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: 7.0.1

Legal Notice

Copyright © 2010 Symantec Corporation. All rights reserved.

Symantec and the Symantec 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.
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 Web site 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:


**Customer service**

Customer service information is available at the following URL:


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 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
## Technical Support

---

### Chapter 1  Introduction

- About Troubleshooting ................................................................. 13
- Define the problem ....................................................................... 13
  - What was the error indication? ................................................. 13
  - What were you doing when the problem occurred? ................. 14
- Record all information ................................................................. 15
- Troubleshooting the problem ....................................................... 16
- About gathering information for problem reports ....................... 16
  - General information ............................................................... 17
  - Gathering information for NetBackup-Java ............................. 18

### Chapter 2  Troubleshooting procedures

- About troubleshooting procedures ............................................ 21
- Preliminary troubleshooting ....................................................... 22
- Troubleshooting installation and configuration problems ........... 27
  - Resolving installation problems ............................................ 27
  - Resolving common configuration problems .............................. 28
- General test and troubleshooting procedures ............................ 33
  - Testing the master server and clients .................................... 33
  - Testing media server and clients ........................................... 37
  - Resolving network communication problems ......................... 40
- Verifying host name and service entries ................................... 48
- Using bpclntcmd ....................................................................... 52
  - Host name and service entry examples - UNIX ....................... 53
- Using the Host Properties window ............................................ 60
- Resolving full disk problems .................................................... 61
- Troubleshooting frozen media ................................................... 62
- Resolving PBX problems ............................................................ 66
  - Checking for PBX installation ............................................... 66
  - Checking that PBX is running ................................................ 67
  - PBX must be set correctly ..................................................... 67
- PBX logging ............................................................................ 68
- PBX security ............................................................................ 69
| Required NetBackup daemon or service not available | 70 |
| New network interface cards | 71 |
| Backup performance and NIC cards | 71 |
| SERVER entries in bp.conf file | 72 |
| Resolving unavailable storage units problems | 73 |
| Troubleshooting NetBackup in a SAN environment | 73 |
| NetBackup enterprise lifecycle: best practices | 74 |
| Using CommandCentral Storage to troubleshoot NetBackup | 75 |
| Common NetBackup troubleshooting use cases | 76 |

**Chapter 3**

**Using logs and reports**

| About using logs and reports | 79 |
| Where is the log and report information? | 80 |
| Reports | 81 |
| Status for user operations | 83 |
| UNIX system logs | 83 |
| Debug logs on servers | 83 |
| Unified logging | 83 |
| Configuring and using unified logging | 93 |
| Submitting unified logging files to & CompanyName; support | 100 |
| Legacy NetBackup logging | 101 |
| Logs to accompany problem reports for synthetic backup | 111 |
| Debug logs on UNIX clients | 113 |
| Unified logging on UNIX clients | 113 |
| Legacy logging on UNIX clients | 113 |
| Controlling log size on UNIX clients | 115 |
| Client logging file name format on UNIX clients | 115 |
| How to set logging levels on UNIX clients | 116 |
| Debug logs on PC clients | 116 |
| Unified logging on PC clients | 116 |
| Legacy debug logging on PC clients | 116 |
| Controlling log size on PC clients | 119 |
| Client logging file name format on PC clients | 120 |
| How to set logging levels on PC clients | 120 |
| Windows Event Viewer logging option | 120 |
| Enabling the logging tool | 121 |
| eventlog file entries | 121 |
| Example | 122 |
| Troubleshooting the Administration Console for UNIX | 123 |
| Required disk space for logging and temporary files | 124 |
Chapter 4 Using NetBackup utilities ..................................................... 129
About using NetBackup utilities .......................................................... 129
Analysis utilities for NetBackup debug logs ......................................... 129
Installation requirements .................................................................. 130
Output format .................................................................................... 130
Limitations .......................................................................................... 131
How to run the log analysis utilities .................................................... 131
Network troubleshooting utilities .......................................................... 134
NetBackup support utility (nbsu) .......................................................... 135
  When to use nbsu ............................................................................ 135
  nbsu progress display ..................................................................... 136
  nbsu output ...................................................................................... 137
  nbsu and NetBackup status codes .................................................... 139
  Notes on running nbsu ................................................................... 140
NetBackup consistency check (NBCC) .................................................... 141
  When to use NBCC ........................................................................ 142
  NBCC progress display .................................................................. 142
  Server aliases file .......................................................................... 145
  NBCC output .................................................................................. 146
  Notes on running NBCC ................................................................. 147
NetBackup consistency check repair (NBCCR) ...................................... 149
  NBCCR files .................................................................................. 150
The nbcplogs utility .......................................................................... 151

Chapter 5 NetBackup status codes and messages ................................. 153
About NetBackup status codes and messages .................................... 153
  NetBackup status codes ............................................................... 154
  NetBackup Messages ..................................................................... 397

Chapter 6 Media and device management status codes and messages ............................................................................. 421
About media and device management status codes and messages .......................................................... 421
  Using debug logs .......................................................................... 422
  Media Manager status codes .......................................................... 422
Appendix A  Backup and restore functional overview ........................................ 631
About backup and restore functional overview ........................................ 631
Backup and restore startup process ....................................................... 632
Backup and archive processes .............................................................. 632
  Job scheduling .................................................................................. 632
  EMM server and master server .......................................................... 633
Backups and archives - UNIX clients .................................................... 633
  Backup process ................................................................................ 634
  Backup with multiple UNIX data streams ........................................... 638
  Snapshot backup and Windows open file backups ............................... 639
  SAN client ...................................................................................... 642
Backups and archives - Windows ............................................................ 645
Backups and archives - NetWare clients ................................................. 646
  Synthetic backups .......................................................................... 647
NetBackup online, hot catalog backup .................................................. 650
Restore processes ................................................................................. 652
  Restoring UNIX and Linux clients ..................................................... 652
  Restoring SAN client (UNIX or Windows) .......................................... 656
  Restoring Windows clients .............................................................. 659
  Restoring NetWare clients .............................................................. 660
  Restoring catalog backups ............................................................. 662
NetBackup directories and files ............................................................. 663
  NetBackup directory structure - UNIX ............................................... 664
  Contents of /usr/openv/netbackup .................................................... 666
NetBackup programs and daemons ......................................................... 667
NetBackup catalogs ............................................................................. 680

Appendix B  Media and device management functional description ........................................ 683
Media and device management startup process ...................................... 683
Media and device management process ................................................ 685
Shared Storage option management process ........................................ 687
Barcode operations .............................................................................. 689
Media and device management components ........................................ 691

Appendix C  Networks and hostnames ........................................ 701
Background for troubleshooting .................................................. 701

Appendix D  Robotic test utilities .................................................. 707
About robotic test utilities ............................................................ 707
Robotic tests on UNIX .............................................................. 707
Robotic tests on Windows ......................................................... 708

Index .............................................................................................. 711
Introduction

This chapter includes the following topics:

- About Troubleshooting
- Define the problem
- Record all information
- Troubleshooting the problem
- About gathering information for problem reports

About Troubleshooting

This chapter explains the steps to take if you encounter a problem while you use NetBackup. Other chapters provide more specific information.

Note: The term "media server", as distinct from "master server" or "server", may or 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. You can ignore references to a media server on a different host.

Define the problem

The first step in troubleshooting is to define the problem.

What was the error indication?

To define the problem, you must know what went wrong. Sometimes the resolution of the problem also requires that you know what went right.
Error messages are usually the vehicle for telling you something went wrong. So the first thing to do is to look for an error message. 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. The log information that NetBackup provides is available:

See “About using logs and reports” on page 79.

The following chapters provide interpretations of NetBackup (and Media Manager) status codes and messages.

What were you doing when the problem occurred?

Another important part in troubleshooting the problem is to define what you tried to do in the first place.

Some questions to ask are as follows:

- 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 and the media servers, was it a master 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?
Record all information

As you define and troubleshoot a problem, always try to capture potentially valuable information, such as the following:

- 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. A benefit of this approach is that you can compare the results of multiple tries. A record of tries is also useful for others at your site and for customer support in the event that you cannot solve the problem. Explanations of the various logs are available.

See “About using logs and reports” on page 79.

On UNIX systems, the /usr/openv/netbackup/bin/goodies/support script 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.

If your troubleshooting try is unsuccessful, customer support can provide further assistance. Before you call, have the following information ready:

- 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 hotfixes that were installed.

What is the definition of the problem as described earlier in this chapter? Copies of logs or core dumps (if any) can also be required.

Have you had this problem before? If so, was there a successful resolution and what did you try that time?

Has the configuration recently changed? If so, what changed?

If necessary, can you communicate with technical support through ftp, email, or fax? These are useful for when you send information such as copies of logs.

The following topic contains the information you need and also provides methods for gathering information.

See “About gathering information for problem reports” on page 16.

Troubleshooting the problem

After you define the problem, use the following information in the other chapters of this manual to correct it:

- When you have a status code or message, the recommended corrective action is available.
  See “About NetBackup status codes and messages” on page 153.
  See “About media and device management status codes and messages” on page 421.

- If no status code or message exists, or the actions in the status code chapters do not solve the problem, check the following topic:
  See “About troubleshooting procedures” on page 21.
  Those procedures describe an effective approach for isolating common problems.

If you don’t find the solution, contact customer support.

The &CompanyName; Technical Support site has a wealth of information that can help you solve NetBackup problems.

For comprehensive troubleshooting details, refer to the following URL:

www.symantec.com/business/support/

About gathering information for problem reports

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

Date: _________________________

Table 1-1  Servers (master_and_media)

<table>
<thead>
<tr>
<th>Platform types and host names</th>
<th>OS Levels</th>
<th>Product version and patch levels</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1-2  Clients

<table>
<thead>
<tr>
<th>Platform types and host names</th>
<th>OS Levels</th>
<th>Product version and patch levels</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1-3  Devices

<table>
<thead>
<tr>
<th>Robotic library and drive models</th>
<th>Firmware levels</th>
<th>Tested firmware level that is listed in the NetBackup hardware compatibility list</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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)
Gathering information for NetBackup-Java

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

The following scripts are available for gathering information:

- The NetBackup-Java administration application startup script, jnbSA, logs data to 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.

- The NetBackup-Java administration application on Windows logs data to 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.

- The /usr/openv/java/get_trace script 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 (see previous bullet).
The `/usr/openv/netbackup/bin/goodies/support` script 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`.

**To get debug data for support to analyze**

1. If the application does not respond for a long time, it may be hung. However, some operations can take quite a while to complete, especially Activity Monitor and Reports applications. Wait for several minutes before you assume that the operation is hung.

   If there is no response within 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.

2. Run `/usr/openv/netbackup/bin/goodies/support` to get data about your configuration. Run this script after you complete the NetBackup installation and every time you change the NetBackup configuration.

3. Provide the support-script output and log file to &CompanyName; support.
Introduction

About gathering information for problem reports
Troubleshooting procedures

This chapter includes the following topics:

■ About troubleshooting procedures
■ Preliminary troubleshooting
■ Troubleshooting installation and configuration problems
■ General test and troubleshooting procedures
■ Using the Host Properties window
■ Resolving full disk problems
■ Troubleshooting frozen media
■ Resolving PBX problems
■ New network interface cards
■ Backup performance and NIC cards
■ SERVER entries in bp.conf file
■ Resolving unavailable storage units problems
■ Troubleshooting NetBackup in a SAN environment

About troubleshooting procedures

This chapter has procedures for finding the cause of NetBackup errors. These procedures 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 &CompanyName; Technical Support site has a wealth of information that can help you solve NetBackup problems. See the following site for comprehensive troubleshooting details:

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.

Preliminary troubleshooting explains what to check first. It branches off to other procedures as appropriate.

Troubleshooting installation and configuration problems apply specifically to installation problems and configuration problems.

General test and troubleshooting procedures define general methods for finding server and client problems and should be used last.

---

**Note:** The term "media server", as distinct from "master server" or "server", does not apply to the NetBackup server product. When you troubleshoot a NetBackup server installation, ignore any references to media server. (This note does not apply to NetBackup Enterprise Server.)

---

**Preliminary troubleshooting**

Preliminary troubleshooting explains what to check first and branches to other procedures as appropriate.
To troubleshoot problems with NetBackup

1  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 device compatibility lists on the following Web site:

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

2  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.

   If the problem involved a backup or archive, check the Backup Status 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 “About NetBackup status codes and messages” on page 153.

   See “About media and device management status codes and messages” on page 421.

3  Check the system log 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 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.

4  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 using logs and reports” on page 79.

5  If you performed corrective actions, retry the operation. If you did not perform corrective actions or the problem persists, continue with the next step.

6  If you see the problem during a new installation, during an upgrade installation, or after you make changes to an existing configuration, see the following:

   See “Troubleshooting installation and configuration problems” on page 27.
7  Ensure that the server and client 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 disaster recovery” on page 569.

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.

8  Enable verbose logging either for everything or only for areas you think are 
related to the problem.

See “About using logs and reports” on page 79.

