synthetic image. It also starts a reader `bptm` (tape) or `bpdm` (disk) process for each component image on a media server that can access the component image. The reader process reads all extents for the component image. The following figure shows how phase 3 operates:  Note that `bpsynth` only starts the parent `bptm` (writer) and `bpdm` (reader) process on the media server. The parent in turn starts a child process. The parent and child communicate by means of buffers in shared memory. The `bpsynth` process sends the extents (starting block and count) for each component image to the corresponding child `bptm` or `bpdm` reader process. The parent `bptm` or `bpdm` reader process reads the data from the appropriate media into the shared buffers. The child `bptm` or `bpdm` reader process sends the data in the shared buffers to the child `bptm` writer process over a socket. The child `bptm` writer process writes the data into the shared buffers. The parent `bptm` writer process copies the data from the shared buffers to the media and notifies `bpsynth` when the synthetic image is complete.
4 - Validate the image	In phase 4, the `bpsynth` process validates the image. The new image is now visible to NetBackup and can be used like any other full or cumulative incremental backup. Synthetic backup requires that True Image Restore (TIR) with move detection be selected for each component image, and that the component images are synthetic images.

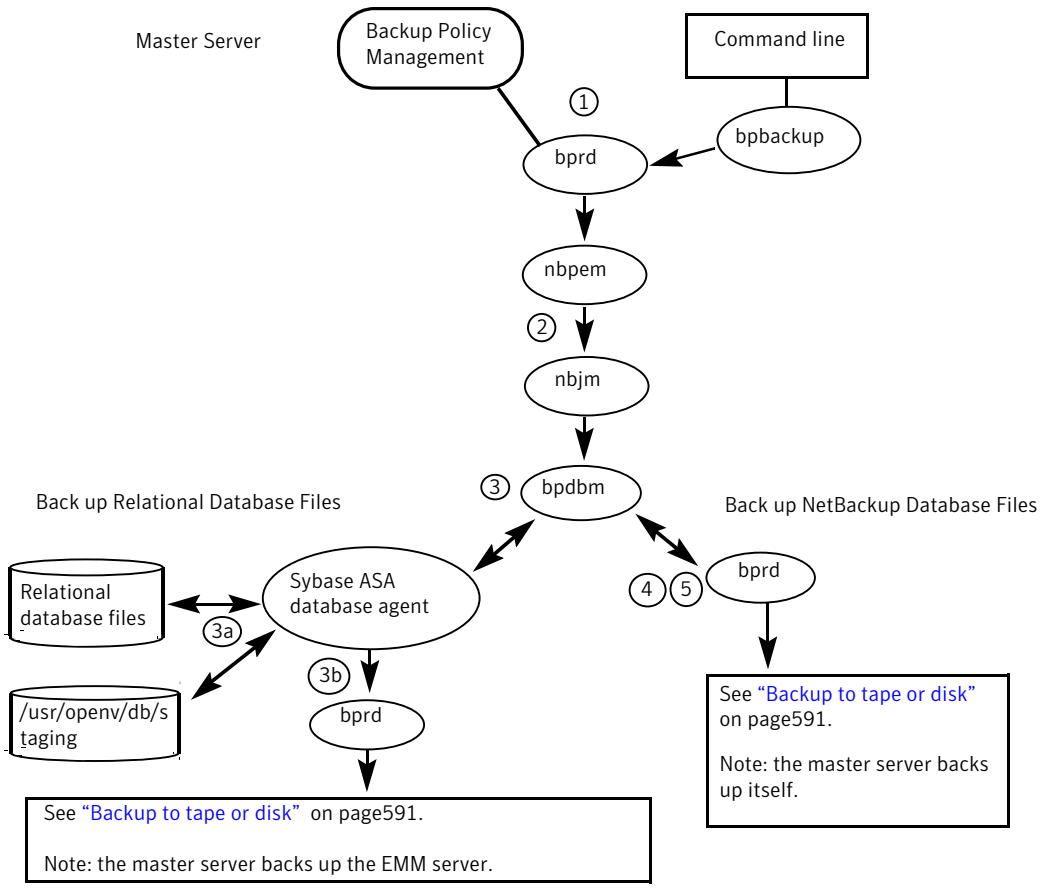
NetBackup hot catalog backup

Hot catalog backup is policy based, with all of the scheduling flexibility of a regular backup policy. This backup type is designed for highly active NetBackup environments where other backup activity usually takes place.

You can use an option in the Administration Console to start a manual backup of the NetBackup catalogs. Or, you can configure a NetBackup policy to automatically back up its catalogs.

Figure A-5 shows the hot catalog backup that is followed by the backup process itself.

Figure A-5 Hot catalog backup process



A hot catalog backup process is as follows (in the order presented):

- A manual backup or a catalog backup policy initiates the backup.
- nbpem submits a parent job to nbjm; nbjm sends a request to bpdbm.
- NetBackup initiates the following hot catalog backup jobs:
  - A parent job that is started manually by the administrator or by a catalog backup policy schedule.
  - A child job that copies NBDB to the staging directory and validates the information.
    The SQL Anywhere files database agent makes an online copy of the relational database files to /usr/openv/db/staging. See the Disaster Recovery chapter for a list of the relational database files.
  - A child job that backs up the NBDB database files.
    After the files are in the staging area, the SQL Anywhere database agent backs them up in the same manner as is used for an ordinary backup.
  - A child job that backs up the NetBackup database files (all files in /usr/openv/netbackup/db).
- NetBackup creates the disaster recovery file, and emails it to the administrator if the email option was selected in the policy.

Consult the following logs for messages on hot catalog backup:

- bpdbm, bpbkar, bpbrm, bpcd, bpbackup, bprd

For messages pertaining only to the relational database files, see the EMM server.log file and the bpdbm log file in the following directories:

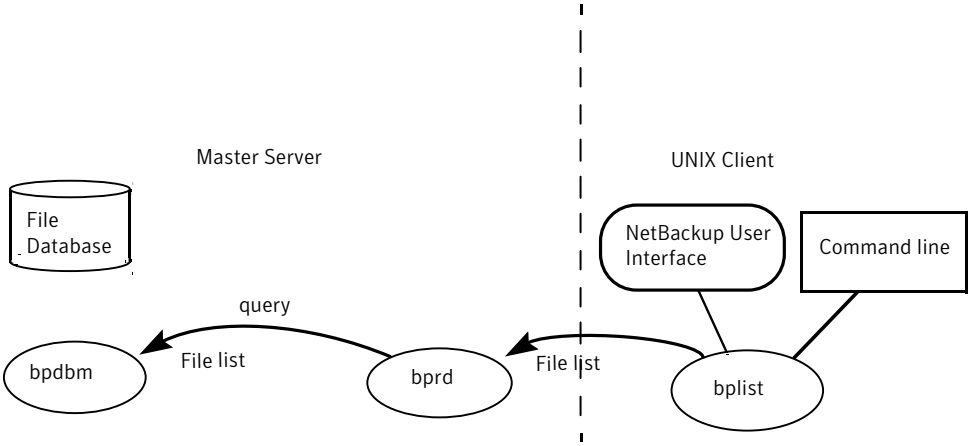
- UNIX: /usr/openv/netbackup/logs/bpdbm
  /usr/openv/db/log/server.log
- Windows: *install_path*\NetBackup\logs\bpdbm
  install_path\NetBackupDB\log\server.log

About UNIX client restoration

Before you start a restore, use the bplist program on the client to browse the file catalog to list the files available in the backup images and select the desired files. You can start bplist directly from the command line and the NetBackup user interface programs can use it.

To retrieve the file list, bplist sends a query to the request daemon (bprd) on the master server (see Figure A-6). The request daemon then queries bpdbm for the information and transmits it to bplist on the client.

Figure A-6 List operation - UNIX client



Refer to the appropriate figure as you read through the restore process.

See Figure A-7 on page 299.

See Figure A-8 on page 300.

The following are the processing steps in a restore (in the order presented):

- When the user starts a restore, NetBackup invokes the client's `bprestore` program which sends a request to the request daemon, `bprd`. This request identifies the files and client. The request daemon then uses `bpcd` (client daemon) to start the backup and restore manager (`bpbrm`).

  Note: To restore Backup Exec images, `bpbrm` initiates `mtfrd` instead of `tar` on the clients. The server processes are the same as those used for NetBackup restores.

- If the disk device or tape device on which the data resides attaches to the master server, the following occurs: `bprd` starts the backup and restore manager on the master server. If the disk unit or tape unit connects to a media server, `bprd` starts the backup and restore manager on the media server.
- The backup and restore manager starts `bptm` and uses the client daemon (`bpcd`) to establish a connection between the NetBackup `tar` program on the client and `bptm` on the server.
- For tape: the `bptm` process identifies which media is needed for the restore, based on the image catalog. `bptm` then requests the allocation of the required media from `nbrb` through `nbjm`. `nbjm` then asks `mds` (part of `nbemm`) for the

resources. nbemm allocates the media and selects and allocates an appropriate drive (for tape media).

bptm asks ltid to mount the tape in the drive.

For disk: bptm does not need to ask nbrb for an allocation, because disk inherently supports concurrent access. bptm uses the file path in a read request to the system disk manager.

- bptm directs the image to the client in one of two ways. If the server restores itself (server and client are on the same host), tar reads the data directly from shared memory. If the server restores a client that resides on a different host, it creates a child bptm process which transmits the data to tar on the client.

  Note: Only the part of the image that is required to satisfy the restore request is sent to the client, not necessarily the entire backup image.

- The NetBackup tar program writes the data on the client disk.

Note: PBX must be running for NetBackup to operate (PBX is not shown in the next diagram).

See "Resolving PBX problems" on page 73.

Figure A-7 shows how to restore from tape in the UNIX environments:

Figure A-7 Restore from tape (UNIX)

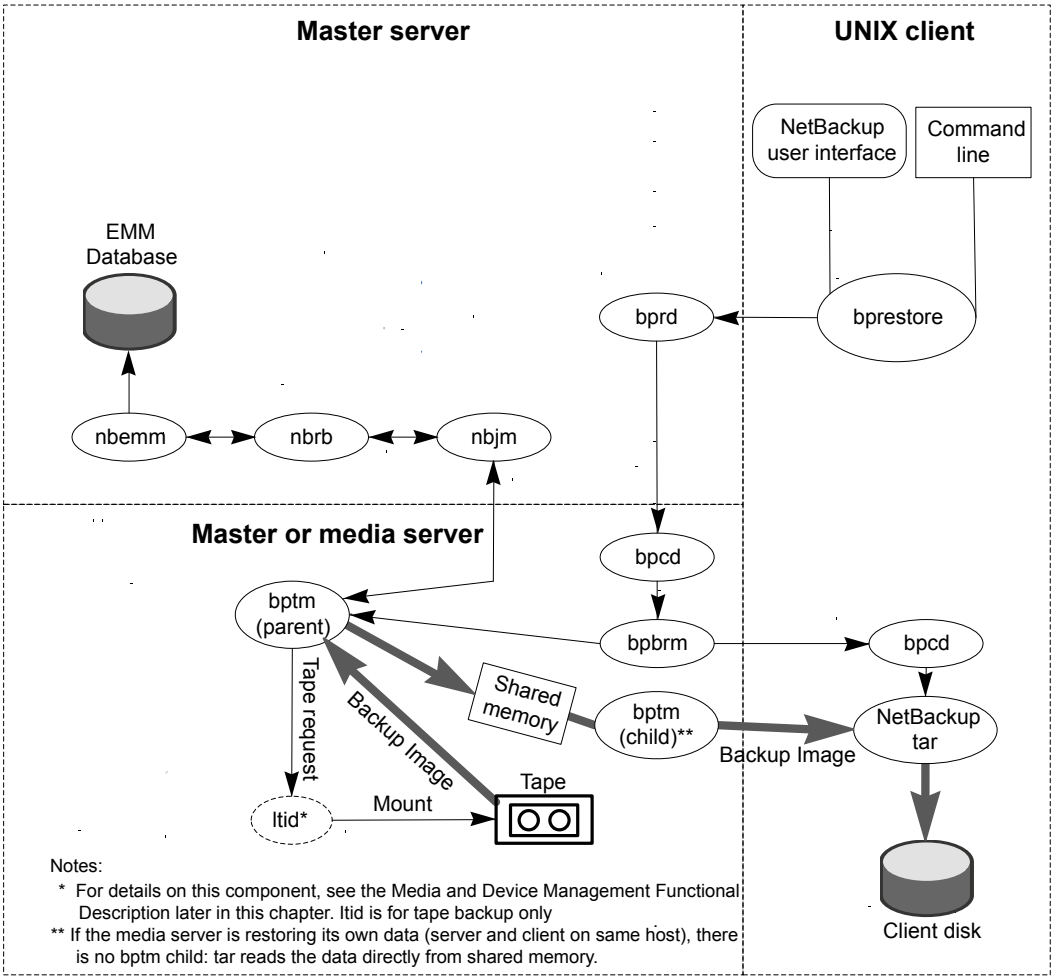
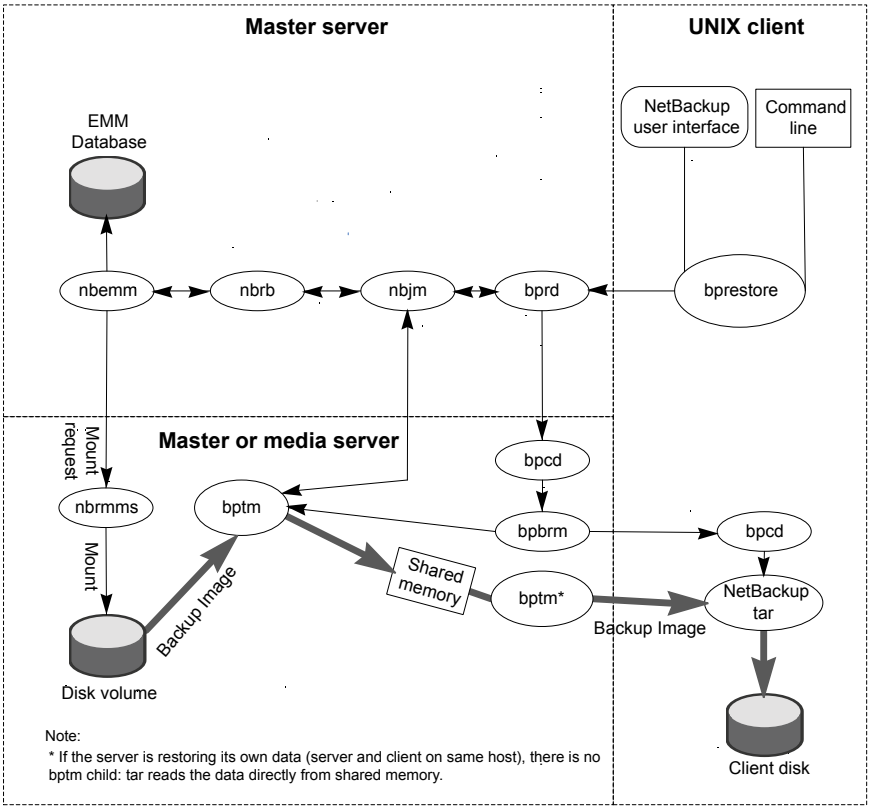