9  Determine which daemons or processes are running. Follow the procedures 
for UNIX or Windows NetBackup servers.

To troubleshoot problems on UNIX NetBackup servers

1  Run the following:

   /usr/openv/netbackup/bin/bpps -a

2  If the master server is also the EMM server, ensure that the nbemm and the 
nbrb services are running. If these services are not running, start them by 
entering the following:

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

   If both nbemm and nbrb are not running, they must be started in this sequence. 
   If only one is not running, start it by using the appropriate command.
3 The `nbpem` and the `nbjm` services must be running on the master server. If these services are not running, start them by entering the following:

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

If both `nbjm` and `nbpem` are not running, they must be started in this sequence. If only one is not running, start it by using the appropriate command.

4 If either the NetBackup request daemon (bprd) or database manager daemon (bpdbm) is not running, run this command to start them:

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

5 If any of the following media and device management processes are not running:
   - `ltid` (*ltid* only needs to be running 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 Stop the device daemon, `ltid`, by running:

```
/usr/openv/volmgr/bin/stopttid
```

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

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

If you use ACS robotic control, the `acsssi` and the `acssel` processes continue to run when `ltid` is stopped. For more information about how to stop these daemons, refer to the following:

See the Automated Cartridge System (ACS) chapter in the *NetBackup Device Configuration Guide*.

8 Stop any robot control daemons that continue to run when `ltid` is terminated. Then, start all daemons by running:

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

For debugging, start `ltid` with the `-v` (verbose) option.
To troubleshoot problems on Windows NetBackup servers

1. 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 them, run `install_path\NetBackup\bin\bpup.exe`.

   The following services must be running on NetBackup 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

   If the master server is also the EMM server, the following services must be running:
   - NetBackup Enterprise Media Manager service
   - NetBackup Resource Broker service

   The following services must be running on NetBackup media servers:
   - NetBackup Device Manager service (if the system has configured devices)
   - NetBackup Volume Manager service
   - NetBackup Client service

   The following service must be running on NetBackup clients (including NetBackup Remote Administration Consoles):
   - NetBackup Client service

2. 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 for Windows, 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.

3 If you had to start any of the processes or services in the previous steps, retry the operation.

If they are running or the problem persists, refer to the following procedure:
See “General test and troubleshooting procedures” on page 33.

If you cannot start any of these processes or services, check the appropriate debug logs for NetBackup problems.
See “About using logs and reports” on page 79.

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 and configuration problems**

Use this procedure to resolve installation and common configuration issues.

**Resolving installation problems**

Before you install or use NetBackup on a Linux client, verify that the `inetd` service is started on that machine. This service ensures proper communication between the NetBackup master and the Linux client.

To resolve installation and configuration issues, ask the following questions:

- Can you install the software on the master and the media servers by using the release media?

Some reasons for failure can be 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 customer support)
- Defective drive (replace the drive or refer to vendor’s hardware documentation)
Improperly configured drive (refer to the system and the vendor documentation)

Can you install NetBackup client software on the clients?

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 and the correct server name is in the client /.rhosts file.

   If the install hangs, check for problems with the shell or the environment variables for the root user on the client. The files to 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 install to a secure UNIX client, check your ftp configuration. For example, you must use a user name and password that the client considers valid.

■ Is the problem related to general network communications?

   See “Resolving network communication problems” on page 40.

Resolving common configuration problems

If this installation is an initial installation or if you changed the configuration, check for these problems before proceeding:

To resolve configuration issues, check for these problems

1 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." This feature is configurable on some platforms. NetBackup requires it. See the *NetBackup Device Configuration Guide* for more information.

- On UNIX, tape devices (other than QIC) are not configured as "variable mode." This feature is configurable on some platforms. NetBackup requires it. When this condition exists, you can frequently perform backups but not restores. Further explanation is available. See “NetBackup status code: 174” on page 255. Also see the *NetBackup Device Configuration Guide*.

- On UNIX, pass-through paths to the tape drives have not been established. Also see the *NetBackup Device Configuration Guide*.

2 Check for the following problems with the daemons or services:

- Daemons or services do not start during reboot (configure system so they start).

- Wrong daemons or services are started (problems with media server start up 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.

3 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 Backup Status 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 “About NetBackup status codes and messages” on page 153. See “About media and device management status codes and messages” on page 421.

- Check the system log on UNIX or the Event Viewer Application and System log on Windows if the problem pertains to media or device management. One of the following is true:
  - NetBackup does not provide a status code
  - You cannot correct the problem by following the instructions in the status codes chapters

- 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 using logs and reports” on page 79.

4 If you performed corrective actions, retry the operation. If you did not perform corrective actions or the problem persists, go to the next section.

- See “General test and troubleshooting procedures” on page 33.

**Resolving device configuration problems**

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
- 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:

**Message:** Drive does not support serialization

**Explanation:** 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.

**Recommended action:** 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.

**Message:** Robot does not support serialization
**Explanation:** 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.

**Recommended action:** 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.

**Message:** No license for this robot type

**Explanation:** NetBackup server does not support the robotic type that is defined for this robot.

**Recommended action:** Define a different robot. Only use the robotic libraries that NetBackup server supports.

**Message:** No license for this drive type

**Explanation:** The drive type that is defined for this drive that the NetBackup server does not support.

**Recommended action:** Define a different drive. Only use the drives that NetBackup supports.

**Message:** Unable to determine robot type

**Explanation:** NetBackup does not recognize the robotic library. The robotic library cannot be auto-configured.

**Recommended action:**
- Download a new device_mapping file from the Symantec support web site, and try again.
- Configure the robotic library manually.
- Use only the robotic libraries that NetBackup supports.

**Message:** Drive is stand-alone or in unknown robot

**Explanation:** Either the drive is stand-alone, 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.

**Recommended action:** 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.

**Message:** Robot drive number is unknown
Explanation: 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.

Recommended action: 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.

Message: Drive is in an unlicensed robot

Explanation: 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.

Recommended action: Configure a drive that does not reside in the unlicensed robot.

Message: Drive's SCSI adapter does not support pass-thru (or pass-thru path does not exist)

Explanation: A drive was found that does not have a SCSI pass-through path configured. Two possible causes for this message are as follows:

- 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.

Recommended action: Change the drive’s adapter or define a pass-through path for the drive. SCSI adapter pass-through information is available.

See the NetBackup Device Configuration Guide.

Message: No configuration device file exists

Explanation: A device has been detected without the corresponding device file necessary to configure that device.

Recommended action: Refer to the chapter for your system type in the NetBackup Device Configuration Guide for information on how to create device files.

Message: Unable to determine drive type

Explanation: The NetBackup server does not recognize the drive. The drive cannot be auto-configured.

Recommended action:

- Download a new device_mapping file from the Symantec support web site, and try again.
- Configure the drive manually.
- Use only the drives that NetBackup supports.
Message: Unable to determine compression device file

Explanation: A drive was detected without the expected compression device file 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.

Recommended action: 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. Refer to the chapter for your system type in the *NetBackup Device Configuration Guide*.

General test and troubleshooting procedures

If the Preliminary troubleshooting or Troubleshooting installation and configuration problems procedures do not reveal the problem, perform the following procedures. Skip those steps that you have already performed.

The procedures assume that the software was successfully installed, but not necessarily configured correctly. If NetBackup never worked properly, you probably have configuration problems.

Repeat the checks that are mentioned in the Troubleshooting installation and configuration problems procedure when you encounter errors.

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 631.

Testing the master server and clients

This procedure tests the master server and clients.
To test the master server and clients

1 Enable appropriate debug logs on the master server.

   See “About using logs and reports” on page 79.

   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.

2 Configure a test policy (set 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 \( \texttt{bplabel} \) command, NetBackup automatically assigns a previously
   unused media ID.

3 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, execute:
     \[
     /usr/openv/netbackup/bin/bpps -a
     \]

   - To check the services on a Windows system, use the NetBackup Activity
     Monitor or the Services application in the Windows Control Panel.

4 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.

   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 631.

   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

   - \( \texttt{vmd} \) debug logs on the EMM database host for the device
bptm debug logs

See the vendor manuals for information on hardware failures.

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, you 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.

5 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.

Start with step 3 to repeat this procedure for the robot. This procedure verifies that NetBackup can find the volume, mount it, and use the robotic drive.

If you have difficulties with the robot, try the test utilities.

See “About robotic test utilities” on page 707.

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.

6 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.

7 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.
Explanations about which logs apply to specific client software are available. See “About using logs and reports” on page 79.

These logs exist only if you enabled debug logging in step 1. 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:

- barchive (UNIX only)
- bpbackup (UNIX only)
- bpbkar
- bpcd
- bplist
- bprd
- bprestore
- nbwin (Windows only)
- bpinetd (Windows only)

8 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.

9 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 using logs and reports” on page 79.

10 Perform a user backup and then a restore from the client that is specified in step 8.

These actions verify the following:
Communications between the client and the master server
- NetBackup software on the client

If an error occurs, check the following:
- All Log Entries report
- 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.

11 When the test policy operates satisfactorily, repeat specific steps as necessary to verify other clients and storage units.

12 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 suggested actions in the status codes chapters.

Testing media server and clients

If you use media servers, verify their operation as explained in the following steps.

Before proceeding, eliminate all problems on the master server.

See “Testing the master server and clients” on page 33.

To test the media server and clients

1 Enable appropriate legacy debug logs on the servers
   See “About using logs and reports” on page 79.
   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.

2 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.
3 Verify the following: all NetBackup daemons or services are running on the master server and Media and Device Management daemons or services are running on the media server.

Do one of the following:

- To perform this check on a UNIX system, run:

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

- To perform this check on a Windows system, use the Services application in the Windows Control Panel.

4 Perform a user backup and then a restore of a file. Perform these operations 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 `nb pem`, `nb jm`, `nrb b`, EMM server process `nbemm`, and media server processes `bpc d` and `bp b rm`
- Communications between media server process `bp b rm` and client processes `bpc d` and `bpbkar`

For the failures that relate to drives or media, ensure that the drive is in an UP state and the hardware functions.

If you suspect a communications problem between the master and the media servers, check the debug logs for the involved 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
- \texttt{vmd} debug logs

See the vendor manuals for information on hardware failures.

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 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.

5 If you previously configured a nonrobotic 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.

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 robotic test utilities” on page 707.

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.

6 When the test policy operates satisfactorily, repeat specific steps as necessary to verify other clients and storage units.

7 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 in the status codes chapters.
Resolving network communication problems

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.

UNIX clients

For UNIX clients, perform the following steps. Before you start this procedure, add the VERBOSE option to the /usr/openv/netbackup/bp.conf file. Also, create a bpcd debug log directory on your server and clients and a bprd log directory on the server. During subsequent retries, the debug logs provide detailed debug information, which can help you analyze the problem.

To resolve network communication problems with UNIX clients

1. If this configuration is a new or a modified configuration, check the following:
   - Check any recent modifications to ensure that they did not introduce the problem.
   - Ensure that the client software was installed.
   - Ensure that the client operating system is one of those supported by the client software.
   - 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” on page 48.

Two other checks that you can make on host names are as follows:

- 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 (verbose) on the server to determine what occurred when the server received the request.
Pay special attention to NIS or the DNS updates that are required. Failure to update these services properly is a common source of network problems with NetBackup.

2 Verify network connectivity between client and server by trying to ping the client from the server.

```bash
ping clientname
```

Where `clientname` is the name of the client as configured in the NetBackup policy configuration, `/etc/hosts`, and also in NIS and DNS (if applicable).

For example, to ping a client that is named ant:

```bash
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
```

Also, try ping from the client to the server.

If ping succeeds in both 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.

Note that some forms of the ping command let you ping the bpcd port on the client as in:

```bash
ping ant 13782
```

or

```bash
ping ant bpcd
```

3 Check that the client listens on the correct port for bpcd connections by running one of the following commands (depending on platform and operating system).

```bash
netstat -a | grep bpcd
```

```bash
netstat -a | grep 13782 (or the value that is specified during the install)
```

```bash
rpcinfo -p | grep 13782 (or the value that is specified during the install)
```

For example, assume that the client is a Solaris system and you run:

```bash
netstat -a | grep 13782
```
If there is no problem with the port, the results are similar to:

```
tcp 0 0 *.*.13782 *.* LISTEN
```

The LISTEN indicates that the client listens for connections on this port.

If there is a problem, this line does not appear and one of the following three conditions exists:

- **/etc/services** (or applicable NIS file) does not have the correct `bpcd` entry. The correct `/etc/services` entry is:

  ```
  bpcd 13782/tcp bpcd
  ```

- **/etc/inetd.conf** (or applicable NIS or DNS file) does not have the correct `bpcd` entry. The correct `/etc/inetd.conf` entry is:

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

- **/etc/inetd.conf** was changed but was not re-read. Correct this condition by running one of the following (whichever works):

  ```
  /bin/ps -ef | grep inetd
  kill -HUP the_inetd_pid
  ```

  Or

  ```
  /bin/ps -aux | grep inetd
  kill -HUP the_inetd_pid
  ```

On a Hewlett-Packard platform, use `inetd -c` to send a SIGHUP to `inetd`.