Figure A-8 shows how to restore from disk in the UNIX environments:

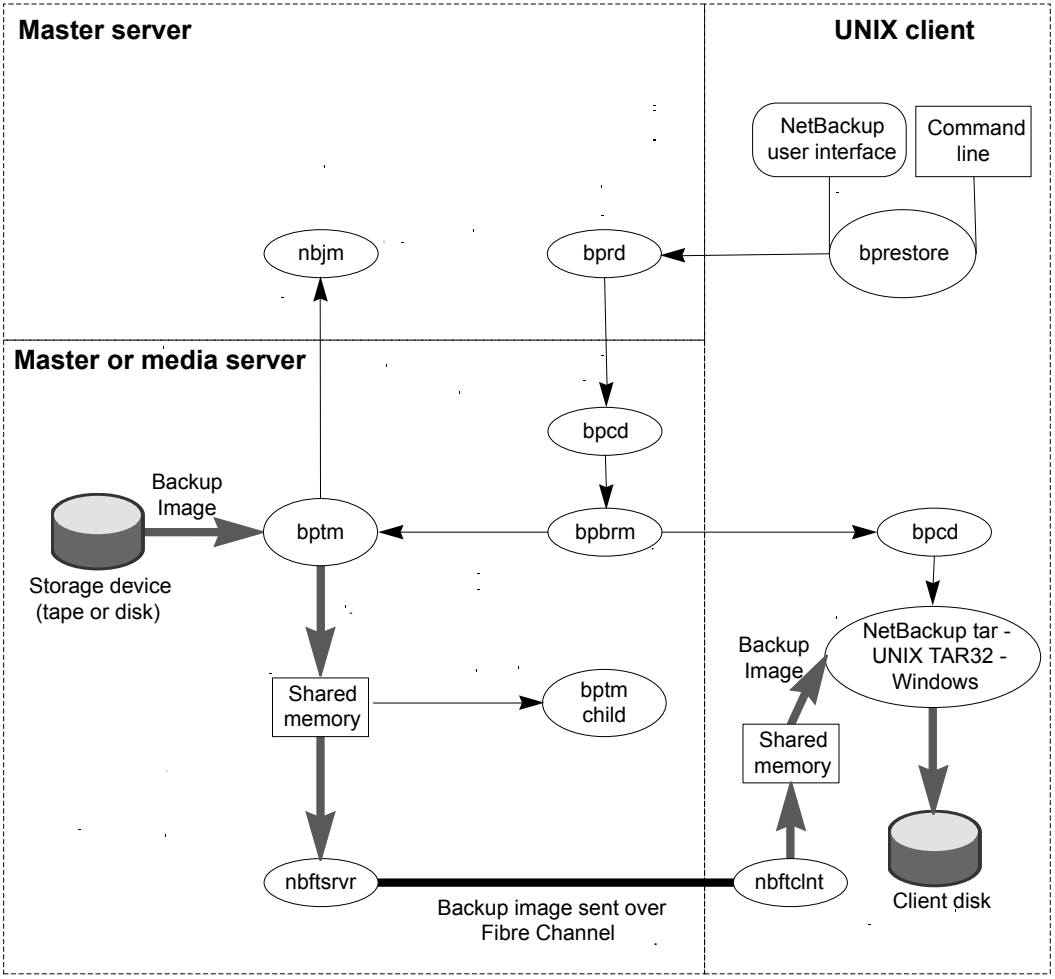
Figure A-8 Restore from disk (UNIX)



About SAN client restoration

Figure A-9 shows the server and client components that are used in a restore of a SAN client over Fibre Channel.

Figure A-9 SAN client restore with Fibre Transport



The process flow for a SAN Client restore is as follows (in the order presented).

- When the user starts a restore, NetBackup invokes the client's `bprestore` program which sends a request to the request daemon, `bprd`. This request identifies the files and client. The request daemon then uses `bpcd` (client daemon) to start the backup and restore manager (`bpbrm`).

Note: To restore Backup Exec images, `bpbrm` invoke `mtfrd` instead of `tar` on the clients. The server processes are the same as those used for NetBackup restores.

- If the disk device or tape device on which the data resides attaches to the master server, then `bprd` starts the backup and restore manager on the master server. If the disk unit or tape unit connects to a media server, `bprd` starts the backup and restore manager on the media server.
- bpbrm starts bptm and provides bptm with the backup ID and the shmfat (shared memory) flag.
- bptm does the following:
  - Requests SAN Client information from nbjm.
  - Sends a restore request to the FT server process (nbftsrvr).
  - Sends a restore request to the FT Client process on the client (nbftclnt). nbftclnt opens a fibre channel connection to nbftsrvr on the media server, allocates shared memory, and writes shared memory information to the backup ID file.
- bpbrm starts tar by means of bpcd and provides tar with the backup ID, socket information, and the shmfat (shared memory) flag.
- bptm does the following:
  - Reads the image from the storage device.
  - Creates a bptm child process. This process filters the backup image so that only the files that are selected for the restore are sent to the client.
  - Writes the image data to the shared buffer on the server.
  - When buffer is full or job is done, sets buffer flag (partial buffers may be sent to the client).
- tar does the following:
  - Sends the status and control information to bpbrm.
  - Reads the shared memory information from the local backup ID file (waits for the file to exist and become valid).
  - Waits for the buffer flag that indicates the data is ready to be read.
  - Reads data from the buffer, extracts files and restores them. When the shmfat (shared memory) flag is provided, tar considers the data to be already filtered.
- The FT Server process nbftsrvr waits for the shared memory buffer flag to be set. nbftsrvr then transfers the image data to the FT Client (nbftclnt) shared memory buffer, and clears the buffer flag.
- The FT Client (nbftclnt) waits for the data from nbftsrvr and writes the data to the shared memory buffer on the client. nbftclnt then sets the buffer flag.

- At the end of the job:
  - bptm informs tar and bpbrm that the job is complete.
  - bptm directs nbftclnt to close the fibre channel connection.
  - nbftclnt closes the fibre channel connection and deletes the BID file.

About Windows client restoration

NetBackup supports the same types of operations on Windows clients as it does for UNIX clients.

The following are the Windows processes involved in restore operations:

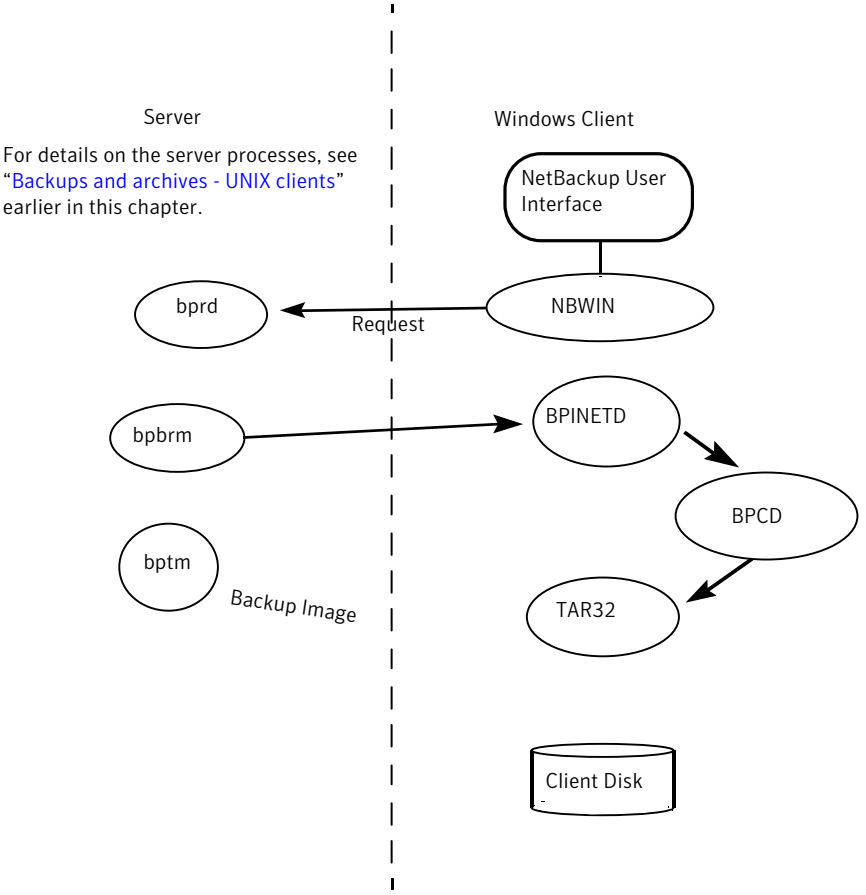
- `NBWIN` is the user interface program on the client. The `bpbackup` function and the `bparchive` function are merged into `NBWIN`.
- `BPINETD` serves the same purpose as `inetd` on UNIX clients.
- The NetBackup client daemon is called `BPCD`.
- `TAR32` is part of NetBackup for Windows and serves the same purpose as NetBackup `tar` on UNIX.

Note: To restore Backup Exec images, `bpbrm` invokes `mtfrd.exe` instead of `tar32.exe` on the clients. The server processes are the same as those used for NetBackup restores.

The server processes are the same as described for UNIX.

Figure A-10 shows the client processes involved in these operations.

Figure A-10 Restore - Windows client



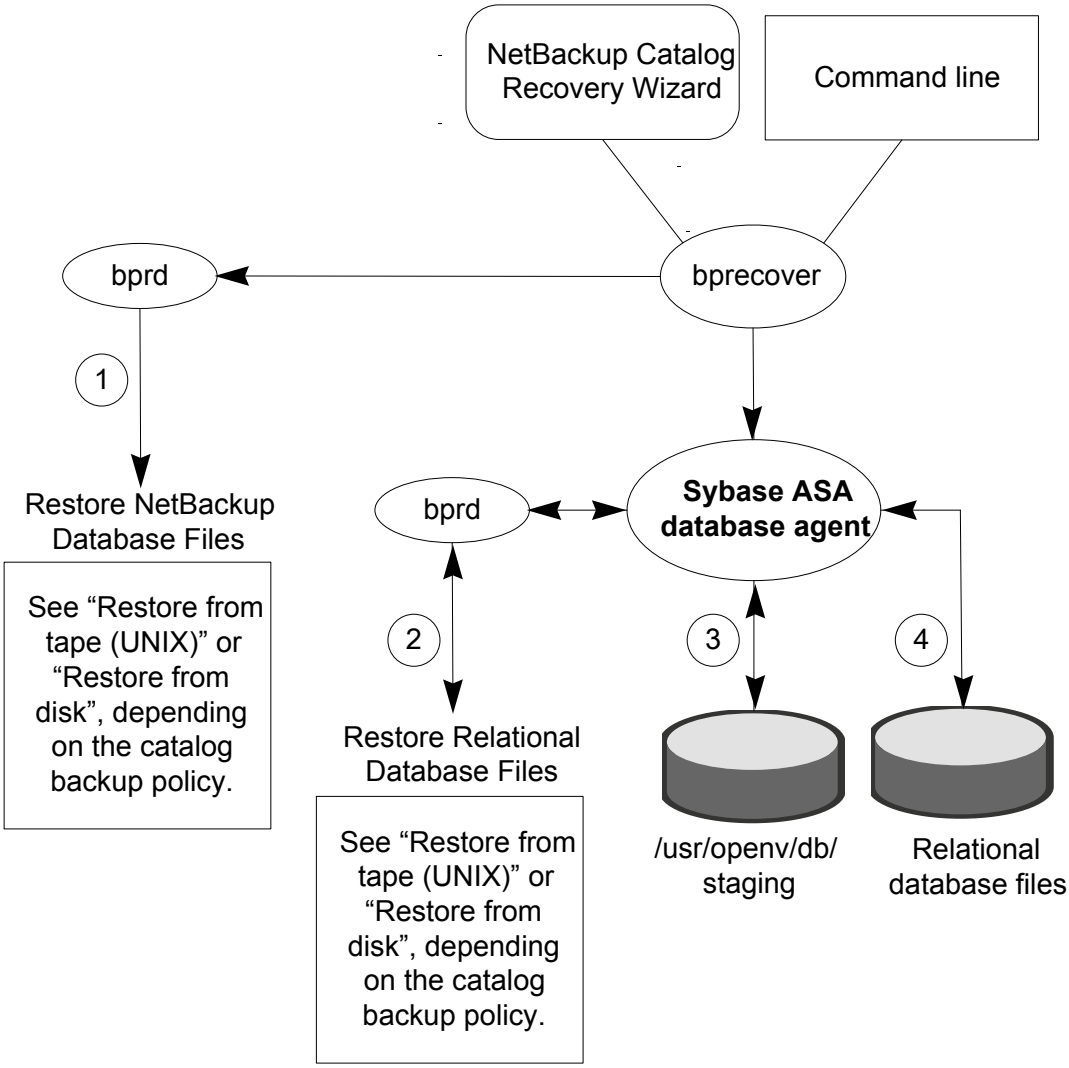
About catalog backup restoration

A catalog restore can be initiated by the NetBackup Catalog Recovery Wizard in the Administration Console, or by manual use of the `bprecover` command. More information is available in the following topic:

See "About disaster recovery" on page 204.

Figure A-11 illustrates the catalog restore and recovery process.

Figure A-11 Catalog restore and recovery



A restore of the NetBackup database and relational database (NBDB) files from a hot catalog backup consists of the following steps (in the order presented):

- The NetBackup catalog image and configuration files are restored.
- The NBDB files are restored. The database files are restored to `/usr/openv/db/staging` (UNIX), or to *`install_path`*`\NetBackupDB\staging` (Windows).

- After the files are restored to the staging directory, the EMM database is recovered.
- The NBDB files are moved from the staging directory to a location determined by the following: the `bp.conf` file `VXDBMS_NB_DATA` setting on UNIX and by the corresponding registry key on Windows. The default location is `/usr/openv/db/data` on UNIX, and *`install_path`*`\NetBackupDB\data` on Windows.
  If the relational database files are relocated, they are moved from the staging directory to the `/usr/openv/db/data/vxdbms.conf` file (UNIX) or the *`install_path`*`\NetBackupDB\data\vxdbms.conf` file (Windows). A description is available of how the NetBackup relational database files can be relocated after installation.
  For more information about the NetBackup relational database (NBDB), see the NetBackup Administrator's Guide, Volume I.

Messages that are related to this catalog recovery process are divided into the following three areas:

- For messages that are related to all catalog recovery steps, consult the `/usr/openv/netbackup/logs/admin` logs (UNIX), or *`install_path`*`\NetBackup\logs\admin` (Windows).
- For messages that are related to the first two bulleted items, consult the `tar`, `bpbrm`, and `bpcd` logs.
- For messages pertaining only to the relational database files, see the progress logs in the following directory:
  `/usr/openv/netbackup/logs/user_ops/root/logs` (UNIX), or *`install_path`*`\NetBackup\logs\user_ops\root\logs` (Windows).

NetBackup directories and files

Figure A-12 shows the NetBackup file and directory structure on UNIX servers and clients. If a host is only a client and not a server, only the files in the Client portion are present. If a host is both a client and a server, the client shares files as necessary from those in the Server portion.

A Windows NetBackup server has equivalent files and folders that are located where NetBackup is installed (`C:\Program Files\VERITAS` by default).

NetBackup directory structure - UNIX

Figure A-12 lists the items that are described in tables on the following pages.

Figure A-12 NetBackup directories and files

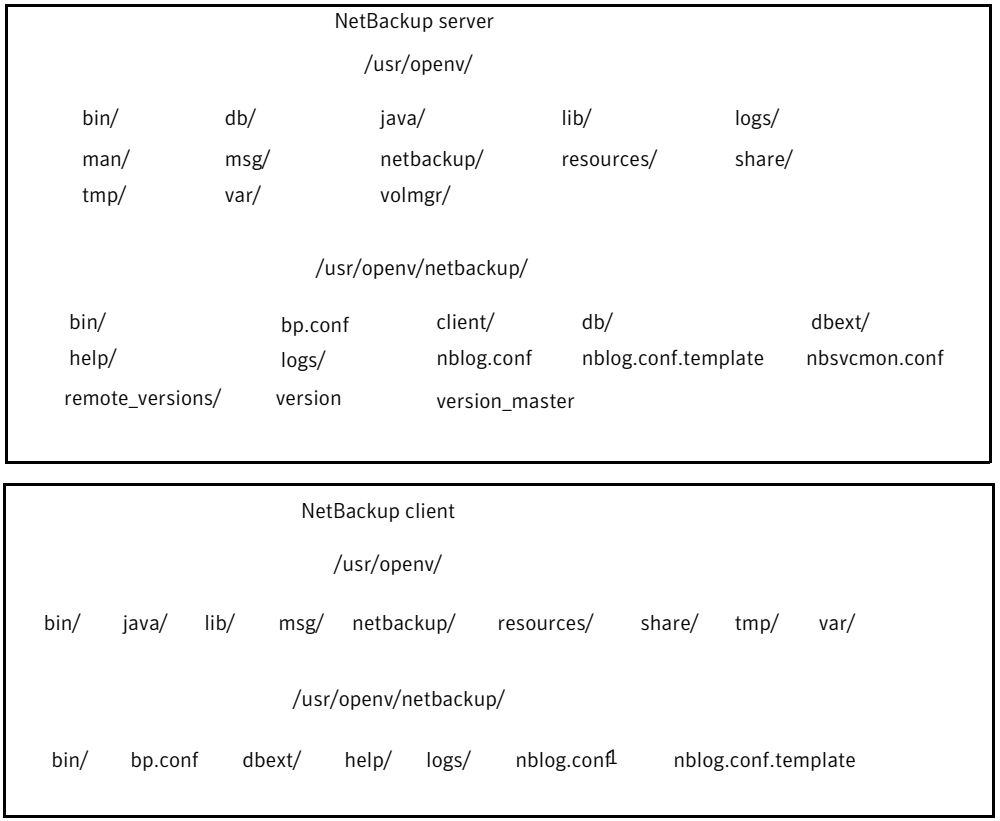


Table A-3 describes the `/usr/openv/` files and directories.

Table A-3 Directories and files in /usr/openv/ - servers and UNIX clients

File or directory in `/usr/openv/`	Contents
`bin/`	Contains miscellaneous executable binaries including the vnetd daemon and utilities for legacy enhanced authentication.
`db/`	Contains the NetBackup Relational Database Manager (SQL Anywhere) and database data file.
`java/`	Contains the NetBackup-Java Administration Console and the Backup, Archive and Restore user interface.

Table A-3 Directories and files in /usr/openv/ - servers and UNIX clients *(continued)*

File or directory in `/usr/openv/`	Contents
`lib/`	Contains shared libraries that are required for NetBackup operation.
`logs/`	Contains all logs that are written by unified logging. You do not have to create subdirectories for these logs.
`man/`	Contains man pages for NetBackup commands.
`msg/`	Contains the message files and a configuration file for all installed languages of NetBackup.
NB-Java.tar.Z	A tar file that contains the NetBackup-Java interfaces.
netbackup/	See Table A-4 on page 309.
resources/	Contains the NetBackup message catalogs that are used by unified logging (VxUL).
share/	Contains static configuration files. These files are normally unchanged between NetBackup releases.
tmp/sqlany	Contains the NetBackup Relational Database Manager (SQL Anywhere) installation trace files, and the log files regarding to database start and stop.
var/	Contains the variable configuration files. These files, which are related to licensing, authentication, authorization, and networking, may change while NetBackup is running. `/usr/openv/var/global` contains various static and variable configuration files. In a cluster, the `/global` directory is shared between nodes.
volmgr/	Contains the media and device management directories and files. See "NetBackup directory structure - UNIX" on page 306.

Contents of /usr/openv/netbackup

Table A-4 describes the `/usr/openv/netbackup` files and directories.

Table A-4 Directories and files in /usr/openv/netbackup/ - servers and UNIX clients

File or Directory in /usr/openv/netbackup/	Contents
bin/	Commands, scripts, programs, daemons, and files that are required for NetBackup operation and administration. On a server, there are two subdirectories under bin. admincmd: Contains various commands that used internally by NetBackup. Use these commands ONLY if they are documented. Most of these commands are not documented and should not be used directly. goodies (UNIX only): Contains scripts and information that may be useful to the administrator. These subdirectories are not present on clients.
bp.conf	Configuration file containing options for NetBackup operation. A detailed explanation is available about each option and how to set it. See the NetBackup Administrator's Guide, Volume II. On a Windows server, these options are set in the NetBackup Administration Console.
client/	NetBackup client software that is installed on the clients during installation.
db/	NetBackup catalogs. See Table A-6 on page 322.
dbext/	For NetBackup database agent software, contains the version file, compressed tar file, and install_dbext script. If no agents are installed, this folder is empty.
help/	Help files that are used by NetBackup programs. These files are in ASCII format.
logs/	Legacy debug logs for NetBackup processes. You must create the necessary subdirectories in order for these log files to be written. See "About legacy logging" on page 153. See Table A-5 on page 311. for an explanation of the processes that produce the logs.

Table A-4 Directories and files in /usr/openv/netbackup/ - servers and UNIX clients *(continued)*

File or Directory in /usr/openv/netbackup/	Contents
nblog.conf	Specifies the settings for unified logging. **Note:** Do not edit this file manually: use the vxlogcfg command instead. See "About unified logging" on page 129.
nblog.conf.template	Specifies the settings for unified logging. **Note:** Do not edit this file manually: use the vxlogcfg command instead. See "About unified logging" on page 129.
nbsvcmon.conf	Configuration file for the NetBackup Service Monitor. It tells the Service Monitor what services to monitor and how to restart them if they fail unexpectedly.
remote_versions/	A cache of the versions of other media servers in the system.
version	Version and release date of the software.
version_master	Identifies the NetBackup master server.

NetBackup programs and daemons

Table A-5 describes the programs and daemons that provide most of the control for backup, archive, and restore operations.

The explanations include what starts and stops the program or daemon, and the debug log subdirectory (if any) where it records its activities.

You must create legacy logging directories manually; see "logs" in the previous table. More information is available.

See "About legacy logging" on page 153.