If the problem is with an AIX client, do the following: use SMIT to verify that the InetServ object policy was updated with information about the `bpcd` process (/etc/inetd.conf and /etc/services information).

If you modify the InetServ object policy by using SMIT, the `inetexp` command automatically runs. If you edit the InetServ object policy by using an ODM editor, do the following: run the `inetexp` command to export the InetServ object policy to the `/etc/inetd.conf` and `/etc/services` files. This command keeps these files in sync with the InetServ object policy.

If you change the `/etc/inetd.conf` or `/etc/services` file by using SMIT, the `inetimp` command automatically updates the InetServ object policy. If you change either file, run the following command to inform the `inetd` daemon of the changes to its configuration file: `refresh -s inetd` or `kill -1 InetdPID`
4 telnet to bpcd on the client. If it succeeds, keep the connection until after you perform step 5, then terminate it with Ctrl-c.

telnet clientname 13782

Where clientname is the name of the client as configured in the NetBackup policy configuration, /etc/hosts, and also in NIS and DNS (if applicable).

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.

■ If the telnet succeeds, then inetd on the client is configured correctly. It can pass its connection to bpcd and NetBackup should also be able to establish a connection.

■ If telnet doesn't work, ensure that the inetd.conf file and /etc/services files on both the server and client are correct and match. By default, these are as follows:
In /etc/services:

```
bpcd 13782/tcp    bpcd
```

In /etc/inetd.conf:

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

Then, run kill -HUP to reread the /etc/inetd.conf file as explained in step 3.
Also, update the applicable NIS or DNS files.
If these files are correct and you cannot connect to the client, you may have network routing problems or a problem with the port assignment. (See the next step.)

5 Check that the client listens on the correct port for the telnet connection to bpcd. To check, run one of the following commands (depending on platform and operating system).

```
netstat -a | grep bpcd
netstat -a | grep 13782 (or the value that is specified during install)
rpcinfo -p | grep 13782 (or the value that is specified during install)
```
For example, assume the client in step 4 is a SunOS system that is named ant. The telnet is from a NetBackup server that is named whale:

```
netstat -a | grep 13782
```

One of the following conditions occurs:

- If the port is not the problem, you see the following:

```
tcp 0 0 ant.nul.nul.com.13782 whale...com.1516 ESTABLISHED
tcp 0 0 *.13782 *.* LISTEN
```

In the first line of the result, ESTABLISHED indicates that the telnet connection was established to bpcd through port 13782 on the client. The LISTEN in the second line indicates that the client listens for further connections on this port.

We suggest that you not change the port number for bpcd or other NetBackup services. Do so only if there is no alternative. Then, remember that all NetBackup servers and clients in the configuration must use this new port assignment.

- If there is a process other than bpcd that uses the port, try to reboot the client to clear the problem. If the problem is still not fixed, it may be necessary to change one of the service numbers (preferably for the other service). To change a service number, modify the `/etc/services` files. Then send SIGHUP signals to the `inetd` processes on your clients.

```
/bin/ps -ef | grep inetd
kill -HUP the_inetd_pid
```

Or

```
/bin/ps -aux | grep inetd
kill -HUP the_inetd_pid
```

On a Hewlett-Packard platform, use `inetd -c` to send a SIGHUP to `inetd`. Also make applicable NIS or DNS updates.
If the problem is with an AIX client and you make changes to the 
/etc/inetd.conf and /etc/services information, do the following: Use 
Smit to verify that the InetServ object policy was updated. See step 4.

6 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 “Using bpclntcmd” on page 52.

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

To resolve network 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 on the TroubleShooting tab in the NetBackup Client Properties dialog box. To display this dialog box, start the Backup, Archive, and Restore interface. Then click NetBackup Client Properties on the File menu. See “Using the Host Properties window” on page 60.

2 If this client is new, verify the client and the server names in your NetBackup configuration.

See “Verifying host name and service entries” on page 48.

3 Verify basic 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 basic 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. Not being turned on is a common source of connection problems with PC workstations.

4 On Microsoft Windows or NetWare clients, check the NetBackup Client service. Do one of the following tasks:

■ Ensure that the service is active by checking the logs or by doing one of the following:

■ On Windows XP or Windows Server 2003 clients, use the Services application in the Control Panel to verify that the NetBackup Client service is running. Start it if necessary.

■ On NetWare clients, enter modules bpcd.nlm from the NetWare server console to verify that the NetBackup client daemon is running. If necessary, type bpstart.ncf from the NetWare server console to start the NetBackup client daemon.

■ Check the bpcd debug logs for problems or errors. Instructions are available on how to enable and use these logs. See “About using logs and reports” on page 79.

■ 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:

■ On Microsoft 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.
On NetWare clients, see the BPCD setting in the SYS:VERITAS\NBUCLT\NetBack\BP.INI file.

On 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” on page 60.
Correct the port number if necessary. Then, on Windows clients and servers, stop and restart the NetBackup Client service. On NetWare clients, stop and restart the NetBackup client daemon (bpcd).
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.

Verify that the NetBackup Request Service (bprd) Port number on Microsoft Windows and NetWare clients is the same as on the server (by default, 13720).

On Microsoft Windows clients (use the same method as in step 4).
On NetWare clients, see the BPRD setting in the SYS:VERITAS\NBUCLT\NetBack\BP.INI file.
Or, instead of the first bullet: On UNIX NetBackup servers, the bprd port number is in the /etc/services file. On Windows NetBackup servers, set these numbers in the Client Properties dialog box in the Host Properties window.
See “Using the Host Properties window” on page 60.

Verify that the hosts file or its equivalent contains the NetBackup server name. The hosts files are the following:
%SystemRoot%\system32\drivers\etc\hosts (Windows XP or 2003)
SYS:etc\hosts (NetWare)
/etc/hosts (UNIX)

Verify client-to-server connectability by using ping or its equivalent from the client (step 3 verified the server-to-client connection).
If the client’s TCP/IP transport allows telnet and ftp from the server, try these as additional connectivity checks.
For a NetWare client, ensure that the server does not try to connect when a backup or restore is already in progress on the client. If you try more than one job at a time on these clients, it results in a "can’t connect" or similar error.
10. Use the `bpclntcmd` utility to verify basic 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 “Using `bpclntcmd`” on page 52.

11. Use the `bpptestbpcd` 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 “Using `bpclntcmd`” on page 52.

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

Verifying host name and service entries

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 following:

- See “Background for troubleshooting” on page 701.
- The "Rules for using host names in NetBackup" section in the *NetBackup Administrator's Guide, Volume II*

To verify the client and the server host names in NetBackup

1. Verify that the correct client and server host names are configured in NetBackup.

   - On Windows servers, Windows clients, and NetWare nontarget clients, check the following:
     - The **General** tab in the **NetBackup Client Properties** dialog box.
     - The Server to use for backups and restores drop-down list in the **Specify NetBackup Machines and Policy Type** dialog box.

   To display these dialog boxes, start the Backup, Archive, and Restore interface on the client. For the General tab, click **NetBackup Client Properties** on the **File** menu. For the Server to use for backups and restores drop-down, click **Specify NetBackup Machines and Policy Type** on the **File** menu.

   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.
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.

- 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 gethostbyname() 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” on page 60.

- 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 NetWare clients, check the SYS:VERITAS\NBUCLT\NetBack\BP.INI file to ensure the following:

- 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.
- The ClientName entry and the entries in the [clients] section are correct and match what is in the policy client list on the master server.

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 examples following this procedure show the default port numbers. 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.

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 Administrator’s Guide, Volume I for a list of these processes.

On UNIX, the services file is /etc/services. On Windows, the services file is %SystemRoot%\system32\drivers\etc\services.

On UNIX, Windows, and NetWare clients, verify the NetBackup client daemon or service number, and the request daemon or service port number.

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:
  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 (Windows)

- On NetWare clients, check the BPCD and the BPRD entries in the SYS:VERITAS\NBUCLT\NetBack\BP.INI file.

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

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

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

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

6 NIS, WINS, or DNS host name information must correspond to what is in the policy configuration and the name entries in the following:

- On Windows NetBackup servers, Microsoft Windows clients, and NetWare nontarget clients:
  - 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:
    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.
  - The \veritas\nbuclt\netback\bp.ini file on NetWare clients.
Also, verify that reverse DNS addressing is configured.

To confirm the setup of the following, use the NetBackup `bpclntcmd` utility: the IP addresses and hostnames in DNS, NIS, and (or) local hosts files on each NetBackup node.

**Using `bpclntcmd`**

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 software. The following directory contains the command that starts the utility:

```
install_path\NetBackup\bin (Windows)
```

```
/usr/openv/netbackup/bin (UNIX)
```

On Windows, run this 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:

- **`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.

- **`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.

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 the following: 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.)

**bpclntcmd -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.

The following is an example of the use of `bpclntcmd`:

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

The following is true of the preceding command:

- `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.

**bpclntcmd -sv**

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

Host name and service entry examples - UNIX

This topic shows five examples of host name and service entries for UNIX systems.

**Example 1: UNIX master server and client**

The example in Figure 2-1 shows a UNIX master server with one UNIX client.
Example 1: UNIX master server and client

UNIX Master Server

Policy Client List
jupiter
mars

/usr/openv/netbackup/bp.conf
SERVER=jupiter
CLIENT_NAME=jupiter

/etc/inetd.conf
bcd ... (see note 1)

/etc/services
# NetBackup services
bcd 13782/tcp bpcd
bprd 13720/tcp bprd
bpdbm 13721/tcp bpdbm
# Volume Manager services #
vmd 13701/tcp vmd
tl8cd 13705/tcp tl8cd

Notes:
1. The complete inetd.conf entry is:
   bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd
2. 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 2: UNIX master server and media server

Figure 2-2 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.
Example 2: UNIX master and media servers

Figure 2-2

UNIX Master Server

Policy Client List
jupiter
mars
saturn

Ethernet

UNIX Media Server

jupiter

mars

UNIX Client

saturn

Notes:

1. The complete inetd.conf entry is:
bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd

2. 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 3: UNIX PC clients

Figure 2-3 shows a NetBackup master server with PC clients, defined here as Windows, NetWare, or Macintosh clients. Server configuration is the same as it is for UNIX clients. These clients do not have inetd.conf entries.
Example 3: UNIX PC clients

**Figure 2-3**

UNIX Master Server

- jupiter

Policy Client List
- jupiter
- mars
- saturn
- pluto

```
/usr/openv/netbackup/bp.conf
SERVER=jupiter
CLIENT_NAME=jupiter
```

```
/etc/inetd.conf
bp... (see note 1)
```

```
/etc/services
# NetBackup services
bp... tcp tcp
bpcd=13782/tcp bpcd
bprd=13720/tcp bprd
bpdbm=13721/tcp bpdbm
# Volume Manager services
vmd=13701/tcp vmd
tl8cd=13705/tcp tl8cd
odld=13706/tcp odld
```

NetBackup Client Properties dialog box

- Server List: jupiter
- General
- Client Name: saturn
- Network
- NetBackup Client Service Port 13782
- NetBackup Request Service Port 13720

Notes:
1. The complete inetd.conf entry is:
   bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd
2. 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 4: UNIX clients in multiple networks

**Figure 2-4** 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.
In example 4, we first examine the configuration of the router system. The NetBackup policy client list shows this 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 to note. 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.

Refer to the *NetBackup Administrator’s Guide, Volume I*, for more information on `altnames` configuration.

Regardless of the type of router, the configuration for the media server, saturn, is the same as in example 2. 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 5: UNIX server that connects to multiple networks**

*Figure 2-5* 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.
Example 5: UNIX server connects to multiple networks

**Figure 2-5** Example 5: UNIX server connects to multiple networks

- Policy Client List
  - jupiter
  - mars
  - saturn
  - pluto

- `/etc/inetd.conf`
  - `bpcd` ...
  - `bpcd` (see note 1)

- `/etc/services`
  - `# NetBackup services` `bpcd` `13782/tcp` `bpcd`
  - `bprd` `13720/tcp` `bprd`
  - `bpdbm` `13721/tcp` `bpdbm`
  - `# Volume Manager services` `vmd` `13701/tcp` `vmd`
  - `tl8cd` `13705/tcp` `tl8cd`
  - `odld` `13706/tcp` `odld`

Notes:

1. The complete `inetd.conf` entry is:
   
   `bpcd` stream tcp nowait root `/usr/openv/netbackup/bin/bpcd` `bpcd`

2. 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 5 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.

Another important item to note is the configuration of the NetBackup server list. 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.

As in example 4, there would be a problem 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 also identical to the solution that is discussed in the following:

See Figure 2-4 on page 57.

Using the Host Properties window

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.

Many procedures in this guide also refer to the NetBackup Client Properties dialog box in the Backup, Archive, and Restore interface on Microsoft Windows clients. This dialog box 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.

For more information, see the online Help or the NetBackup Administrator’s Guide, Volume I.