Table A-5 NetBackup daemons and programs

Program/Daemon	Description
bp	On UNIX clients, this menu-driven, character-based interface program has options for starting user-directed backups, restores, and archives. Started By: /usr/openv/netbackup/bin/bp command on the client. Stopped By: Exiting the interface program. Debug Log: /usr/openv/netbackup/logs/bp on the client. The debug logs for bpbackup, bparchive, bprestore, and bplist also have information about bp activities.
bpadm	On a UNIX master server, this administrator utility has a menu-driven, character-based, interface with options for configuring and managing NetBackup. Started By: /usr/openv/netbackup/bin/bpadm command on the master server. Stopped By: Quit option from within bpadm. Debug Log: admin legacy log directory on the server.
bparchive	On UNIX clients, this program communicates with bprd on the master server when a user starts an archive. Started By: Starting an archive by using the client-user interface or by executing the /usr/openv/netbackup/bin/bparchive command on the client. Stopped By: Completion of operation. Debug Log: bparchive legacy log directory on the client.
bpbackup	On UNIX clients, this program communicates with bprd on the master server when a user starts a backup. Started By: Starting a backup by using the client-user interface or by executing the /usr/openv/netbackup/bin/bpbackup command on the client. Stopped By: Completion of operation Debug Log: bpbackup legacy log directory on the client.

Table A-5 NetBackup daemons and programs *(continued)*

Program/Daemon	Description
bpbkar	On UNIX clients the Backup/Archive Manager generates the backup images. Started By: bpbrm on the server with the storage unit. Stopped By: Completion of operation. Debug Log: bpbkar legacy log directory on the client.
BPBKAR32	On Windows clients, the Backup/Archive Manager generates the backup images. Started By: BPCDW32 on the client. Stopped By: Completion of operation. Debug Log: BPBKAR legacy log directory in the NetBackup logs directory on the client.
bpbrm	On master and media servers, the Backup/Restore Manager manages the client and bptm or bpdm process. It also uses error status from the client and from bptm or bpdm to determine the final status of backup or restore operations. Started By: For each backup or restore, nbjm starts an instance of bpbrm on the server with the appropriate storage unit. Stopped By: Completion of operation. Debug Log: bpbrm legacy log directory on the server.
bpcd	On UNIX clients, bpcd is the NetBackup client daemon and lets NetBackup start programs on remote hosts (can be UNIX clients or other servers). For example, the server can connect to UNIX clients without requiring /.rhosts entries on the remote host. The program is used when nbjm starts bpbrm and when bpbrm communicates with the client. (For a description of the NetBackup client daemon on PC clients, see BPCDW32.EXE and BPCD.NLM in this table.) Started By: inetd. Stopped By: Completion of operation. Debug Log: bpcd legacy log directory on both client and server.

Table A-5 NetBackup daemons and programs *(continued)*

Program/Daemon	Description
BPCDW32.EXE	On Windows clients, BPCDW32.EXE is the executable file that starts the NetBackup client daemon. Started By: When Windows starts if the daemon is in the Startup group. Otherwise, by double clicking on its icon. Stopped By: On Windows, you can stop it through the Services application in the Control Panel. Debug Log: BPCD legacy log directory on the client.
bpdbjobs	On UNIX master servers, this program is used to clean up the NetBackup jobs database. Started By: /usr/openv/netbackup/bin/admincmd/bpdbjobs. When bprd starts, it runs this command automatically. The administrator can also execute it manually or with a cron job. Stopped By: No terminate option exists for this command outside of using kill. Debug Log: bpdbjobs legacy log directory on the server.
bpdbm	On master servers, the NetBackup database manager program that manages the configuration, error, and file databases. Started By: bprd (also by /usr/openv/netbackup/bin/initbpdbm on UNIX) Stopped By: /usr/openv/netbackup/bin/bpdbm -terminate command on UNIX and by stopping the NetBackup Database Manager service on Windows. Debug Log: bpdbm legacy log directory on the server.
bpdm	On master and media servers, bpdm is used for the following disk operations: read phase of disk duplication, read phase of synthetic backups, disk verify and disk import, true image restore from disk, disk image deletion. Started By: For each operation, bpbrm starts an instance of bpdm, on the server with the storage unit. Stopped By: Completion of operation. Debug Log: bpdm legacy log directory on the server.

Table A-5 NetBackup daemons and programs *(continued)*

Program/Daemon	Description
`bpfis`	On clients, bpfis creates and deletes snapshots. Note that bpfis is part of the Snapshot Client add-on product. Started By: `bpbrm`. Stopped By: Completion of operation. Debug Log: `bpfis` legacy log directory on the client or alternate client.
`bphdb`	On SQL, Oracle, Informix, Sybase, DB2, and SAP database clients, `bphdb` executes scripts to back up the database. Started By: Client-user interface when the user starts a database backup operation. Stopped By: Completion of operation. Debug Log: `bphdb` legacy log directory on the client.
`bpjava-msvc`	NetBackup-Java master server application program. This program runs on all NetBackup UNIX systems and authenticates the users that start the NetBackup-Java interface programs. Started By: `inetd` during startup of the NetBackup Java interfaces. Stopped By: When authentication is complete. Debug Log: `bpjava-msvc` legacy log directory on the server.
`bpjava-susvc`	NetBackup-Java server application program. This program services all requests from the NetBackup-Java console when performing server type functions such as configuration, policies, reports, activity monitor, etc. Started By: `bpjava-msvc` upon successful login through the Login dialog box that is presented when a NetBackup-Java interface is started. Stopped By: When the interface program is terminated. Debug Log: `bpjava-susvc` legacy log directory.

Table A-5 NetBackup daemons and programs *(continued)*

Program/Daemon	Description
`bpjava-usvc`	NetBackup-Java user server application program. This program services all requests from the NetBackup-Java user backup and archive restore interface. Started By: `bpjava-msvc` upon successful login through the Login dialog box that is presented when a NetBackup-Java interface is started. Stopped By: When the interface program is terminated. Debug Log: `bpjava-usvc` legacy log directory.
`bplist`	On UNIX clients, this program communicates with `bprd` on the master server when a user browses the database during a restore operation. Started By: Starting a search of the image database by using the client-user interface or by executing the `/usr/openv/netbackup/bin/bplist` command on the client. Stopped By: Completion of operation Debug Log: `bplist` legacy log directory on the client, `bprd` log directory on the master.
`bprd`	On master servers, the request daemon responds to client and administrative requests for the following: ■ Restores ■ Backups (scheduled and user-directed) ■ Archives ■ List that is backed up or archived files ■ Manual immediate backups (started through the NetBackup administration interface manual backup option) Started By: Application startup scripts or the `/usr/openv/netbackup/bin/initbprd` command. Stopped By: Application shutdown. Debug Log: `bprd` legacy log directory on the server.

Table A-5 NetBackup daemons and programs *(continued)*

Program/Daemon	Description
bprestore	On UNIX clients, this program communicates with bprd on the master server when a user starts a restore. Started By: Starting restore by using the client-user interface (or by executing the /usr/openv/netbackup/bin/bprestore command on the client). Stopped By: Completion of operation Debug Log: bprestore legacy log directory on the client.
bptm	On master and media servers, bptm manages both disk and tape backup and restore. It is used when the storage unit type is either disk or Media Manager. This program manages the transfer of images between the client and the storage device. Started By: For each backup or restore, bpbrm starts an instance of bptm on the server that has the storage unit. Stopped By: Completion of operation. Debug Log: bptm legacy log directory on the server.
jbpSA	A Java-based program for performing backups, archives, and restores of UNIX clients. Started By: On UNIX, the /usr/openv/netbackup/bin/jbpSA command. Debug Log: None, although the logs for the bpbackup, bparchive, bplist, and bprestore commands on the client can be useful. Also, check the bpjava-msvc and bpjava-usvc logs.
jnbSA	A Java-based administration utility for managing NetBackup on UNIX. In addition, administration of supported UNIX systems can be performed by using the NetBackup-Java Windows Display Console on a Windows system. Started By: On UNIX, the /usr/openv/netbackup/bin/jnbSA command. On a NetBackup-Java Windows Display console, the NetBackup - Java on *host* menu item on the Programs/NetBackup menu. Stopped By: Exit option in jnbSA. Debug Log: None, although the logs for bpjava-msvc and bpjava-susvc can be helpful.

Table A-5 NetBackup daemons and programs *(continued)*

Program/Daemon	Description
nbemm	On the server that is defined as the EMM server, nbemm manages devices, media, and storage unit configuration, and performs resource selection. Replaces vmd as the device allocator. Started By: Started when NetBackup starts. Stopped By: /usr/openv/netbackup/bin/nbemm -terminate Debug Log: On the server, /usr/openv/logs (UNIX) or *install_path*\NetBackup\logs (Windows). See "About unified logging" on page 129.
nbaudit	On the master server, the audit daemon accepts audit requests from other NetBackup components and persists the audit records in the database. It also queries and returns the audit records from the database to display to the user. Started By: Started when NetBackup starts. Stopped By: /usr/openv/netbackup/bin/nbaudit -terminate. Debug Log: On the server, /usr/openv/logs/nbaudit (UNIX) or *install_path*\logs\NetBackup\nbaudit (Windows).
nbfdrv64	On a media server that is enabled for SAN Client backup over fibre channel, nbfdrv64 is the following: a user mode component that is used for both backup and restore. nbfdrv64 uses a windrvr6 proxy to move fibre channel data between nbftclnt and bptm buffers. Started By: /usr/openv/netbackup/bin/nbftsrvr Stopped By: /usr/openv/netbackup/bin/nbftsrvr -terminate Debug Log: On the server, /usr/openv/logs (UNIX) or *install_path*\NetBackup\logs (Windows). See "About unified logging" on page 129.

Table A-5 NetBackup daemons and programs *(continued)*

Program/Daemon	Description
`nbftclnt`	On clients that are enabled for SAN Client backup over fibre channel, nbftclnt transfers the backup image over fibre channel to nbftsrvr on the media server. Started By: Started when NetBackup starts. Stopped By: `/usr/openv/netbackup/bin/nbftclnt -terminate`. Debug Log: On the client, `/usr/openv/logs` (UNIX) or *`install_path`*`\NetBackup\logs` (Windows). See "About unified logging" on page 129.
`nbftsrvr`	On a media server that is enabled for SAN Client backup over fibre channel, nbftsrvr does the following: reads the backup image from nbftclnt and transfers it to shared memory on the media server. Started By: Started when NetBackup starts. Stopped By: `/usr/openv/netbackup/bin/nbftsrvr -terminate`. Debug Log: On the server, `/usr/openv/logs` (UNIX) or *`install_path`*`\NetBackup\logs` (Windows). See "About unified logging" on page 129.
`nbjm`	On master servers, the nbjm service accepts job requests from nbpem and from media commands such as bplabel and tpreq. nbjm acquires job resources from nbrb, and runs the jobs once resources are available. Started By: Started when NetBackup starts. Stopped By: `/usr/openv/netbackup/bin/nbjm -terminate` Debug Log: On the server, `/usr/openv/logs` (UNIX) or *`install_path`*`\NetBackup\logs` (Windows). See "About unified logging" on page 129.

Table A-5 NetBackup daemons and programs *(continued)*

Program/Daemon	Description
nbpem	On master servers, the nbpem service uses nbproxy to get the policy list from bpdbm, creates the policy-client tasks, determines when jobs are due to run, and starts due jobs. Started By: Started when NetBackup starts. Stopped By: /usr/openv/netbackup/bin/nbpem -terminate Debug Log: On the server, /usr/openv/logs (UNIX) or *install_path*\NetBackup\logs (Windows). See "About unified logging" on page 129.
nbproxy	Runs on the master server and the media server as a child of the process it serves. nbproxy provides a thread-safe API for the libraries that are not yet thread safe. Started By: the process that uses nbproxy as a proxy. Stopped By: stops the process that uses nbproxy. Debug Log: nbproxy legacy log directory on the server.
nbrb	On the server that is defined as the EMM server, the nbrb service accepts resource requests from nbjm, acquires physical resources from nbemm, and manages logical resources. Started By: Started when NetBackup starts. Stopped By: /usr/openv/netbackup/bin/nbrb -terminate Debug Log: On the server, /usr/openv/logs (UNIX) or *install_path*\NetBackup\logs (Windows). See "About unified logging" on page 129.
ndmpagent	Controls backup and restore operations on a NAS server. The ndmpagent service is for remote NDMP, backing up NDMP data to a drive that is configured in a Media Manager storage unit on a NetBackup media server. Started By: bpbrm. Stopped By: Completion of backup or restore. Debug Log: On the server, /usr/openv/logs (UNIX) or *install_path*\NetBackup\logs (Windows). See "About unified logging" on page 129.