To access configuration settings through Host Properties

1. Start the NetBackup Administration Console.
2. Click Host Properties.
3. Select the servers or clients where you want to make the change.
5. In the properties dialog box, select the appropriate tab 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 diagnose and correct a full disk problem

1. The NetBackup Resource Broker (nrb) 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 nrb 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: -1
   Sqlstate: HY000

   The nrb log (originator ID 118) is written in /usr/openv/logs (UNIX) or install_path\NetBackup\logs (Windows). More information is available about unified logging.

   See “About using logs and reports” on page 79.

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 using logs and reports” on page 79.

Consider moving the NetBackup unified logging files to a different file system. See “Changing log file locations” on page 84.

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.

Troubleshooting frozen media

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:

■ 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 involved when media is frozen.

The following logs are useful when troubleshooting frozen media:

UNIX and Linux:

- 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

The verbosity of the bptm process log should be set 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 bptm verbosity for bptm on individual media servers by changing their logging levels under Host Properties on the NetBackup Administration Console.

The following conditions can cause media to freeze:

- The same media has excessive errors during backup. 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 media. One of the first symptoms of a dirty drive is frozen media. Clean the drive according to the manufacturer’s suggestions.

- The drive itself. Check for tape device errors reported by the operating system logs or by the device driver. 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 reported by the operating system logs or by their driver. If any are found, follow the hardware manufacturer’s recommendations for this type of error.
Ensure that the tape drives appear on the hardware compatibility list as supported for NetBackup. This list is located on the following &CompanyName; support web site:

http://www.symantec.com/business/support/overview.jsp?pid=15143

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.

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

The following circumstances 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. The error can also occur if 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 are configured with the wrong tape paths. Drive configuration that use the correct robot drive number is important to the proper mounting and utilization of media. The robot drive number is normally set based on the relationship of the drive serial number with the drive serial number information from the robotic library. This number must be determined and validated before you consider the device configuration complete.

- The media contain a non-NetBackup format.

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 tapes have usually been written outside of NetBackup, and have found their way into the library. By default, NetBackup will only write to a blank media or other NetBackup media. Other media types (DBR, TAR, CPIO, ANSI, MTF1 and recycled Backup Exec BE-MTF1 media) will be frozen as a safety measure. Change this behavior by using the following procedure:

On UNIX and Linux:
To allow NetBackup to overwrite foreign media, add the following to the bp.conf file 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 overwrite protection, select one or more of the listed media formats.
Stop and restart the NetBackup services for the changes to take effect.
Do not select a foreign media type for overwriting unless it is certain that this media type should be overwritten.
For more details on what each media type is, see the NetBackup System Administrator's Guide.

- The media is a tape formerly used for the NetBackup catalog backup.

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

This 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

<table>
<thead>
<tr>
<th>ID</th>
<th>rl</th>
<th>images</th>
<th>allocated</th>
<th>last updated</th>
<th>density</th>
<th>kbytes restores</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>04/22/2005 10:12</td>
<td></td>
<td></td>
<td>---------</td>
</tr>
<tr>
<td>DIV08</td>
<td>1</td>
<td>1</td>
<td>04/22/2005</td>
<td>10:12</td>
<td>hcart</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>05/06/2005 10:12</td>
<td></td>
<td></td>
<td>FROZEN</td>
</tr>
</tbody>
</table>
```

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.

In troubleshooting PBX, consider the issues that are described in this section.

**Note:** If PBX is not installed or is configured incorrectly, NetBackup is unresponsive.

Checking for PBX installation

NetBackup requires the &CompanyName; 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 re-install it.

To see if PBX is installed

1. Look for the following directory on the NetBackup master server:
   - On UNIX: /opt/VRTSpbx
   - On Windows: install_path\VxPBX

2. 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:
   
   ```bash
   ps | grep pbx_exchange
   ```

2. To start PBX on UNIX, type the following:

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

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

PBX must be set correctly

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

To verify the PBX settings

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

   - On UNIX, type the following:

     ```bash
     /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:

     ```bash
     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.

PBX logging

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 “Unified logging” on page 83.

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:

05/11/05 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

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 “Configuring and using unified logging” on page 93.
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. 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). 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.

**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
```


To correct a PBX security problem

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`

**Required NetBackup daemon or service not 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 nature of the 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.)

```
05/17/05 10:00:47.179 [Info] PBX_Manager:: handle_input with fd = 4
05/17/05 10:00:47.179 [Info] PBX_Client_Proxy::parse_line, line = ack=1
```
To correct not having a daemon or service 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
     ```

New network interface cards

If the network interface card (NIC) in a NetBackup master or media server is changed, or if the server’s IP address changes, CORBA communications may be interrupted in a variety of ways. To address this situation, stop and restart NetBackup.

Backup performance and NIC cards

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.

For help on how to view and reset duplex mode for a particular host or device, consult the manufacturer’s documentation.
To view and reset duplex mode for a host or device (if the manufacturer's documentation does not help)

1. Log in to the host that contains the network interface card(s).
2. Enter the following command to view the current duplex setting.
   
   ```
   ifconfig -a
   ```

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

   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
   ```

   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.

**SERVER entries in 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 machine, 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.

Resolving unavailable storage units 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 ...

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, the following can occur: some of the machines or devices that
NetBackup needs may not be available. 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 (or the earlier SANPoint Control) 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 SharedDisk, refer to the "SharedDisk troubleshooting checklist" in the NetBackup Shared Storage Guide.

For information on how to implement persistent bindings, refer to 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**

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 determining root cause problems quickly. In addition, because NetBackup administrators and SAN administrators
are often in different groups, the fragmented operations that lead to resolution delays may be avoided. 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.

In addition, having an environment inventory to provide to support for troubleshooting is valuable to the support process.

**General troubleshooting tools**

Some ways to investigate a backup failure are as follows:

- Launch CommandCentral Storage in context from NetBackup to check fabric health.
- Check reports for fabric events occurring around the time NetBackup generated the error log.

**Common NetBackup troubleshooting use cases**

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 revolve around connectivity issues.

**Use Case 1: NetBackup cannot access drives or robots**

Typically found as an error 213 (no storage units available for use) in NetBackup, this problem represents a loss of connectivity. This issue is a problem because NetBackup freezes tapes with two write failures, even when SAN problems cause the failures.

**Symptom:** Backup jobs fail

**To troubleshoot the inability to access drives or robots**

1. Check the NetBackup device monitor to see whether a device is down. If a device is down, try to bring it back up.

2. If the drive is still down, check the following for status 219 (the required storage unit is unavailable) and 213 (no storage units available for use) on the media server:
3 Check the NetBackup logs for status 83, 84, 85, and 86. These codes relate to write, read, open, position failures to access the drive.

4 Try a `robtest` to determine connectivity.
   If there is no connectivity, the likely problem is with hardware.

5 From the master server, select the robot or device the storage unit is associated with.

6 Launch CommandCentral Storage for a view of the media server and devices.

7 Check the fabric connectivity (whether any I/O path devices are down).

**Use Case 2: NetBackup device discovery cannot see a robot or drive**

The NetBackup administrator installs a new device and runs the Device Configuration Wizard to discover and configure it. The wizard does not see the newly installed device.

CommandCentral Storage topology is a good visual tool for checking connectivity between the hosts and the devices. You can use it to see if a network cable was dislodged or if some other problem exists.

This use case may be encountered when you configure off-host backups. Off-host backups require the media server to be able to see all devices with which it conducts the backup: disk array, disk cache, data mover, library, and drive. Connectivity must be correct. In addition, the `bptpcinfo` command in NetBackup Snapshot Client generates a 3pc.conf configuration file for running the backup. Often the WWN (world wide name) for some devices is incorrect. You can use CommandCentral Storage to verify that the contents of the 3pc.conf file correlate to the actual fabric configuration.

For a description of off-host backup, the `bptpcinfo` command, and the 3pc.conf file, refer to the *NetBackup Snapshot Client Configuration* document.

For help accessing this document, see "Snapshot Client Assistance" in the *NetBackup Snapshot Client Administrator’s Guide*.

Symptom: After you run the Device Configuration Wizard, the new device does not appear in the discovered devices list.
To troubleshoot the inability to see (discover) a robot or drive

1. Run device discovery again.
2. If the new device is still not seen, the likely problem is with hardware. Launch CommandCentral Storage.
3. If the new device does not appear in the CommandCentral Storage topology, check SAN hardware connections to determine whether or not 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 Robotic status code: 214, robot number does not exist.

   See “Robotic status code: 214” on page 532.
4. Rerun the Device Configuration Wizard.

Use Case 3: Intermittent drive failure

A drive fails and causes a backup to fail, but on examination the drive looks fine. Sometimes a problem with a switch or bridge either before or during the backup job causes the job to fail and takes down the drive. This problem is one of the most difficult to diagnose. By the time the NetBackup administrator looks at the SAN everything may be fine again. To use CommandCentral Storage to troubleshoot this issue, do the following: check for alerts around the time of the job failure and see if a SAN problem occurred that would have caused the job to fail.

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.

Symptom: The backup job fails intermittently and the drive is down intermittently. No errors appear in the error log other than that the job failed.

To troubleshoot an intermittent drive failure problem

1. Select a drive inside the NetBackup Device Monitor. Launch CommandCentral Storage in the drive context to see whether the drive is connected to the SAN.
2. Check CommandCentral Storage alert reports to see whether a SAN problem existed that would have affected the drive during the time the backup job failed.
Using logs and reports

This chapter includes the following topics:

- About using logs and reports
- Where is the log and report information?
- Reports
- Status for user operations
- UNIX system logs
- Debug logs on servers
- Debug logs on UNIX clients
- Debug logs on PC clients
- Windows Event Viewer logging option
- Troubleshooting the Administration Console for UNIX
- Query string overview

About using logs and reports

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

Note: The log-entry format in the NetBackup logs is subject to change without notice.
Note: The term "media server", as distinct from "master server" or "server", does not apply to the NetBackup server product. When you troubleshoot a NetBackup server installation, ignore any references to media server. (This note does not apply to NetBackup Enterprise Server.)

Where is the log and report information?

Users need to know where log and report information is on their systems. Figure 3-1 shows the location of the log and report information on the client and the server and the processes that make the information available.
More information is available on the programs and daemons that are mentioned in this figure.

See “About backup and restore functional overview” on page 631.

Reports

NetBackup provides the standard reports that show most of the status information and error information. To run these reports, use the NetBackup Administration Console.
See the *NetBackup Administrator’s Guide, Volume I*, for instructions and detailed descriptions about these reports.

Table 3-1 provides a summary of the reports.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status of Backups</td>
<td>Displays status information and error information on the jobs that complete within the specified time period. If an error has occurred, a short explanation of the error is included. On UNIX systems, environment variables allow modification of character lengths of some fields.</td>
</tr>
<tr>
<td>Client Backups</td>
<td>Displays the detailed information on the jobs that complete within the specified time period.</td>
</tr>
<tr>
<td>Problems</td>
<td>Lists the problems that the server has logged during the specified time period. This information is a subset of the information in the All Log Entries report.</td>
</tr>
<tr>
<td>All Log Entries</td>
<td>Lists all log entries for the specified time period. This report includes the information from the Problems report and Media Logs report.</td>
</tr>
<tr>
<td>Images on Media</td>
<td>Lists the contents of the media as recorded in the NetBackup image catalog. You can generate this report for any type of media (including disk) and filter it according to client, media ID, or path.</td>
</tr>
<tr>
<td>Media Logs</td>
<td>Displays the media errors or the informational messages that are recorded in the NetBackup error catalog.</td>
</tr>
<tr>
<td>Tape Reports</td>
<td>Displays the information about the images that are stored on tape media (such as tape logs, tape contents, and tape summary).</td>
</tr>
<tr>
<td>Disk Reports</td>
<td>Displays the information about the images that are stored on disk media (such as disk logs, and disk storage unit and disk pool status).</td>
</tr>
<tr>
<td>Audit Reports</td>
<td>Displays a record of user-initiated actions in a NetBackup environment. Auditing lets you track changes to NetBackup policies, host properties, and storage units. It can also track changes to NetBackup runtime objects such as labeling or expiring media, initiating a restore job, and canceling or suspending a job. More information is available on audit reports. Refer to the Auditing NetBackup Administration chapter of the <em>NetBackup Administrator’s Guide, Vol. I</em>.</td>
</tr>
</tbody>
</table>
Status for user operations

NetBackup lets you view status on the progress of user operations.

See the NetBackup Backup, Archive, and Restore Getting Started Guide for information on the Task Progress tab.

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.

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

See “Enabling system logs” on page 106.

Debug logs on servers

If a problem requires more information than is available through the normal logs and reports, consult the debug logs. They show detailed information about specific processes.

The following sections describe the two forms of debug logging: unified logging and legacy logging.

Unified logging

Unified logging creates log file names and messages in a standardized format. Certain NetBackup processes use unified logging.

A list of the processes that use unified logging is available.

See Table 3-2 on page 86.

Log locations

All unified logs are written to the /usr/openv/logs directory (UNIX) and the install_path\NetBackup\logs folder (Windows). Unlike legacy logging, you do not need to create logging subdirectories. Log files for originator IDs are written to a subdirectory with the name specified in the log configuration file.
Changing log file locations

The unified logging files can consume a lot of disk space. You can direct them to a different location, if needed.

To direct unified logs to a different file system, enter the following:

- **On 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`.

- **On 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`.

Message types

The following three kinds of messages can appear in unified logging files:

- **Application log messages** include informational, warning, and error messages. Application messages are always logged and cannot be disabled. These messages are localized.
  
  An example of an application message follows:

  05/02/09 11:02:01.717 [Warning] V-116-18 failed to connect to nbjm, will retry

- **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.
  
  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** are intended primarily for &CompanyName; engineering. Like diagnostic messages, they can be issued at various levels of detail. These messages are not localized.

**Note:** Like diagnostic messages, 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]

Unified logging file name format

Unified logging uses a standardized naming format for log files, as follows:

```
productID-originatorID-hostID-date-rotation.log
```

The following shows the meaning of each of the variables in the log file name:

- `product ID`: Identifies the product. The NetBackup product ID is 51216.
- `originatorID`: Identifies the log writing entity, such as a process, service, script, or other software.
- `hostID`: Identifies the host that created the log file. Unless the file was moved, this ID is the host where the log resides.
- `date`: Shows when the log was written, in YYMMDD format.
- `rotation`: A numbered instance of a log file for a given originator. This numbering is used for log file rotation.

See “Unified logging file rollover” on page 92.

Example log file name:

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

Where:

- 51216: The product ID (entity ID) for NetBackup.
- 116: The originator ID of the `nbpcm` process (the NetBackup policy execution manager).
- 2201360136: The host ID for the host that created this log.
- 041029: The date in YYMMDD format.
The rollover number that indicates the instance of this log file. By default, log files roll over 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 “Unified logging file rollover” on page 92.

Server processes that use unified logging

The unified logging originator ID lists the processes. More than one process may use an originator ID.

See the UNIX and Windows client sections later in this chapter for the client processes that use unified logging.

All logs with the following IDs are written to the /usr/openv/logs subdirectory on UNIX or to the install_path\NetBackup\logs subdirectory on Windows (except as noted in this table).

Table 3-2 lists the NetBackup server processes that use unified logging.

Table 3-2 Unified logging: originator IDs and NetBackup processes

<table>
<thead>
<tr>
<th>Originator ID</th>
<th>Processes that use the originator ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>103</td>
<td>Private Branch Exchange service (PBX). Writes logs to /opt/VRTSpbx/log (UNIX) and install_path\VxPBX\log (Windows).</td>
</tr>
<tr>
<td>111</td>
<td>nbemm: Enterprise Media Manager (EMM). This process runs only on the EMM server.</td>
</tr>
<tr>
<td>116</td>
<td>nbpem: NetBackup Policy Execution Manager. This process runs only on the master server.</td>
</tr>
<tr>
<td>117</td>
<td>nbjm: NetBackup Job Manager. This process runs only on the master server.</td>
</tr>
<tr>
<td>118</td>
<td>nbrb: NetBackup Resource Broker. This process runs only on the EMM server.</td>
</tr>
<tr>
<td>119</td>
<td>bmr and bmrbd: Bare Metal Restore (BMR) master (or boot) server daemons. bmrbd runs on the BMR boot server.</td>
</tr>
<tr>
<td>121</td>
<td>bmrsavecfg: Bare Metal Restore data collection utility. bmrsavecfg runs on the NetBackup client, not server.</td>
</tr>
<tr>
<td>Originator ID</td>
<td>Processes that use the originator ID</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>122 bmrc</td>
<td>The Bare Metal Restore utility that UNIX clients use to communicate to the BMR master server during a restore. bmrc originates on the BMR boot server and runs on the restoring client.</td>
</tr>
<tr>
<td>123 bmrs</td>
<td>the Bare Metal Restore commands and database interface.</td>
</tr>
<tr>
<td>124 bmrcreatefloppy.exe</td>
<td>(Windows only) used by the Bare Metal Restore commands that create floppy disks. bmrcreatefloppy.exe runs on the BMR boot server.</td>
</tr>
<tr>
<td>125 bmrseradm</td>
<td>The Bare Metal Restore utility that creates a shared resource tree and bootable CDs, and runs on the BMR boot server.</td>
</tr>
<tr>
<td>126 bmrprep</td>
<td>The Bare Metal Restore utility that prepares BMR servers for a client restoration.</td>
</tr>
<tr>
<td>127 bmrsetupmaster and bmrsetupboot</td>
<td>Bare Metal Restore installation, configuration, and upgrade processes.</td>
</tr>
<tr>
<td>128</td>
<td>Bare Metal Restore libraries get their log messages from this catalog.</td>
</tr>
<tr>
<td>129 bmrconfig</td>
<td>The Bare Metal Restore utility that modifies a client's configuration.</td>
</tr>
<tr>
<td>130 bmrpkg and bmrcreatepkg</td>
<td>Bare Metal Restore utilities to add the following: Windows drivers, service packs, and hotfixes to the BMR master server so they can be used in a restore.</td>
</tr>
<tr>
<td>131 bmrrst.exe and bmrmap.exe</td>
<td>(Windows systems only). Utilities that restore Windows Bare Metal Restore clients. They run on the restoring client.</td>
</tr>
<tr>
<td>132 nbsl</td>
<td>NetBackup Service Layer.</td>
</tr>
<tr>
<td>134 ndmpagent</td>
<td>NDMP Agent daemon that manages NDMP backup and restore.</td>
</tr>
<tr>
<td>137</td>
<td>Controls the logging level in the NetBackup libraries. The application and diagnostic messages are for customer use; debug messages are intended for &amp;Company; engineering.</td>
</tr>
<tr>
<td>140</td>
<td>Media server user interface for the Enterprise Media Manager (EMM).</td>
</tr>
<tr>
<td>142 bmrepadm</td>
<td>a utility that manages the Bare Metal Restore external procedures that are used during a restore.</td>
</tr>
</tbody>
</table>
Table 3-2 Unified logging: originator IDs and NetBackup processes (continued)

<table>
<thead>
<tr>
<th>Originator ID</th>
<th>Processes that use the originator ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>143</td>
<td>mds: the media selection component and device selection component of Enterprise Media Manager (EMM).</td>
</tr>
<tr>
<td>144</td>
<td>Device Allocator, for shared drives.</td>
</tr>
<tr>
<td>146</td>
<td>The &amp;CompanyName; OpsCenter reporting service, part of &amp;CompanyName; OpsCenter.</td>
</tr>
<tr>
<td>147</td>
<td>The &amp;CompanyName; OpsCenter Client, part of &amp;CompanyName; OpsCenter.</td>
</tr>
<tr>
<td>148</td>
<td>The &amp;CompanyName; OpsCenter Server, part of &amp;CompanyName; OpsCenter.</td>
</tr>
<tr>
<td>151</td>
<td>NDMP protocol messages, avrd, and robotic processes.</td>
</tr>
<tr>
<td>154</td>
<td>bmrovradm: a utility that manages custom override functions for Bare Metal Restore.</td>
</tr>
<tr>
<td>156</td>
<td>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 &amp;CompanyName; engineering. <strong>Note:</strong> If you are instructed to increase the logging level by &amp;CompanyName; support, you must increase the debug level for OID 137 to 4 or higher. <strong>Warning:</strong> A debug logging level greater than 0 generates large amounts of data.</td>
</tr>
<tr>
<td>158</td>
<td>Remote access interface for NetBackup clients.</td>
</tr>
<tr>
<td>159</td>
<td>Transmater for NetBackup clients.</td>
</tr>
<tr>
<td>163</td>
<td>NetBackup Service Monitor (svcmon), which monitors the NetBackup services and attempts to restart a service that unexpectedly terminates.</td>
</tr>
<tr>
<td>166</td>
<td>NetBackup Vault.</td>
</tr>
<tr>
<td>178</td>
<td>Disk Service Manager (DSM), which performs set and get operations on disk storage and disk storage units.</td>
</tr>
<tr>
<td>199</td>
<td>nbftsrvr: the FT Server process, part of SAN Client.</td>
</tr>
<tr>
<td>200</td>
<td>nbftclnt: the FT Client process, part of SAN Client.</td>
</tr>
</tbody>
</table>
Table 3-2 Unified logging: originator IDs and NetBackup processes (continued)

<table>
<thead>
<tr>
<th>Originator ID</th>
<th>Processes that use the originator ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>FT Service Manager (FSM) component of the Enterprise Media Manager (EMM), for SAN Client.</td>
</tr>
<tr>
<td>210</td>
<td>Exchange Firedrill Wizard for NetBackup clients.</td>
</tr>
<tr>
<td>219</td>
<td>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.</td>
</tr>
<tr>
<td>220</td>
<td>Disk polling service for NetBackup clients.</td>
</tr>
<tr>
<td>221</td>
<td>The Media Performance Monitor Service (MPMS). This service runs on every media server within RMMS and gathers CPU load and free memory information for the host.</td>
</tr>
<tr>
<td>222</td>
<td>Remote monitoring and Management Service (RMMS), which is the conduit through which EMM discovers and configures disk storage on media servers.</td>
</tr>
<tr>
<td>226</td>
<td>The storage lifecycle manager (libssmgr), which controls lifecycle image duplication operations.</td>
</tr>
<tr>
<td>230</td>
<td>The Remote Disk Service Manager interface (RDSM) that runs within the Remote Manager and Monitor Service. RMMS runs on media servers.</td>
</tr>
<tr>
<td>231</td>
<td>Event Manager Service (nbevtmgr). nbevtmgr provides asynchronous event Management Services for cooperating participants.</td>
</tr>
<tr>
<td>248</td>
<td>BMR launcher (bmrlauncher). A utility in the Windows BMR Fast Restore image that configures the BMR environment.</td>
</tr>
<tr>
<td>261</td>
<td>Artifact generator generated source.</td>
</tr>
<tr>
<td>263</td>
<td>NetBackup Administration Console for Windows (nbconsole).</td>
</tr>
<tr>
<td>271</td>
<td>Legacy error codes.</td>
</tr>
<tr>
<td>272</td>
<td>The Expiration Manager (libexpmgr), which handles capacity management and image expiration for storage lifecycle operations.</td>
</tr>
<tr>
<td>286</td>
<td>Encryption Key Management service</td>
</tr>
<tr>
<td>293</td>
<td>NetBackup Audit service</td>
</tr>
</tbody>
</table>
Table 3-2  Unified logging: originator IDs and NetBackup processes (continued)

<table>
<thead>
<tr>
<th>Originator ID</th>
<th>Processes that use the originator ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>294</td>
<td>NetBackup Audit messages</td>
</tr>
<tr>
<td>360</td>
<td>NetBackup Client Oracle utility</td>
</tr>
<tr>
<td>363</td>
<td>nbars: Database Agent Request server process call</td>
</tr>
</tbody>
</table>

How to set logging levels

Unified logging is enabled by default to log debug messages at a low volume and diagnostic and application messages at the highest volume (finest detail).

To change the logging level

1. In the NetBackup Administration Console, expand **NetBackup Management > Host Properties**.
2. Select **Master Servers**, **Media Servers**, or **Clients**.
3. In the **Details** pane, click the server or client to view the version and platform. Then, double-click to view the properties.
4. In the left pane, click **Logging**.
5. Note the **Global logging level** setting.
   
   If you make changes with **Global logging level**, it affects the logging level that both unified logging and legacy logging use.

The following, however, are not affected:

- PBX logging
- Media and device management logging (**vmd, ltid, avrd, robotic daemons, media manager commands**)
- Any unified logging processes whose debug level has been changed from the default setting

Set logging levels for PBX.

See “**PBX logging**” on page 68.

For logging information on media manager, see the following:

See “**Media and device management legacy debug logs**” on page 105.

To set verbosity levels for legacy logging without affecting unified logging, use the **bp.conf** and **vm.conf** files.

See “**How to set legacy logging levels**” on page 110.
To set the logging level for unified logging without affecting legacy logging, use the `vxlogcfg` command.

See “Configuring and using unified logging” on page 93.

The NetBackup Administration Console **Global logging level** field allows values of 0 to 5.

**Table 3-3** lists the kind of detail each level includes.

<table>
<thead>
<tr>
<th>Logging level</th>
<th>Information to be logged</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Very important low-volume diagnostic and debug messages</td>
</tr>
<tr>
<td>1</td>
<td>This level adds verbose diagnostic and debug messages</td>
</tr>
<tr>
<td>2</td>
<td>Adds the progress messages</td>
</tr>
<tr>
<td>3</td>
<td>Adds the informational dumps</td>
</tr>
<tr>
<td>4</td>
<td>Adds the function entry and exits</td>
</tr>
<tr>
<td>5</td>
<td>Finest detail: everything is logged</td>
</tr>
</tbody>
</table>

Note the following:

- In the Global logging level field of the Administration Console, 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 field in the NetBackup Administration Console. You can set it with the `vxlogcfg` command. See “Configuring and using unified logging” on page 93.

- A change to Global logging level 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, it only affects the legacy logging level.

- If you make a change with the `vxlogcfg` command, it only affects the unified logging level.
Unified logging file rollover

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

Log rollover can occur according to any of the following options as set by the \texttt{vxlogcfg} command:

- File size (this option is the default), as defined by the MaxLogFileSizeKB option.
- Local time, as defined by the RolloverAtLocalTime option.
- Periodic (elapsed time), as defined by the RolloverPeriodInSeconds option.
- File size or Local time, whichever limit is encountered first
- File size or Periodic, whichever limit is encountered first

To set these options, use the \texttt{vxlogcfg} command with the RolloverMode option.

An example that uses \texttt{vxlogcfg} is available:

See “\texttt{vxlogcfg} command” on page 96.

By default, log-file rollover is based on file size (5120 KB). When a log file reaches 5120 KB in size, the file is closed and a new one is created.

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

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

Logs for the processes that are listed in Table 3-2 can use rotation. Certain legacy logs can also use rotation.

See “Legacy logging file rotation (robust logging)” on page 107.

Log file recycling (removing older log files)

Two ways to automatically delete log files are as follows:

- Unified logging files can be automatically deleted when the number of log files exceeds a certain number. The NumberOfLogFiles option on the \texttt{vxlogcfg} command defines that number. An example of \texttt{vxlogcfg} usage is available:
  See “\texttt{vxlogcfg} command” on page 96.

- The Keep logs For setting can delete both unified logs and legacy logs. This parameter is located in the Clean-up dialog box under Host Properties in the NetBackup Administration Console.
Note the following regarding the Keep logs For setting:

- Logs that age beyond the number of days that the Keep logs For setting specifies are deleted for unified and legacy logging.

- Unified logging log files can also be deleted explicitly using the `vxlogmgr` command. If `vxlogmgr` does not manually delete or move files, the Keep logs For setting removes the old logs for both unified and legacy logging.

If the `vxlogcfg LogRecycle` option is ON (true), the Keep logs For 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 is specified by `NumberOfLogFiles` on the `vxlogcfg` command.

Configuring and using unified logging

This section describes commands for controlling unified logging with examples.

To access logging controls in the NetBackup Administration Console, click **Host Properties > Master/Media Server > Properties > Logging**. Also, three commands that manage unified logging are also available and described in this section. These commands are located in `/usr/openv/netbackup/bin` (UNIX) and `install_path\NetBackup\bin` (Windows).

**vxlogview command**

Use this command to view the logs that unified logging creates. These logs are stored in subdirectories in `/usr/openv/logs` on UNIX or `install_path\logs` on Windows.

Unlike the files that are written in legacy logging, you cannot view unified logging files 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.

- Specify the PBX product ID by entering `-p 50936` as a parameter on the `vxlogview` command line.

**vxlogview examples**

Example 1
Display the log messages for NetBackup that show only the date, time, message type, and message text:

   vxlogview --prodid 51216 --display D,T,m,x

Example 2
Display the log messages for originator 116 (nbpem) that were issued during the last 20 minutes:

   vxlogview -o 116 -t 00:20:00

Note that you can specify -o nbpem instead of -o 116.

Example 3
Display the log messages for nbpem that were issued during a particular time period:

   vxlogview -o nbpem -b "05/03/05 06:51:48 AM" -e "05/03/05 06:52:48 AM"

Example 4
You can use the -i option instead of -o, to specify an originator:

   vxlogview -i nbpem

The vxlogview -i option searches only the log files that the specified process (nbpem) creates. The originator ID of these files in the log file name is 116. 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 messages that are logged by the specified process.

**Note:** If you use the -i option with a process that is not a service (no originator ID in the file name), vxlogview returns the message "No log files found." In this case, use the -o option instead of the -i option. Typically, the NetBackup process is a service if it appears in the Activity Monitor of the NetBackup Administration Console, under the Daemons tab (UNIX) or Services tab (Windows).

Example 5
You can search the logs for a particular job ID:

   vxlogview -i nbpem | grep "jobid=job_ID"
Note: The jobid= search key should contain no spaces, and jobid= must be lowercase.

When searching for a job ID, you can use any `vxlogview` command options. This example uses the -i option with the name of the process (nbpem).

**vxlogmgr command**

Use this command to manage unified logging files, such as to move or delete logs.

**Example 1**

List all unified log files for the `nbrb` service:

```
vxlogmgr -s -o nbrb
```

**Example output:**

```
/usr/openv/logs/nbrb/51216-118-1342895976-050503-0000000000.log
/usr/openv/logs/nbrb/51216-118-1342895976-050504-0000000000.log
/usr/openv/logs/nbrb/51216-118-1342895976-050505-0000000000.log
Total 3 file(s)
```

If the `vxlogcfg NumberOfLogFiles` option is set to 1, the following deletes the two oldest log files for the `nbrb` service:

```
vxlogmgr -d -o nbrb -a
```

**Example output:**

```
Following are the files that were found:
/usr/openv/logs/nbrb/51216-118-1342895976-050504-0000000000.log
/usr/openv/logs/nbrb/51216-118-1342895976-050505-0000000000.log
Total 2 file(s)
Are you sure you want to delete the file(s)? (Y/N): Y
Deleting /usr/openv/logs/nbrb/51216-118-1342895976-050505-0000000000.log ...
Deleting /usr/openv/logs/nbrb/51216-118-1342895976-050504-0000000000.log ...
```

**Example 2**

Delete the unified log files that NetBackup created in the last 15 days:

```
vxlogmgr -d --prodid 51216 -n 15
```

**Example 3**
Delete all unified log files for originator `nbrb`:

```
vxlogmgr -d -o nbrb
```

Example 4
Delete all unified log files for NetBackup:

```
vxlogmgr -d -p NB
```

**vxlogcfg command**

Use this command to configure unified logging settings. For instance, use `vxlogcfg` to change logging levels and rollover settings.

Note the following items:

- `vxlogcfg` 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` settings for robust file logging (`MaxLogFileSizeKB` and `NumberOfLogFiles`) also affect certain legacy logs. See “Legacy logging file rotation (robust logging)” on page 107.
- Absolute paths must be specified, not relative ones.

**Controlling log file size**

By default, the maximum log file size in unified logging is 5120 KB. After a log file reaches 5120 KB, the file closes and a new log file opens.

You can change the maximum file size with the `vxlogcfg` command’s `MaxLogFileSizeKB` option. The following example changes the default maximum log size to 2048 KB for product NetBackup:

```
vxlogcfg -a -p 51216 -o Default -s MaxLogFileSizeKB=2048
```

**Note:** For `MaxLogFileSizeKB` to be effective, the `vxlogcfg` command’s `RolloverMode` option must be set to `FileSize`.

The following sets the default NetBackup rollover mode:

```
vxlogcfg -a --prodid 51216 --orgid Default -s RolloverMode=FileSize
```
MaxLogFileSizeKB can be set per originator. If it is not configured for a given originator, that originator 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
```

To make nbrb follow the default setting again, execute:

```
vxlogcfg -r -p 51216 -o nbrb -s MaxLogFileSizeKB
```

### Setting rollover mode

The following example sets the NetBackup (prodid 51216) rollover mode to periodic:

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

This example sets rollover mode for nbem (originator ID 116) to periodic. It also sets the interval until the next nbem log file rollover to 24 hours (86400 seconds).

### Setting 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=5120 NumberOfLogFiles=999999 LogRecycle=TRUE
```

This example sets nbemm rollover mode to file size, and turns on log recycling. When the number of log files exceeds 999999, the oldest log file is deleted.

See “Controlling the number of log files with vxlogmgr” on page 98.

### Setting debug level and diagnostic level

The following example sets the debug level and diagnostic level for all the originators of product ID NetBackup (51216):

```
vxlogcfg -a --prodid 51216 --orgid ALL -s DebugLevel=0
DiagnosticLevel=1
```

For further details on these commands, refer to the *NetBackup Commands* manual or to the man pages.
Listing 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, NumberOfLogFile, and RolloverMode are included in the output.

```
vxlogcfg -l -o nbrb -p NB
```

Output:

```
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
NumberOfLogFile = 4
OIDNames = nbrb
L10nLib = /usr/openv/lib/libvxexticu.so
L10nResource = nbrb
L10nResourceDir = /usr/openv/resources
SyslogIdent = VRTS-NB
SyslogOpt = 0
SyslogFacility = LOG_LOCAL5
LogFilePermissions = 436
```

Controlling the number of log files with `vxlogmgr`

You can use the `vxlogmgr` command with the `vxlogcfg` command's `NumberOfLogFile` option to manually delete log files.

For example, you currently have 10 unified logging files and the `vxlogcfg` command's `NumberOfLogFile` option is set to 2. Enter the following to keep the two most recent log files and delete the rest for all originators:

```
vxlogmgr -a -d
```

The following applies to all NetBackup originators:

```
vxlogmgr -a -d -p NB
```
The following applies to all PBX originators:

```
 vxlogmgr -a -d -p ics
```

The following deletes log files for the `nbrb` service only:

```
 vxlogmgr -a -d -o nbrb
```

**Controlling disk space usage with `vxlogmgr`**

Periodically run the `vxlogmgr -a` 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:

\[
\text{NumberOfFiles for originator} \times \text{MaxLogFileSizeKB for originator}
\]

The total disk space NetBackup 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:

\[
\text{Number of NetBackup originators} \times \text{default MaxLogFileSizeKB} \times \\
\text{default NumberOfFiles}
\]

To see the current unified logging settings, use the `vxlogcfg` command as shown in the following topic:

See “Listing unified logging settings” on page 98.

For example, assume the following:

- `vxlogmgr -a -p NB` is configured as a cron job with a frequency of 1 hour.
- No NetBackup originators override default settings for `MaxLogFileSizeKB` or `NumberOfFiles`.
- The number of active NetBackup originators on the host is 10. (This total may be typical of a NetBackup master server that is not running BMR or NDMP.)
- The default `NumberOfFiles` is equal to 3.
- The default `MaxLogFileSizeKB` is equal to 5120.

Given these conditions, unified logging consumes:

\[
\text{Number of NetBackup originators} \times \text{default MaxLogFileSizeKB} \times \\
\text{default NumberOfFiles}
\]

Which is \(10 \times 5120 \times 3 \text{ KB}, \) or 15360 kilobytes of disk space at the end of each hour.
Submitting unified logging files to &Company Name; support

This topic describes an example of how to gather unified logs for NetBackup.

To gather unified logs for NetBackup

1. Create a directory:
   ```bash
   mkdir /upload
   ```

2. To copy unified logs (for NetBackup only) to the /upload directory:
   ```bash
   vxlogmgr -p NB -c --dir /upload
   ```

Example output:

Following are the files that were found:

```
/usr/openv/logs/bmrsetup/51216-157-2202872032-050125-0000000000.log
/usr/openv/logs/nbemm/51216-111-2202872032-050125-0000000000.log
/usr/openv/logs/nbrb/51216-118-2202872032-050125-0000000000.log
/usr/openv/logs/nbjm/51216-117-2202872032-050125-0000000000.log
/usr/openv/logs/nbpm/51216-116-2202872032-050125-0000000000.log
/usr/openv/logs/nbsl/51216-132-2202872032-050125-0000000000.log
Total 6 file(s)
```

Copying

```bash
/usr/openv/logs/bmrsetup/51216-157-2202872032-050125-0000000000.log ...
Copying
/usr/openv/logs/nbemm/51216-111-2202872032-050125-0000000000.log ...
Copying
/usr/openv/logs/nbrb/51216-118-2202872032-050125-0000000000.log ...
Copying
/usr/openv/logs/nbjm/51216-117-2202872032-050125-0000000000.log ...
Copying
/usr/openv/logs/nbpm/51216-116-2202872032-050125-0000000000.log ...
Copying
/usr/openv/logs/nbsl/51216-132-2202872032-050125-0000000000.log ...
```
3 Change to the /upload directory and list its contents:

```bash
cd /upload
ls
```

Output:

- 51216-111-2202872032-050125-0000000000.log
- 51216-116-2202872032-050125-0000000000.log
- 51216-117-2202872032-050125-0000000000.log
- 51216-118-2202872032-050125-0000000000.log
- 51216-132-2202872032-050125-0000000000.log
- 51216-157-2202872032-050125-0000000000.log

4 Tar the log files:

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

Legacy NetBackup logging

Certain NetBackup processes use unified logging.

See “Unified logging” on page 83.

All other NetBackup processes use legacy logging.

**Enabling legacy logging**

In legacy debug logging, each process creates logs of debug activity in its own logging directory. To enable legacy debug logging on NetBackup servers, create the appropriate directories for each process for the following platforms:

- **On UNIX:**
  ```
  /usr/openv/netbackup/logs
  /usr/openv/volmgr/debug
  ```

- **On Windows:**
  ```
  install_path\NetBackup\logs
  install_path\Volmgr\debug
  ```

Information is available about how to enable the Status Collector Daemon:

See “Enabling the status collector daemon” on page 107.

Tables are available that list the log directories that you must create.
See Table 3-4 on page 102.

See Table 3-5 on page 105.

**Note:** You must create these directories before logging can take place. If these directories exist, NetBackup creates log files in the directory for the associated process. A debug log file is created when the process begins.

**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.

## NetBackup server legacy debug logs

Table 3-4 describes the server legacy debug logs.

<table>
<thead>
<tr>
<th>Debug log directory to create</th>
<th>Create directory under</th>
<th>Associated process</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td><code>/usr/openv/netbackup/logs</code> (UNIX)</td>
<td>Administrative commands.</td>
</tr>
<tr>
<td></td>
<td><code>install_path\NetBackup\logs</code> (Windows)</td>
<td></td>
</tr>
<tr>
<td>bpbrm</td>
<td><code>/usr/openv/netbackup/logs</code> (UNIX)</td>
<td>NetBackup and restore manager.</td>
</tr>
<tr>
<td></td>
<td><code>install_path\NetBackup\logs</code> (Windows)</td>
<td></td>
</tr>
<tr>
<td>bpcd</td>
<td><code>/usr/openv/netbackup/logs</code> (UNIX)</td>
<td>NetBackup client daemon or manager. The NetBackup Client service starts this process</td>
</tr>
<tr>
<td></td>
<td><code>install_path\NetBackup\logs</code> (Windows)</td>
<td></td>
</tr>
<tr>
<td>bpdbjobs</td>
<td><code>/usr/openv/netbackup/logs</code> (UNIX)</td>
<td>NetBackup jobs database manager program.</td>
</tr>
<tr>
<td></td>
<td><code>install_path\NetBackup\logs</code> (Windows)</td>
<td></td>
</tr>
<tr>
<td>bpdm</td>
<td><code>/usr/openv/netbackup/logs</code> (UNIX)</td>
<td>NetBackup disk manager.</td>
</tr>
<tr>
<td></td>
<td><code>install_path\NetBackup\logs</code> (Windows)</td>
<td></td>
</tr>
<tr>
<td>bpdbm</td>
<td><code>/usr/openv/netbackup/logs</code> (UNIX)</td>
<td>NetBackup database manager. This process runs only on master servers. On Windows systems, it is the NetBackup database manager service.</td>
</tr>
<tr>
<td></td>
<td><code>install_path\NetBackup\logs</code> (Windows)</td>
<td></td>
</tr>
<tr>
<td>Debug log directory to create</td>
<td>Create directory under</td>
<td>Associated process</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------</td>
<td>--------------------</td>
</tr>
</tbody>
</table>
| bpjava-msvc                  | /usr/openv/netbackup/logs (UNIX)  
install_path\NetBackup\logs (Windows)  | 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                 | /usr/openv/netbackup/logs (UNIX)  
install_path\NetBackup\logs (Windows)  | 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 `bpjava-msvc` is running (all Windows platforms). |
| bprd                         | /usr/openv/netbackup/logs (UNIX)  
install_path\NetBackup\logs (Windows)  | NetBackup request daemon or manager. On Windows systems, this process is called the NetBackup Request Manager service. |
| bpsynth                      | /usr/openv/netbackup/logs (UNIX)  
install_path\NetBackup\logs (Windows)  | The NetBackup process for synthetic backup. `nbjm` starts `bpsynth`. `bpsynth` runs on the master server. |
| bptm                         | /usr/openv/netbackup/logs (UNIX)  
install_path\NetBackup\logs (Windows)  | NetBackup tape management process. |
| syslogs                      | You must enable system logging to troubleshoot `ltid` or robotic software. See the `syslogd` man page. | System log. |
### Table 3-4 NetBackup legacy logs (not media and device management) (continued)

<table>
<thead>
<tr>
<th>Debug log directory to create</th>
<th>Create directory under</th>
<th>Associated process</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_ops</td>
<td>/usr/openv/netbackup/logs (UNIX)</td>
<td>The <strong>user_ops</strong> 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 user Backup, Archive, and Restore program (<strong>jbpSA</strong>) generates. This directory must exist for successful operation of any of the Java programs and must have public read, write, and execute permissions. The <strong>user_ops</strong> 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 <strong>nbjlogs</strong> subdirectory. All files in the <strong>user_ops</strong> directory hierarchy are removed according to the setting of the <strong>KEEP_LOGS_DAYS</strong> configuration option.</td>
</tr>
<tr>
<td>vnetd</td>
<td>/usr/openv/netbackup/logs (UNIX)</td>
<td>The Symantec network daemon, used to create &quot;firewall friendly&quot; socket connections. Started by the <strong>inetd</strong> process. <strong>Note:</strong> Logging occurs in either the <strong>/usr/openv/logs</strong> directory or the <strong>/usr/openv/netbackup/logs</strong> if the <strong>vnetd</strong> directory exists there. If the <strong>vnetd</strong> directory exists in both locations, logging occurs only in <strong>/usr/openv/netbackup/logs/vnetd</strong>.</td>
</tr>
</tbody>
</table>

More information is available on the programs and daemons that write the logs. See “About backup and restore functional overview” on page 631.

On UNIX systems, also refer to the **README** file in the **/usr/openv/netbackup/logs** directory.
Media and device management legacy debug logs

The debug log directories that are written to /usr/openv/volmgr/debug (UNIX) or \install_path\Volmgr\debug (Windows) enable logging for the media management processes and device management processes.

Note the following items:

- NetBackup creates one log per day in each of the debug directories.
- Information is available about the format of the log file names. See “Legacy logging file name format without log file rotation” on page 109.
- On UNIX: To disable vmd debug logging, either delete or rename the /usr/openv/volmgr/debug/daemon directory.
- On Windows, to disable debug logging for the NetBackup Volume Manager service, either delete or rename the \install_path\Volmgr\debug\daemon folder.
- NetBackup retains debug logs for the number of days you specify with the DAYS_TO_KEEP_LOGS = entry in the vm.conf file. (The default is infinite retention.) For instructions on how to use this entry, see the NetBackup Administrator’s Guide, Volume II.

Table 3-5 describes the media management legacy debug log and device management legacy debug logs.

<table>
<thead>
<tr>
<th>Debug log directory to create</th>
<th>Create directory under</th>
<th>Associated process</th>
</tr>
</thead>
<tbody>
<tr>
<td>acsssi</td>
<td>/usr/openv/volmgr/debug (UNIX)</td>
<td>Debug information on transactions between NetBackup and the Storage Tek ACSLS server.</td>
</tr>
<tr>
<td>daemon</td>
<td>/usr/openv/volmgr/debug (UNIX) \install_path\Volmgr\debug (Windows)</td>
<td>Debug information for vmd (NetBackup Volume Manager service, Windows) and its associated processes (oprd and rdevmi). Stop and restart vmd after creating the directory.</td>
</tr>
<tr>
<td>ltid</td>
<td>/usr/openv/volmgr/debug (UNIX) \install_path\Volmgr\debug (Windows)</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 3-5  Media and device management legacy debug logs (continued)

<table>
<thead>
<tr>
<th>Debug log directory to create</th>
<th>Create directory under</th>
<th>Associated process</th>
</tr>
</thead>
</table>
| reqlib                       | /usr/openv/volmgr/debug (UNIX)  
install_path\Volmgr\debug (Windows) | Debug information on the processes that request media management services from vmd or EMM. Stop and restart vmd after creating the directory. |
| robots                       | /usr/openv/volmgr/debug (UNIX)  
install_path\Volmgr\debug (Windows) | Debug information on all robotic daemons, which includes tldcd, tl8cd, and tl4d daemons. Stop and restart robotic daemons. |
| tpcommand                    | /usr/openv/volmgr/debug (UNIX)  
install_path\Volmgr\debug (Windows) | Debug information for device configuration, including the tpconfig and the tpautoconf commands and the NetBackup Administration Console. |
| vmscd                        | /usr/openv/volmgr/debug/ (UNIX)  
install_path\Volmgr\debug\ (Windows) | Debug information for the NetBackup Status Collection daemon. Stop and restart vmscd after creating the directory. |

### Enabling system logs

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.

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.

The command you use is one of the following:

- 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.

  Or

- A command to start a specific daemon (for example, `acsd -v`).

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

**Enabling the status collector daemon**

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:

- **On UNIX:** `/usr/openv/volmgr/debug/reqlib`
- **On Windows:** `install_path\Volmgr\debug\reqlib\`

**Controlling legacy logs**

NetBackup retains legacy debug logs for the number of days that are specified in the Keep Logs global attribute (28 days by default). Then it deletes them.

Instructions are available on how to change Keep Logs.

See the *NetBackup Administrator’s Guide, Volume I*.

A robust logging feature is also available for controlling the size of debug logs that certain NetBackup processes create.

See “Legacy logging file rotation (robust logging)” on page 107.

Debug logs can grow very large. Enable them only if unexplained problems exist. Delete the logs and the associated directory when they are no longer needed.

**Legacy logging file rotation (robust logging)**

To control the size of legacy logs written by certain NetBackup processes, a feature called robust logging can be used. This feature does not apply to media and device management logging.

See “Media and device management log retention” on page 108.

This feature involves file rotation, as used in unified logging.

See “Unified logging file rollover” on page 92.

To limit the amount of disk space that the logs consume, do the following: set the maximum size for a log file and the 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 is opens. If the new file exceeds the number of log files that is allowed for the directory, the oldest file is deleted.

Logs created by the following NetBackup processes can use log rotation (robust logging):
- `bpbkar` (client process only)
- `bpbrm`
- `bpcd`
- `bpdbm`
- `bpdm`
- `bprd`
- `bptm`

For the legacy logs created by other NetBackup processes (but not media and device management), use the Keep Logs For setting as follows:

- Windows: In the **Host Properties > Properties > Clean-up** dialog box
- UNIX: In the **Host Properties > Properties > Global Attributes** dialog box

The Keep Logs For setting ultimately applies to all legacy logs. If this setting is 10 and robust file logging settings allow logs to exist more than 10 days, the logs are deleted on day 11.

**Media and device management log retention**

For media and device management legacy logs, use the DAYS_TO_KEEP_LOGS setting in the `vm.conf` file to control log file rotation. This file is located in `/usr/openv/volmgr/` (UNIX) and `install_path\Volmgr\` (Windows). For example, enter the following in the `vm.conf` file:

```
DAYS_TO_KEEP_LOGS = 3
```

**Configuring legacy log rotation**

This procedure shows how to configure legacy log rotation.
To configure the legacy log rotation

1. Go to Host Properties > Master Servers > Properties > Logging and click the Enable robust logging box to enable legacy log rotation. This item applies to legacy logs only.

   By default, the maximum file size is 5120 KB and the number of files that are kept per log directory is 3.

   If Enable robust logging is disabled, the standard log-file behavior remains in effect: one log file is created per log directory per day, and log deletion is based on the Keep Logs For setting.

2. To change the maximum file size, or number of log files per directory, use the MaxLogFileSizeKB and NumberOfLogFiles options on the vxlogcfg command.

   The vxlogcfg command is located in /usr/openv/netbackup/bin (on UNIX) and install_path\NetBackup\bin (on Windows).

   For example:

   vxlogcfg -a -p 51216 --orgid Default -s MaxLogFileSizeKB=2048,NumberOfLogFiles=10

   This example sets the maximum file size to 2048 KB and sets the maximum number of log files per log directory to 10.

   It sets the default values for all unified logging processes and for the legacy processes for NetBackup (product ID 51216). A list of these processes is available:

   See “Legacy logging file rotation (robust logging)” on page 107.

   More examples of the vxlogcfg command are available.

   See “Configuring and using unified logging” on page 93.

   You can also refer to the vxlogcfg man page or to the NetBackup Commands manual.

Legacy logging file name format without log file rotation

Two log file name formats are used in legacy logging. The format depends on whether or not the log uses file rotation (robust logging).

In the standard legacy log system, a NetBackup process creates one debug log file per day.

The log file name is of the following format:

- On UNIX: log.mmdyyyy
For example: log.040805

- On Windows: mmddyy.log
  For example: 040105.log

**Legacy logging file name format with log file rotation**

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. The file name is of this format:

```
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 log files are already created with the standard legacy naming format and then robust file logging is enabled, the following occurs: only the new log files for the processes that robust logging governs use the new file rotation naming format.

Any mixture of new and old log file names in a legacy debug log directory is managed according to the following: the **Keep Logs For** setting and the robust logging settings, when applicable.

See “[Legacy logging file rotation (robust logging)](page-107)” on page 107.

**How to set legacy logging levels**

You can set legacy logging levels to increase the amount of information that processes can write in the logs.

The following settings affect legacy logging, except media and device management.

- On Windows or UNIX systems, set the Global Logging Level to a higher level, in the Logging dialog box. (Click Host Properties > Master Server Properties > Logging tab > Logging dialog box.)

  Note: This setting affects legacy logging (but not media and device management logging) and unified logging.