Table A-5 NetBackup daemons and programs *(continued)*

Program/Daemon	Description
`nbstserv`	Runs on the master server. The `nbstserv` service manages lifecycle operations including duplication, staging, and image expiration. Started By: Started when NetBackup starts. Stopped By: `/usr/openv/netbackup/bin/nbstserv -terminate` Debug Log: On the server, `/usr/openv/logs` (UNIX) or *`install_path`*`\NetBackup\logs` (Windows). For more information about OID 226 and 272, see the following topic: See "Originator IDs for the entities that use unified logging" on page 134.
`nbrmms`	Remote Manager and Monitor Service (`nbrmms`) is the conduit through which EMM discovers and configures storage on media servers. In addition to configuration management, It provides all access to media server resources for monitoring and event notifications. Started By: Started when NetBackup starts, or by `/usr/openv/netbackup/bin/nbrmms` Stopped By: Stopped when NetBackup stops, or by `/usr/openv/netbackup/bin/nbrmms -terminate` Debug Log: On the server, `/usr/openv/logs` (UNIX) or *`install_path`*`\NetBackup\logs` (Windows). See "About unified logging" on page 129.
`pbx_exchange`	Private Branch Exchange (PBX) is a common services framework that helps limit the number of TCP/IP ports that the CORBA services of NetBackup use. Started By: Started when NetBackup starts, or by `/opt/VRTSpbx/bin/vxpbx_exchanged start`. Stopped By: Stopped when NetBackup stops, or by `/opt/VRTSpbx/bin/vxpbx_exchanged stop`. Debug Log: On the server, `/opt/VRTSpbx/log` (UNIX) or *`install_path`*`\VxPBX\log` (Windows). See "Accessing the PBX logs" on page 76.

Table A-5 NetBackup daemons and programs *(continued)*

Program/Daemon	Description
ql2300_stub	On a Solaris media server that is enabled for SAN Client transfers over fibre channel: ql2300_stub is a device driver used to read and write to the NVRAM on a target mode Fibre Channel Host Bus Adapter. On Linux, it also prevents initiator mode drivers from binding to the target mode fibre channel HBAs. Started By: Device driver that is started by the operating system on a reboot after nbftsrv_config -nbhba on Linux and Solaris. On Linux, it is also started on all reboots after nbftsrv_config. Stopped By: Device driver that is stopped by nbfdrv64 on Linux and nbftsrv_config on Solaris. Debug Log: The host operating system handles the logging for the device driver in the system messages log: /var/adm/messages (Solaris) or /var/log/messages (Linux).
tar	On UNIX clients, the Tape ARchive program is a special version of tar provided with NetBackup and used to restore images. Started By: For each restore, bpbrm starts an instance of tar on the client. Stopped By: Completion of restore operation. Debug Log: tar legacy log directory on the client.
TAR32	On Windows clients, the TAR32 program is a special version of tar provided with NetBackup and used to restore images. Started By: For each restore, NetBackup starts an instance of TAR32 on the client. Stopped By: Completion of restore operation. Debug Log: TAR legacy log directory on the client.

Table A-5 NetBackup daemons and programs *(continued)*

Program/Daemon	Description
`windrvr6`	On a Media Server that is enabled for SAN Client transfers using fibre channel: windrvr6 is a kernel device driver used to communicate through the PCI bus to the target mode Fibre Channel Host Bus Adapters. Started By: Device driver that is started by the operating system at boot (Solaris) or by nbfdrv64 (Linux). Stopped By: Device driver that is stopped by the operating system at shutdown. Debug Log: The host operating system handles the logging in the system messages log log: `/var/adm/messages` (Solaris) or `/var/log/messages` (Linux).

NetBackup catalogs

The NetBackup catalogs contain the information that is used internally by NetBackup and reside in the `/usr/openv/netbackup/db` directory on UNIX servers and in the *`install_path`*`\NetBackup\db` directory on Windows NetBackup servers.

The `/usr/openv/netbackup/db/class` directory (*`install_path`*`\NetBackup\db\class` on Windows) has a subdirectory for each NetBackup policy that contains information about the policy.

Table A-6 describes the NetBackup catalogs.

Table A-6 NetBackup catalogs

Database	Contents
config	Configuration information. This database resides on the master server and has three parts: `policy`: Contains the information about each NetBackup policy. `config`: Contains the information about global attributes, storage units, and database backups. `altnames`: Contains the information about client names for restores.

Table A-6 NetBackup catalogs *(continued)*

Database	Contents
error	Error and status information about NetBackup operations. This database resides on the master server and has two parts: `error`: Contains the information that is recorded during backup operations and used in the NetBackup reports. `failure_history`: Contains the daily history of backup errors.
images	Information about the backup images and resides only on the master server. One of the files in the `images` directory is the `file` database. The `file` database is the one that NetBackup accesses when a user browses for files to restore.
jobs	Job information that is used by the NetBackup job monitor (UNIX NetBackup server) and activity monitor (Windows NetBackup server). The Jobs database is on the master server.
media	Media related information that is used by `bptm`. Also has an errors file that contains error history information for media and devices.

The NetBackup Search feature uses the catalog to help locate backup files, hold them, and then release them. It backs up the NetBackup client data to the media server and backs up the catalog metadata to the master server. The NetBackup indexing server indexes the metadata in the catalog on the master server.

Appendix B

Media and device management functional description

This appendix includes the following topics:

- Media and device management startup process
- Media and device management process
- Shared Storage Option management process
- Barcode operations
- Media and device management components

Media and device management startup process

Media and device management processes are automatically initiated during NetBackup startup. To start these processes manually, run `bp.start_all` (UNIX) or `bpup` (Windows). The `ltid` command automatically starts other daemons and programs as necessary. The daemons should be running after initial startup.

See Figure B-1 on page 326.

In the case of robotic daemons, such as `tl8d` and `tlhd`, the associated robot must also be configured for the daemon to run. Additional ways to start and stop daemons are available.

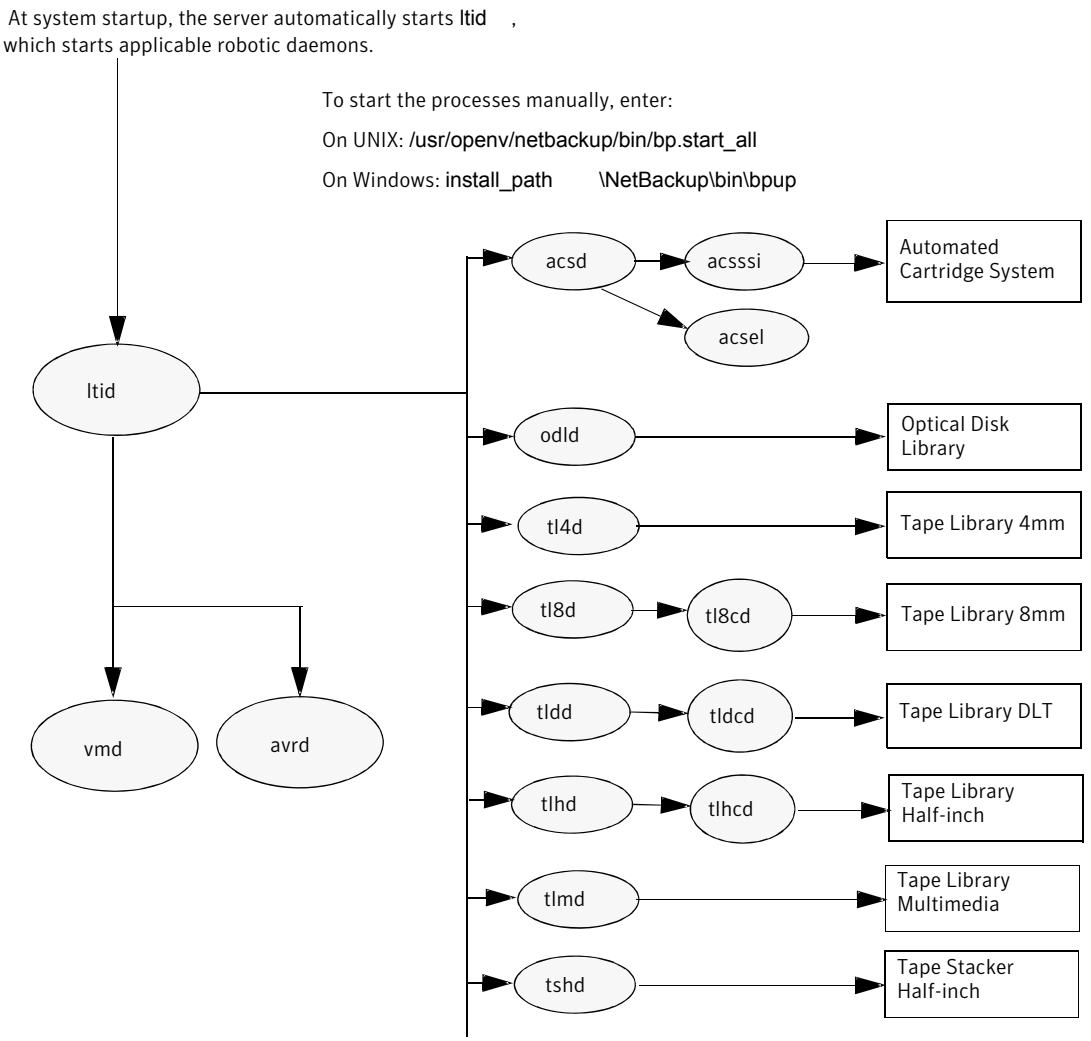
See Table B-1 on page 333.

TL8, TLH, and TLD require following types of daemons:

robotic	Each host with a robotic drive attached must have a robotic daemon. These daemons provide the interface between `ltid` and the robot. If different drives within a robot can attach to different hosts, the robotic daemon communicates with a robotic-control daemon (see Figure B-1).
robotic control	Robotic-control daemons centralize the control of robots when drives within a robot can connect to different hosts. A robotic-control daemon receives mount and unmount requests from the robotic daemon on the host to which the drive is attached. It then communicates these requests to the robot.

You must know the hosts that are involved to start all the daemons for a robot.

Figure B-1 Starting media and device management



Media and device management process

When the media management and device management daemons are running, NetBackup, Storage Migrator (UNIX), Storage Migrator for Microsoft Exchange (Windows), or users can request data storage or retrieval. The scheduling services initially handles the request.

See "Backup and archive processes" on page 279.

The resulting request to mount a device is passed from `nbjm` to `nbrb`, which acquires the physical resources from `nbemm` (the Enterprise Media Manager service).

If the backup requires media in a robot, `ltid` sends a mount request to the robotic daemon that manages the drives in the robot that are configured on the local host. The robotic daemon then mounts the media, and sets a drive busy status in memory shared by itself and `ltid`. Drive busy status also appears in the Device Monitor.

See Figure B-2 on page 328.

Assuming that the media is physically in the robot, the media is mounted and the operation proceeds. If the media is not in the robot, `nbrb` creates a pending request, which appears as a pending request in the Device Monitor. An operator must insert the media in the robot and use the appropriate Device Monitor command to resubmit the request so the mount request occurs.

A mount request is issued if the media is for a nonrobotic (standalone) drive that does not contain the media that meets the criteria in the request. If the request is from NetBackup and the drive does contain appropriate media, then that media is automatically assigned and the operation proceeds.

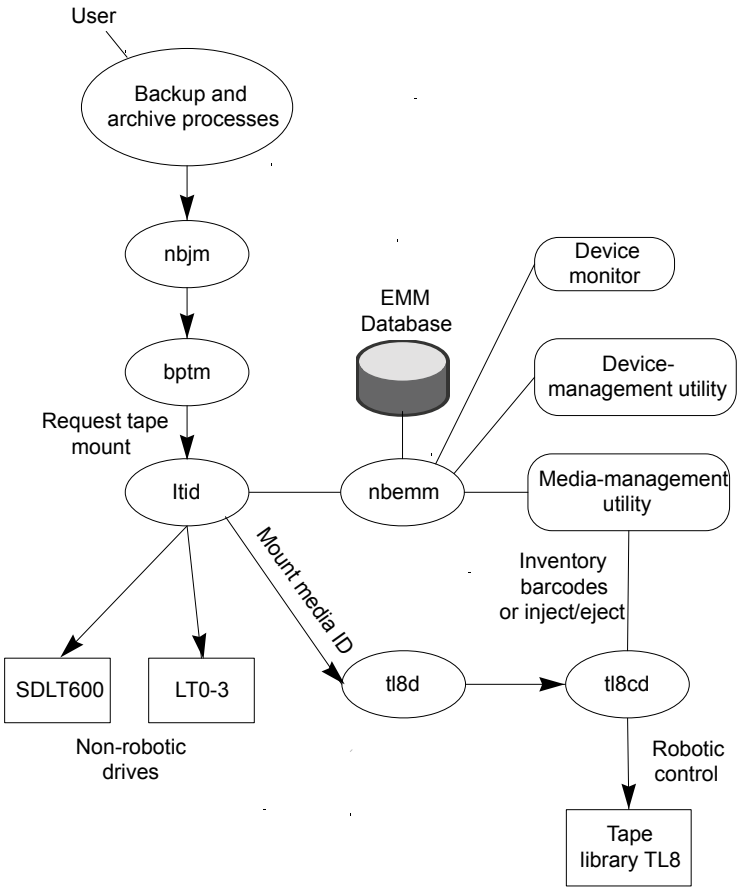
For more information about NetBackup media selection for nonrobotic drives, see the NetBackup Administrator's Guide, Volume II.

Note: , when you mount a tape on UNIX, the drive_mount_notify script is called. This script is in the /usr/openv/volmgr/bin directory. Information on the script can be found within the script itself. A similar script is called for the unmount process (drive_unmount_notify, in the same directory).

When a robotic volume is added or removed through the media access port, the media management utility communicates with the appropriate robotic daemon to verify the volume location or barcode. The media management utility (through a library or command-line interface) also calls the robotic daemon for robot inventory operations.

Figure B-2 shows an example of the media and device management process.

Figure B-2 Media and device management example process



Shared Storage Option management process

Shared Storage Option (SSO) is an extension to tape drive allocation and configuration for media and device management. SSO allows individual tape drives (standalone or in a robotic library) to be dynamically shared between multiple NetBackup media servers or SAN media servers.

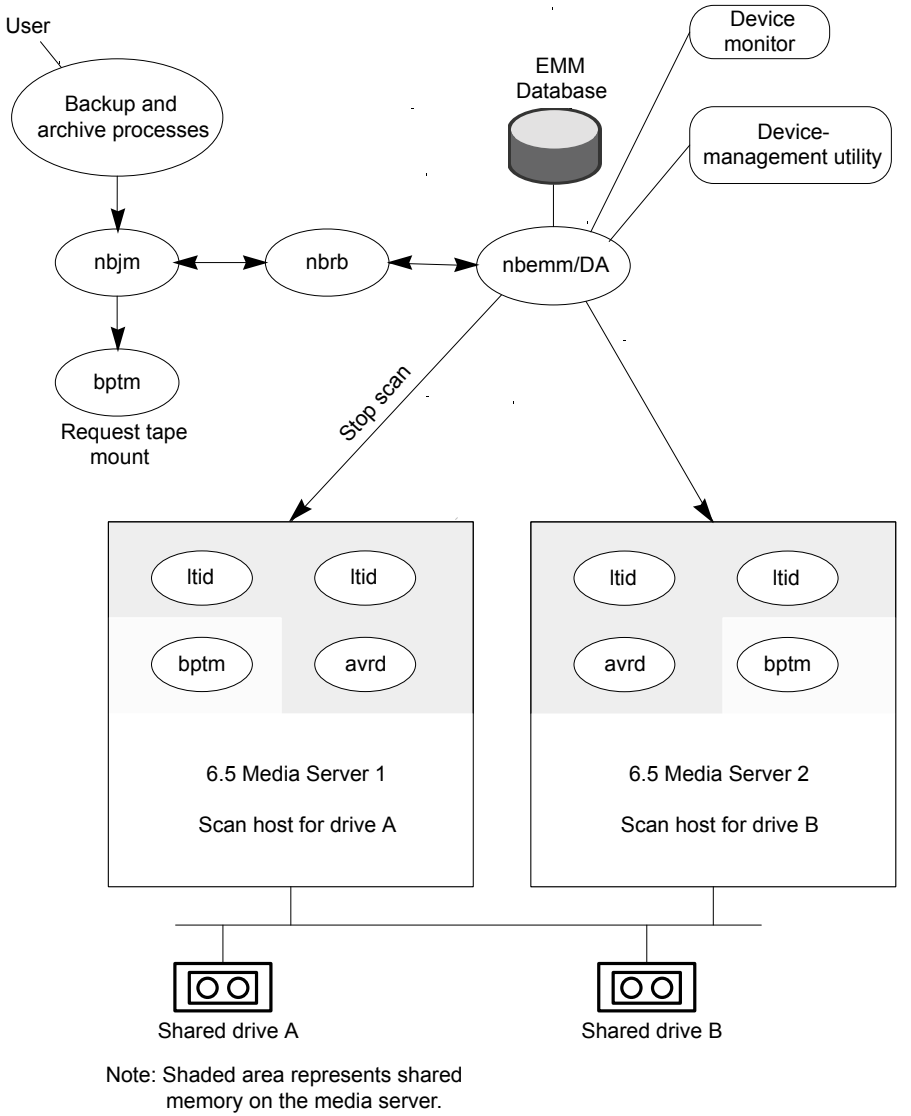
For more information about the Shared Storage Option, see the NetBackup Administrator's Guide, Volume II.

The following shows the Shared Storage Option management process in the order presented:

- NetBackup, Storage Migrator, or users can initiate backups. The nbjm process makes a mount request for the backup.
- nbrb tells the EMM server to obtain a drive for the backup.
- nbrb tells the device allocator (DA) in the EMM server to stop scanning the selected drive.
- nbemm tells the appropriate media server (the scan host for the selected drive) to stop scanning the drive. The stop scan request is carried out by means of oprd, ltid, and avrd in the media server's shared memory.
- nbemm informs nbrb when scanning on the selected drive has stopped.
- nbrb informs nbjm that the selected drive (A) is available for the backup.
- nbjm conveys the mount request and drive selection to bptm, which proceeds with the backup. To protect the integrity of the write operation, bptm uses SCSI reservations.
  For more information about how NetBackup reserves drives, see the NetBackup Administrator's Guide, Volume II.
- The mount-media operation is initiated.
- bptm makes position checks on the drive to ensure that the drive has not been rewound by another application. bptm also does the actual write to the tape.
- When the backup is complete, nbjm tells nbrb to release resources.
- nbrb de-allocates the drive in EMM.
- EMM tells the scan host to resume scanning the drive. The scan request is carried out by means of oprd, ltid, and avrd in the media server's shared memory.

Figure B-3 illustrates the Shared Storage Option management process.

Figure B-3 Media and device management process flow showing SSO components



Barcode operations

Barcode reading is mainly a function of the robot hardware rather than media and device management. When a robot has a barcode reader, it scans any barcode

that may be on a tape and stores the code in its internal memory. This associates the slot number and the barcode of the tape in that slot. NetBackup determines that association for its own use by interrogating the robot.

If a robot supports barcodes, NetBackup automatically compares a tape's barcode to what is in the EMM database as an extra measure of verification before you mount the tape. A request for the media that is in a robot that can read barcodes begins in the same manner as other requests.

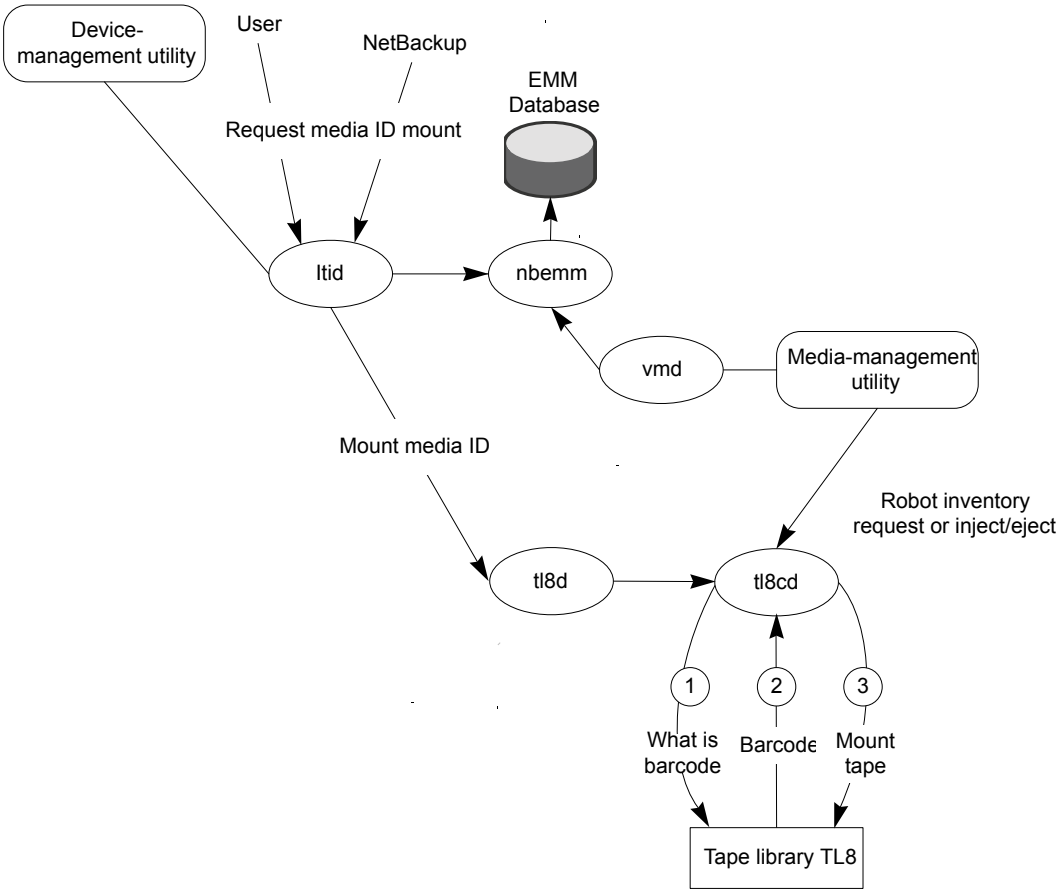
See Figure B-4 on page 332.

The `ltid` command includes the media ID and location information in a mount request to the robotic daemon for the robot that has the media ID. This request causes the robotic daemon to query the robotic-control daemon or the robot for the barcode of the tape in the designated slot. (This is a preliminary check to see if the correct media is in the slot.) The robot returns the barcode value it has in memory.

The robotic daemon compares this barcode with the value it received from `ltid` and takes one of the following actions:

- If the barcodes don't match, and the mount request is not for a NetBackup backup job, the robotic daemon informs `ltid` and a pending action request (Misplaced Tape) appears in the Device Monitor. An operator must then insert the correct tape in the slot.
- If the barcodes don't match and the mount request is for a NetBackup backup job, the robotic daemon informs `ltid` and the mount request is canceled. NetBackup (bptm) then requests a new volume from nbjm and from EMM.
- If the barcodes match, the robotic daemon requests the robot to move the tape to a drive. The robot then mounts the tape. At the start of the operation, the application (for example, NetBackup) checks the media ID and if it also matches what should be in this slot, the operation proceeds. For NetBackup, a wrong media ID results in a "media manager found wrong tape in drive" error (NetBackup status code 93).

Figure B-4 Barcode request



Media and device management components

This topic shows the file and directory structure and the programs and daemons associated with the media management and device management.

Figure B-5 shows the file structure and directory structure for media management and device management on a UNIX server. A Windows NetBackup server has equivalent files and directories that are located in the directory where NetBackup is installed (by default, C:\Program Files\VERITAS).

Figure B-5 Media and device management directories and files

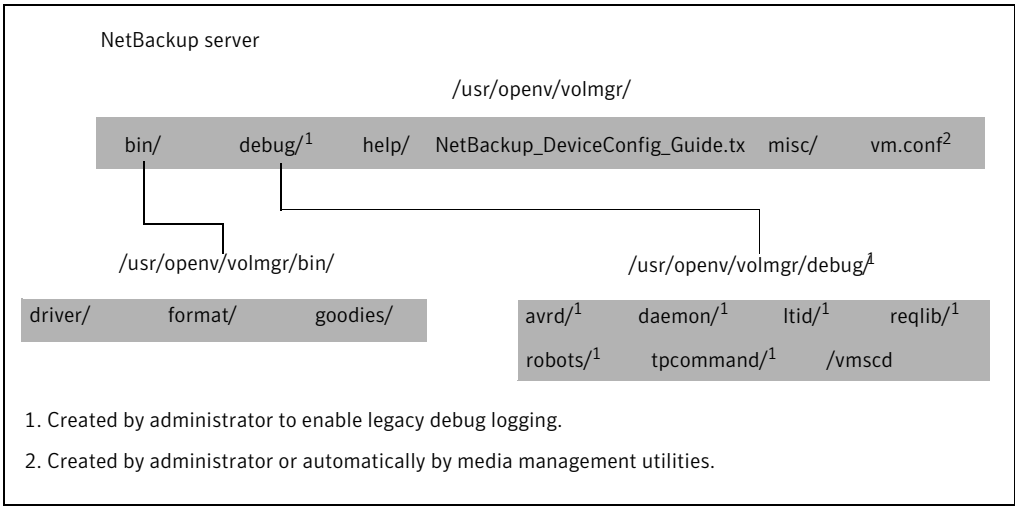


Table B-1 describes the directories and files that are of special interest.

Table B-1 Media and device management directories and files

File or directory	Contents
bin	Commands, scripts, programs, daemons, and files required for media and device management. Three subdirectories under bin are available. driver: Contains the SCSI drivers used on various platforms to control robotics. format: Disk format information for optical platters on Solaris (SPARC only) platforms. goodies: Contains the `vmconf` script and scan utility.
debug	Legacy debug logs for the Volume Manager daemon, `vmd`, and all requesters of `vmd`, `ltid`, and device configuration. The administrator must create these directories for debug logging to occur.
help	Help files that are used by media and device management programs. These files are in ASCII format.

Table B-1 Media and device management directories and files *(continued)*

File or directory	Contents
misc	Lock files and temporary files that are required by various components of media and device management.
vm.conf	Media and device management configuration options.

Table B-2 describes the media management and device management programs and daemons. The explanations include what starts and stops the program or daemon, and the log (if any) where it records its activities. On UNIX, all of the components discussed in this table reside under `/usr/openv/volmgr/bin`. On Windows, they reside under `install_path\volmgr\bin`.

Note: The following table contains references to the system log. This log is managed by syslog on UNIX (the facility is daemon). On Windows the Event Viewer manages the system log (the log type is Application).

Table B-2 Media and device management daemons and programs

Program or daemon	Description
acsd	The Automated Cartridge System daemon interfaces with the Automated Cartridge System. It communicates with the server that controls the ACS robotics through the `acsssi` process (UNIX) or the STK Libattach Service (Windows). Also, for UNIX, see the `acsssi` and acssel programs. **Started By**: Starting ltid (or on UNIX, independently by using the `/usr/openv/volmgr/bin/ascd` command. **Stopped By**: Stopping ltid (or on UNIX, independently by finding the PID (process id) and then using the kill command). **Debug Log**: Errors are logged in the system log and robots debug log. Debug information is included by adding VERBOSE to the vm.conf file. On UNIX, debug information is also included by starting the daemon with the -v option: this option can also be used through ltid, or by putting VERBOSE in the vm.conf file.
acssel	Available only on UNIX. See the NetBackup Device Configuration Guide.

Table B-2 Media and device management daemons and programs *(continued)*

Program or daemon	Description
acsssi	Available only on UNIX. See the NetBackup Device Configuration Guide.
avrd	The automatic-volume-recognition daemon controls automatic volume assignment and label scanning. This lets NetBackup read labeled tape and optical disk volumes and to automatically assign the associated removable media to requesting processes. **Started By**: Starting `ltid` (or on UNIX, independently by using the /usr/openv/volmgr/bin/avrd command). **Stopped By**: Stopping `ltid`, (or on UNIX, independently by finding the PID (process id) and then using the kill command). **Debug Log**: All errors are logged in the system log. Debug information is included by adding VERBOSE to the vm.conf file. On UNIX, debug information is also included by aborting avrd and starting the daemon with the -v option.
ltid	The device demon (UNIX) or NetBackup Device Manager service (Windows) controls the reservation and assignment of tapes and optical disks. **Started By**: /usr/openv/volmgr/bin/ltid command on UNIX or Stop/Restart Device Manager Service command in Media and Device Management window on Windows. **Stopped By**: /usr/openv/volmgr/bin/stopltid command on UNIX or Stop/Restart Device Manager Service command in the **Media and Device Management** window on Windows. **Debug Log**: Errors are logged in the system log and `ltid` debug log. Debug information is included if the daemon is started with the -v option (available only on UNIX) or adding VERBOSE to the vm.conf file.

Table B-2 Media and device management daemons and programs *(continued)*

Program or daemon	Description
odld	The Optical Disk Library daemon interfaces with the Optical Disk Library, communicating with the robotics through a SCSI interface. This library is not supported on Windows. **Started By**: Starting ltid or independently by using the /usr/openv/volmgr/bin/odld command. **Stopped By**: Stopping ltid or independently by finding the PID (process id) and then using the kill command. **Debug Log**: All errors are logged in the system log. Debug information is included if the daemon is started with the -v option (either by itself or through ltid) or adding VERBOSE to the vm.conf file.
tl4d	The Tape Library 4MM daemon is the interface between `ltid` and the Tape Library 4MM and communicates with the robotics through a SCSI interface. **Started By**: Starting `ltid` (or on UNIX, independently by using the /usr/openv/volmgr/bin/tl4d command). **Stopped By**: Stopping ltid (or on UNIX, independently by finding the PID (process id) and then using the kill command). **Debug Log**: All errors are logged in the system log. Debug information is included by adding VERBOSE to the vm.conf file. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through `ltid`).

Table B-2 Media and device management daemons and programs *(continued)*

Program or daemon	Description
tl8d	The Tape Library 8MM daemon provides the robotic control for a TL8 robot (Tape Library 8mm or Tape Stacker 8mm). The Tape Library 8MM daemon drives in the same TL8 robot may be attached to different hosts than the robotic control. tl8d is the interface between the local `ltid` and the robotic control. If a host has a device path for a drive in a TL8 robot, then mount or unmount requests for that drive go first to the local ltid and then to the local tl8d (all on the same host). tl8d then forwards the request to tl8cd on the host that is controlling the robot (could be on another host). **Started By**: Starting `ltid` (or on UNIX, independently by using the /usr/openv/volmgr/bin/tl8d command). **Stopped By**: Stopping `ltid` (or on UNIX, independently by finding the PID (process id) and then using the kill command. **Debug Log**: Errors are logged in the system log and robots debug log. Debug information is included by adding VERBOSE to the vm.conf file. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through `ltid`).
tl8cd	The tape library 8MM control daemon provides the robotic control for a TL8 robot and communicates with the robotics through a SCSI interface. tl8cd receives mount and unmount requests from tl8d on the host to which the drive is attached and then communicates these requests to the robot. **Started By**: Starting `ltid` (or on UNIX, independently by using the `/usr/openv/volmgr/bin/tl8cd command`). **Stopped By**: Stopping `ltid` or by using the `tl8cd -t` command. **Debug Log:** Errors are logged in the system log and robots debug log. Debug information is included by adding VERBOSE to the vm.conf file. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through `ltid`).

Table B-2 Media and device management daemons and programs *(continued)*

Program or daemon	Description
tldd	The Tape Library DLT daemon works in conjunction with tldcd to handle requests to TLD robots (Tape Library DLT and Tape Stacker DLT). tldd provides the interface between the local `ltid` and the robotic control (tldcd) in the same manner as explained previously for tl8d. **Started By**: Starting `ltid` (or on UNIX, independently by using the /usr/openv/volmgr/bin/tldd command). **Stopped By**: Stopping `ltid` (or on UNIX, independently by finding the PID (process id) and then using the kill command). **Debug Log**: Errors are logged in the system log and robots debug log. Debug information is included by adding VERBOSE to the vm.conf file. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through `ltid`).
tldcd	The tape library DLT control daemon provides robotic control for a TLD robot in the same manner as explained previously for tl8cd. **Started By**: Starting `ltid` (or on UNIX, independently by using the /usr/openv/volmgr/bin/tldcd command). **Stopped By**: Using the tldcd -t command. Stopping `ltid` or by using the tldcd -t command. **Debug Log**: Errors are logged in the system log and robots debug log. Debug information is included by adding VERBOSE to the vm.conf file. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through `ltid`).
tlhd	The Tape Library Half-inch daemon works in conjunction with tlhcd to handle requests to TLH robots that are in an IBM Automated Tape Library (ATL). tlhd provides the interface between the local ltid and the robotic control (tlhcd) in the same manner as explained previously for tl8d. **Started By**: Starting `ltid` (or on UNIX, independently by using the /usr/openv/volmgr/bin/tlhd command). **Stopped By**: Stopping `ltid` (or on UNIX, independently by finding the PID (process id) and then using the kill command). **Debug Log**: Errors are logged in the system log and robots debug log. Debug information is included by adding VERBOSE to the vm.conf file. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through `ltid`).

Table B-2 Media and device management daemons and programs *(continued)*

Program or daemon	Description
tlhcd	The tape library half-inch control daemon provides robotic control for a TLH robot that is in an IBM Automated tape library (ATL) in a similar manner to that which was explained previously for `tl8cd`. **Started By**: Starting `ltid` (or on UNIX, independently by using the /usr/openv/volmgr/bin/tlhcd command). **Stopped By**: Stopping `ltid` or by using the tlhcd -t command. **Debug Log**: Errors are logged in the system log and robots debug log. Debug information is included if the daemon is started with the -v option (either by itself or through `ltid`). The -v option is available only on UNIX. Also, add the VERBOSE option to the vm.conf file.
tlmd	The Tape Library Multimedia daemon is the interface between `ltid` and a TLM robot that is in an ADIC Distributed AML Server (DAS). This daemon communicates with the TLM robotics through a network API interface. **Started By**: Starting `ltid` or independently by using the /usr/openv/volmgr/bin/tlmd command. **Stopped By**: Stopping `ltid` or independently by finding the PID (process id) and then using the kill command. **Debug Log**: Errors are logged in the system log and robots debug log. Debug information is included if the daemon is started with the -v option (either by itself or through `ltid`). The -v option is available only on UNIX. Also, add the VERBOSE option to the vm.conf file.
tpconfig	The tape library Multimedia daemon is the interface between `ltid` and a TLM robot that is in an ADIC Distributed AML Server (DAS). This daemon communicates with the TLM robotics through a network API interface. **Started By**: Starting `ltid` or independently by using the /usr/openv/volmgr/bin/tlmd command. **Stopped By**: Stopping `ltid` or independently by finding the PID (process id) and then using the kill command. **Debug Log**: Errors are logged in the system log and robots debug log. Debug information is included if the daemon is started with the -v option (either by itself or through `ltid`). The -v option is available only on UNIX. Also, add the VERBOSE option to the vm.conf file.

Table B-2 Media and device management daemons and programs *(continued)*

Program or daemon	Description
tshd	The Tape Stacker Half-inch daemon is the interface between `ltid` and the half-inch-cartridge stacker and communicates with the robotics through a SCSI interface. This robot is not supported on Windows. **Started By**: Starting `ltid` (or on UNIX, independently by using the /usr/openv/volmgr/bin/tshd command). **Started By**: `tpconfig` command. **Stopped By**: Quit option from within the utility on UNIX. On Windows, `tpconfig` is only a command-line interface that runs to completion (no quit option). **Debug Log**: tpcommand debug logs.
vmd	The Volume Manager daemon (NetBackup Volume Manager service on Windows) allows remote administration and control of Media and Device Management. **Started By**: Starting ltid (or on UNIX, independently by using the Initiate Media Manager Volume Daemon option in vmadm) **Stopped By**: Terminate Media Manager Volume Daemon option in vmadm). **Debug Log**: System log and also a debug log if the daemon or reqlib debug directories exist
vmadm	Available only on UNIX. An administrator utility with options for configuring and managing volumes under control of media and device management. It has a menu-driven, character-based interface that can be used from workstations that do not have graphical display capabilities. **Started By**: /usr/openv/volmgr/bin/vmadm command **Stopped By**: Quit option from within the utility. **Debug Log**: /usr/openv/volmgr/debug/reqlib
vmscd	The Media Manager Status Collector Daemon keeps the EMM server database up-to-date with the actual status of drives attached to 5.x servers. **Started By**: the EMM server. **Stopped By**: the EMM server. **Debug Log**: /usr/openv/volmgr/debug/vmscd (UNIX), install_path\Volmgr\debug\vmscd (Windows)

Index

A

acssel, description 334
acsssi, description 335
acstest 125
Adaptive Server Anywhere 69
admin log 159
admincmd
    directory 309
administration interface
    activity logging 176
    errors 174
AdvancedDisk 208, 216
Alternate client restores
    host.xlate file 52
altnames file 322
application server status codes (Java interface) 174
archiving
    for NBCC 113
    for nbsu 109
ascd, description 334
Auth User
    for PBX 75
auto-configuration problems 31
avrd, description 335

B

backup
    NetBackup catalogs 296
    process
        multiplexing 281
        Windows clients 291
    process overview 282, 289
    snapshot overview 285
    synthetic processes 292
    UNIX clients 280
Bare Metal Restore 206, 208, 223
bin
    Media and Device Management 333
    UNIX client 307, 309
bp
    description 311
bp *(continued)*
    UNIX client log 154
bp.conf
    file 281
        UNIX client/server 309
    SERVER entries 91
bp.kill_all 77–78
bp.start_all 78
bpadm
    description 311
bparchive
    description 311
    log 154, 156
bpbackup
    description 311
    log 154, 156
bpbackup log 156
BPBACKUP_POLICY 281
BPBACKUP_SCHED 281
bpbkar
    description 312
    log 154, 156
bpbkar log 156
BPBKAR32 291, 312
bpbrm 287
    description 312
bpbrm log 159
bpcd
    description 312
    server log 159
    UNIX client log 154, 156
BPCDW32.EXE 313
bpdbjobs
    description 313
bpdbjobs log 159
bpdbm
    description 313
bpdbm log 159
bpdm
    description 313
bpdm log 159
bpdown command 77, 79, 219, 222

bpfis 287, 314
bphdb
description 314
log 154
BPINETD 291, 303
bpinetd log 156
bpinetd.log 156
bpjava-msvc 314–315
bpjava-msvc log 160, 177
bpjava-usvc log 177
bplist
description 315
log 154, 157
bplist log 157
bpmount
log 154
bpmount log 157
bporaexp log 155
bporaexp64 log 155
bporaimp log 155
bporaimp64 log 155
bpps 25
bprd
description 315
bprd log 160
bprestore
description 316
log 155, 157
bprestore log 157
bpsched
see also nbpem 319
bpsynth 292
bptm
description 316
bptm log 160
bptpcinfo 97
bpup command 79, 219
bundling
NBCC output 113
nbsu output 109

C

catalog backup 296
catalog recovery
catalog image files 243
clustered master server 243
class database file 322
client
NetBackup
configured name 50
debug logs. *See* UNIX clients. *See* Windows and NetWare clients
installation problems 29
multiple hostnames 49
peername 49
software location. *See* UNIX clients
testing configuration 35, 38
Client Properties dialog 68
client, NetBackup
Windows disk recovery 223
CommandCentral Storage 93
communications problems
PC clients 46
UNIX clients 42
compression
for NBCC 113
for nbsu 109
config file 322
configuration database 322
configuration problems 29

D

daemons
robotic 324
robotic control 324
database backup (see catalog backup) 296
DAYS_TO_KEEP_LOGS vm.conf setting 164
db directory
NetBackup 307, 309
debug level 169
debug logs 176
analysis utilities 100
NetBackup 333
vmd 161, 333
debug.properties file 177
debugging
NBCC 112
nbsu 106
device configuration problems 31
Device Configuration Wizard 218
directory structure
Media and Device Management 332
disaster recovery
preparing for disaster 204
disk full 68

disk recovery
Windows client 223
disk space
for logs files 150
drive_mount_notify script 327
drive_unmount_notify script 327
driver directory 333
duplex mode and performance 90

E

E-mail 207
EMM server 280
enable debug logging 161
Enable robust logging 165
Enterprise Media Manager (EMM) 280
error database 323
Event viewer logging option 171
eventlog 172
file entries 172
exception errors in Java admin interface 174

F

failure_history file 323
fibre channel 288
file database 323
files
restore process 296
format directory 333
FSM 288
FT Service Manager 288
full disk 68
full duplex mode 90
functional overview
introduction 278
Media and Device Management
device management 326
directories and files 332
volume management 326
NetBackup
restores 296
startup 279

G

Global Logging Level 162
Global logging level 167–168
goodies
directory 309
goodies directory 333

H

Half duplex and poor performance 90
help files
Media and Device Management 333
UNIX client 309
host name entries
checking 53
Host Properties 67
host.xlate file 52
hostID
unified logging 133

I

ifconfig
for checking NIC duplex mode 90
images database 323
importing backups 274, 276
inetd 29
Information E-mail 207
installation
Linux 29
installation problems 28
ipconfig
for checking NIC duplex mode 90

J

Java interface
debug logging 176
troubleshooting background 174
jbpSA
overview 316
job ID search in unified logs 148
jobs
queued for long periods 68
jobs database 323

K

Keep logs For setting 142
Keep Logs setting 163

L

legacy logging 153
client logs 154
configuring rotation 165
controlling size of 163
directories 153
file name format 158

legacy logging *(continued)*
locations 153
PC clients 155
rotation of 164
levels for logging 167
Linux 29
log analysis utilities
debug logs 100
limitations 103
output format 104
Log level
Windows clients 169
logging
changing location of 140
levels 167
see legacy logging 153
setting level on PC clients 169
synthetic backup 170
logs
debug
enabling detailed 176
event viewer logging option 171
file retention 142
overview[Logs
aaa] 127
PC client activity
bparchive 156
bpbackup 156
bpbkar 156
bpcd 156
bpinetd 156
bplist 157
bpmount 157
bprestore 157
tar 157
user_ops 158
reports
NetBackup 128
server activity
acssi 161
admin 159
bpbrm 159
bpcd 159
bpdbjobs 159
bpdbm 159
bpdm 159
bpjava-susvc 160
bprd 160
bpsynth 160
logs *(continued)*
server activity *(continued)*
bptm 160
daemon 161
ltid 161
nbatd 134, 160
nbazd 160
nbjm 135
nbpem 135
reqlib 161
robots 161
syslogs 160
tpcommand 162
setting retention period 163
system 129
UNIX client activity
bp 154
bparchive 154
bpbackup 154
bpbkar 154
bpcd 154
bphdb 154
bpjava-msvc 160
bplist 154
bpmount 154
bprestore 155
obackup_tape 155
tar 155
user_ops 155
logs directory
UNIX client/server 309
ltid 163
ltid, description 335

M

master server
test procedure 35, 39
MaxLogFileSizeKB 150–152, 165
media database 323
media server
test procedure 38
misc file 334
mklogdir.bat 153
moving log locations 140
multiplexed backups 281

N

name format
    legacy logging 158
NB_dbsrv daemon 69
nbatd log 160
nbaudit 317
nbazd log 160
NBCC
    archiving and compression 113
    does the following 112
    introduction 111
    location of 112
    nbcc-info.txt file 113
    Notes on running 112
    output 113
    progress display 114
    troubleshooting 112
    when to use 112
nbcc-info.txt file 113
nbdb_move 218
nbemm 25, 280, 317
nbfdrv64 317
nbftclnt 288, 290, 302, 318
    and bp.conf 91
nbftsrvr 288, 290, 302, 318
nbjm 25, 135, 280, 287, 292, 318–319
nbpem 25, 135, 279–280, 287, 292, 319
nbproxy 319
nbrb 25, 69, 280, 319
nbrmms 320
nbstserv 320
nbsu
    and status codes 110
    archiving and compression 109
    bundling 109
    creating xml output file 109
    introduction 105
    location of 105
    nbsu_info.txt file 107
    output files 107
    progress display 110
    troubleshooting 106
    when to use 106
nbsu_info.txt file 107
NBWIN 291, 303
ndmpagent
    overview 319
NetBackup
    if unresponsive 68
NetBackup *(continued)*
    product ID 133
NetBackup Administration Console
    debug logging 176
    errors 174
NetBackup Client Service
    start and stop 27
NetBackup consistency check
    see NBCC 111
NetBackup Database Manager service
    start and stop 27
NetBackup Device Manager service
    start and stop 27
NetBackup Enterprise Media Manager service
    start and stop 27
NetBackup Job Manager service
    start and stop 27
NetBackup Policy Execution Manager service
    start and stop 27
NetBackup Request Manager service
    start and stop 27
NetBackup Resource Broker service
    start and stop 27
NetBackup Status Collection daemon.. *See* vmscd
NetBackup Support Utility
    see nbsu 105
NetBackup Volume Manager service
    start and stop 27
network connections
    multiple 49
network daemon (vnetd) 161
network interface cards 90
network problems
    PC clients 46
    UNIX clients 42
NIC cards and full duplex 90
NumberOfFiles 150
NumberOfLogFiles 152, 165

O

obackup_tape log 155
odld, description 336
odltest 124
off-host backup 97
OpenStorage 208, 216
operating system errors 175
originator IDs
    list of 134

originatorID
    unified logging 133

P

patches (installing during recovery) 224
PBX
    Auth User 75
    logging 76
    Secure Mode 75, 77
    starting 74
    starting/stopping 77
    troubleshooting 73
pbx_exchange 74, 320
pbxcfg 75
preliminary troubleshooting procedure 22
Private Branch Exchange (PBX) 73
procedures
    recovery
        Windows client disk 223
    troubleshooting
        communications problems 41, 46
        host names and services 53
        installation and configuration 28
        introduction 20
        master server and clients 35
        media server and clients 38
        preliminary 22
processes (see functional overview) 278
product ID for NetBackup 133
productID
    unified logging 133

Q

ql2300_stub 321
query string 144
queued jobs 68

R

raw partitions
    restore process 296
recording information 14
recovery procedures
    Windows client disk 223
RedHat 29
relational database 69
reports
    NetBackup 128
reqlib directory 153
restore process 296
    Windows 2000 client 303
retention
    of logs 142
robot drive selection 327
robotic control daemons 325
robotic daemons 325
robotic test utility 123
    acstest 125
    odltest 124
    tl4test 124–125
    tl8test 124–125
    tldtest 124–125
    tlhtest 125
    tshtest 124
robtest 124–125
robust file logging 151
RolloverMode 152
rotation
    legacy logging 164
    of logs 141
    unified logging 133

S

SAN Client 288
SAN client
    and bp.conf 91
SANPoint Control 93
Secure Mode
    for PBX 75
server
    installation problems 28
    NetBackup debug logs 153
    test procedure for master 35, 39
    test procedure for media server 38
SERVER entries
    bp.conf 91
services entries
    checking 53
SharedDisk 208, 216
slow performance and NIC cards 90
snapshot
    backup process overview 286
software version
    determining
        UNIX client/server 310
starting NetBackup processes 78
startup
    NetBackup 279

status codes
and nbsu 110
Status Collection Daemon 153
stderr 174
stdout 174
stopping NetBackup processes 77–78
storage units 91
SuSE 29
synthetic backup 292
logs 170
syslogd 129
system logs 129

T

tar
log 157
log files 132
NetBackup 321
TAR32 303
test utility
robotic 123
tl4d, description 336
tl4test 124–125
tl8cd, description 337
tl8d, description 337
tl8test 124–125
tldcd, description 338
tldd, description 338
tldtest 124–125
tlhcd, description 339
tlhd, description 338
tlhtest 125
tlmd, description 339
tpautoconf 162, 211
tpconfig 162
tpconfig, overview 339
traceroute 52
troubleshooting procedure
communication problems
PC clients 46
UNIX clients 42
general
master server and clients 35, 39
media server and clients 38
host name and services entries 53
installation 28
preliminary 22
try file 170
tshd, overview 340
tshtest 124

U

unavailable 91
unified logging 129
changing location of 140
client logs 154
configuring settings 151
controlling disk space usage 150
controlling number of log files 150
controlling size of 151
deleting logs 149
file name format 133
file rotation 141
format of files 143
listing settings 152
location 130
message types 132
NetBackup product ID 133
processes using 134
retention 142
setting level on PC clients 169
settings levels 167
submitting to Technical Support 131
tar log files 132
upload directory 132
user-directed backups 281
user_ops log 155, 158, 160
utility
robotic test 123

V

VERBOSE 163
verbose flag 163
VERBOSE level 168
vm.conf 163
vm.conf file 334
vmadm, overview 340
vmd 161
debug logging 161
overview 340
vmscd 153
logging 162
vmscd, overview 340
vnetd log 161
Volume Configuration Wizard 218
vxlogcfg 140, 165
vxlogcfg command 151–152, 168

vxlogmgr command 148, 150
vxlogview command 143
    query string overview 144
    with job ID option 148
vxpbx_exchanged 77

W

Windows open file backup 286
windrvr6 322

X

xinetd 29
XML 155
xml
    for nbsu 109