  More information is available for synthetic backup.  
  See “[Logs to accompany problem reports for synthetic backup](page-111)” on page 111.
On UNIX, add a `VERBOSE` entry in the `/usr/openv/netbackup/bp.conf` file. `VERBOSE` by itself sets the verbose value 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.

Use the Logging dialog box to set the logging level for individual processes. (Click Host Properties > Master Server Properties > Logging tab > Logging dialog box.) Or, specify the verbose flag (if available) when you start the program or daemon.

See the NetBackup Administrator’s Guide, Volume I.

In media and device management legacy logging, only two levels exist: not verbose (the default), and verbose. To set the verbose (higher) level, add the word `VERBOSE` to the `vm.conf` file. Create the `vm.conf` file if necessary and restart `ltid` and `vmd` after you add the `VERBOSE` entry.

On UNIX, add `VERBOSE` to the `/usr/openv/volmgr/vm.conf` file.

On Windows, add `VERBOSE` to the `install_path\Volmgr\vm.conf` file. This entry affects logging levels in the Event Viewer Application and System log.

Logs to accompany problem reports for synthetic backup

To debug problems with synthetic backups, you must include in the problem report a complete set of logs.

The two types of logs to include are as follows:

- Log files that unified logging creates
  For information about how to gather unified logging files relevant to the problem, see the following:
  See “Submitting unified logging files to &CompanyName; support” on page 100.

- Log files that legacy logging creates
  If the following legacy log directories have not been created, you must create the directories. Set the debug level to 5 and then rerun the job.

  1. Create the following directories on the master server:
     
        ```
        install_path/netbackup/logs/bpsynth
        install_path/netbackup/logs/bpdbm
        install_path/netbackup/logs/vnetd
        ```

  2. Create the following directories on the media server:
install_path/netbackup/logs/bpcd
install_path/netbackup/logs/bptm
install_path/netbackup/logs/bpdm

- Set the logging level as follows:
  Use the Global logging level option on the Logging tab in the Master Server Properties dialog box.
  See “Using the Host Properties window” on page 60.

- Rerun the job and then 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.

Try file
Include the try file for the job ID from the following directory:

install_path/netbackup/db/jobs/trylogs/jobid.t

For instance, if the job ID of the synthetic backup job was 110, then the try file is named 110.t.

Policy attributes
Capture the output from the following command and send it to Support with the rest of the information:

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 output from the following command and send it to Support with the rest of the information:

install_path/netbackup/bin/admincmd/bpstulist -L
Debug logs on UNIX clients

Most UNIX client logs are of the legacy type, with the exception of a few Bare Metal Restore processes, as explained in this section.

Unified logging on UNIX clients

The following are the UNIX client processes that use unified logging:

- **nbftclnt**: originator ID 200.
- **bmrsavecfg**: originator ID 121.
- **bmrc**: originator ID 122. bmrc originates from the BMR boot server, which may or may not be a NetBackup server, and runs on the restoring client.
- **nbbrowse**: originator ID 359. NetBackup Client Browser.
- **nbcs**: originator ID 366. Client service.

A description is available of unified logging file name format and other details:

See “Unified logging” on page 83.

Unified logging is enabled by default.

Legacy logging on UNIX clients

To enable legacy debug logging on UNIX clients, create the appropriate directories in the following directory path:

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

The following table lists the legacy debug log directories that apply to UNIX clients. Additional information on legacy logging is available:

See “Legacy NetBackup logging” on page 101.

---

**Note:** Create the directories with access modes of 777 so that user processes can write to the log files.

Table 3-6 describes the UNIX client debug logs for legacy logging.
## Table 3-6 UNIX client debug logs: Legacy logging

<table>
<thead>
<tr>
<th>Debug log directory</th>
<th>Associated process</th>
</tr>
</thead>
<tbody>
<tr>
<td>bp</td>
<td>Menu driven client-user interface program.</td>
</tr>
<tr>
<td>bparchive</td>
<td>Archive program. Also useful for debugging bp.</td>
</tr>
<tr>
<td>bpbackup</td>
<td>Backup program. Also useful for debugging bp.</td>
</tr>
<tr>
<td>bpbkar</td>
<td>Program that is used to generate backup images.</td>
</tr>
<tr>
<td>bpcd</td>
<td>NetBackup client daemon or manager.</td>
</tr>
<tr>
<td>bphdb</td>
<td>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.</td>
</tr>
<tr>
<td>bpjava-msvc</td>
<td>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.</td>
</tr>
<tr>
<td>bpjava-usvc</td>
<td>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.</td>
</tr>
<tr>
<td>bplist</td>
<td>Program that lists backed up and archived files. Also useful for debugging bp.</td>
</tr>
<tr>
<td>bmpmount</td>
<td>Program that determines local mount points and wildcard expansion for Multiple Data Streams.</td>
</tr>
<tr>
<td>bporaexp</td>
<td>Command-line program on clients to export Oracle data in XML format. Communicates with bprd on server.</td>
</tr>
<tr>
<td>bporaexp64</td>
<td>64-bit command-line program on clients to export Oracle data in XML format. Communicates with bprd on server.</td>
</tr>
<tr>
<td>bporaimp</td>
<td>Command-line program on clients to import Oracle data in XML format. Communicates with bprd on server.</td>
</tr>
<tr>
<td>bporaimp64</td>
<td>64-bit command-line program on clients to import Oracle data in XML format. Communicates with bprd on server.</td>
</tr>
<tr>
<td>bprestore</td>
<td>Restore program. Also useful for debugging bp.</td>
</tr>
</tbody>
</table>
Table 3-6 UNIX client debug logs: Legacy logging (continued)

<table>
<thead>
<tr>
<th>Debug log directory</th>
<th>Associated process</th>
</tr>
</thead>
<tbody>
<tr>
<td>db_log</td>
<td>For more information on these logs, see the NetBackup guide for the database-extension product that you use.</td>
</tr>
<tr>
<td>mtfrd</td>
<td>These logs have information about the mtfrd process, which is used for phase 2 imports and restores of Backup Exec media.</td>
</tr>
<tr>
<td>tar</td>
<td>tar process during restores.</td>
</tr>
<tr>
<td>user_ops</td>
<td>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 user 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.</td>
</tr>
</tbody>
</table>

Controlling log size on UNIX clients

For the unified logging files that the Bare Metal Restore process bmrsavecfg creates, you can control logging with log file rotation.

See “Unified logging file rollover” on page 92.

For the legacy logging files that the bpbkar and the bpcd processes create, you can control logging with log file rotation.

See “Legacy logging file rotation (robust logging)” on page 107.

For all other client logs, logs are kept for the number of days that are specified in the following setting: Keep status of user-directed backups, archives, and restores for on the Host Properties > Clients > Properties > UNIX Client > Client Settings dialog box.

Client logging file name format on UNIX clients

A description of logging file name format is available.
How to set logging levels on UNIX clients

To increase the amount of information that client processes write in the logs, go to the Logging dialog box. (Click Host Properties > Clients > Properties > Logging dialog box.)

Debug logs on PC clients

Most PC client logs are of the legacy type, with the exception of a few Bare Metal Restore processes, as explained in this section.

Unified logging on PC clients

The following are Windows client processes that use unified logging:

- nbftclnt: originator ID 200
- bmrsavecfg: originator ID 121.
- bmrc: originator ID 122. bmrc originates from the BMR boot server, which may or may not be a NetBackup server, and runs on the restoring client.
- bmrrst.exe and bmrmap.exe: originator ID 131. These originate from the BMR boot server, which may or may not be a NetBackup server, and run on the restoring client.

A discussion of file name format and other unified logging details is available.

See “Unified logging file name format” on page 83.

Unified logging is enabled by default.

Legacy debug logging on PC clients

To enable detailed legacy debug logging on Microsoft Windows or NetWare target clients, create the appropriate directories in the following locations:
Note: These are the default locations in which to place these directories. You can specify another location during client installation.

- **Windows clients** - C:\Program Files\VERITAS\NetBackup\Logs\n- **NetWare clients** - SYS:VERITAS\NBCTL\NetBack\logs\n
Table 3-7 lists the legacy debug log directories that apply to these clients:

<table>
<thead>
<tr>
<th>Debug log directory</th>
<th>NetBackup client</th>
<th>Associated process</th>
</tr>
</thead>
<tbody>
<tr>
<td>bp</td>
<td>NetWare target</td>
<td>Client-user interface program for NetWare.</td>
</tr>
<tr>
<td>bpinitd</td>
<td>Windows2003</td>
<td>Client service logs. These logs have information on the bpinetd32 process.</td>
</tr>
<tr>
<td>bparchive</td>
<td>Windows 2003</td>
<td>Archive program that is run from the command line.</td>
</tr>
<tr>
<td>bpbackup</td>
<td>Windows 2003</td>
<td>The backup program that is run from the command line.</td>
</tr>
<tr>
<td>bppkar</td>
<td>Windows 2003</td>
<td>Backup and archive manager. These logs have information on the bppkar32 process.</td>
</tr>
<tr>
<td>bpcd</td>
<td>All Windows and NetWare clients</td>
<td>NetBackup client daemon or manager. These logs have information on communications between the server and client. On NetWare clients, these logs also contain the log information for the backup and restore processes.</td>
</tr>
<tr>
<td>bpjava-msvc</td>
<td>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.)</td>
<td>bpjava-msvc</td>
</tr>
</tbody>
</table>
Table 3-7  PC client debug logs: Legacy logging *(continued)*

<table>
<thead>
<tr>
<th>Debug log directory</th>
<th>NetBackup client</th>
<th>Associated process</th>
</tr>
</thead>
<tbody>
<tr>
<td>bpjava-usvc</td>
<td>NetBackup program that <code>bpjava-msvc</code> starts upon successful login through the Login 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 <code>bpjava-msvc</code> is running. <em>(On all Windows platforms.)</em></td>
<td>bpjava-usvc</td>
</tr>
<tr>
<td>bplist</td>
<td>Windows 2003 List program that is run from the command line.</td>
<td></td>
</tr>
<tr>
<td>bpmount</td>
<td>Windows 2003 The program that is used to collect drive names on the client for multistreaming clients.</td>
<td></td>
</tr>
<tr>
<td>bprestore</td>
<td>Windows 2003 The restore program that is run from the command line.</td>
<td></td>
</tr>
<tr>
<td>bpsrv</td>
<td>NetWare nontarget NetBackup service utility. This program allows the system with the user interface to communicate with the NetBackup for NetWare client.</td>
<td></td>
</tr>
<tr>
<td>tar</td>
<td>Windows 2003 <code>tar</code> process. These logs have information about the <code>tar32</code> process.</td>
<td></td>
</tr>
</tbody>
</table>
Table 3-7  PC client debug logs: Legacy logging (continued)

<table>
<thead>
<tr>
<th>Debug log directory</th>
<th>NetBackup client</th>
<th>Associated process</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_ops</td>
<td>Windows 2003</td>
<td>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 user 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.</td>
</tr>
</tbody>
</table>

Controlling log size on PC clients

For the unified logging files that the Bare Metal Restore process bmrsavecfg creates, you can control logging with log file rotation.

See “Unified logging file rollover” on page 92.

For the legacy logging files that the bpbkar and the bpcd processes create, you can control logging with log file rotation.

See “Legacy logging file rotation (robust logging)” on page 107.

For all other client logs, note the following:

- For Windows clients, logs are kept for the number of days that are specified in the Backup, Archive, and Restore interface. On the File menu, click NetBackup Client Properties > General tab: Keep status of user-directed backups, archives, and restores for.
For NetWare clients, logs are kept the number of days that are specified in file `\veritas\nbuclt\netback\bp.ini` (under `Keep_Logs_Days`).

Client logging file name format on PC clients

A description of logging file name format is available.
See “Unified logging file name format” on page 85.
See “Legacy logging file name format without log file rotation” on page 109.

How to set logging levels on PC clients

To increase the amount of information that client processes write in the logs:

- For the unified logging files that the Bare Metal Restore process `bmrsavecfg` creates, you also can control logging level with the `vxlogcfg` command. See “Configuring and using unified logging” on page 93.
- On NetWare clients, change the value of the `level` and the `tcp` parameters in the debug section of the `bp.ini` file. For instructions, see the NetBackup user guide for the client.

An increase in the log level can cause the logs to grow very large; increase the logging level only if unexplained problems exist.

Windows Event Viewer logging option

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.

For example, execute the following to route 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 be effective, restart NetBackup services.
Enabling the logging tool

This topic shows you how to enable the logging tool.

To enable the logging tool

1. Create the following file on the NetBackup master server:

   \install_path\NetBackup\db\config\eventlog

2. Add an entry (optional) to the eventlog file that specifies the severity and type of NetBackup messages that are written. The following is an example:

   56 255

eventlog file entries

The eventlog entry has the following two parameters:

- The first parameter controls the messages that NetBackup writes to the Application Log, which are based on severity level.
- The second parameter controls the type of messages that NetBackup writes to the Application Log.

Both parameters are specified as decimal numbers and equate to a bitmap that expresses these 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

If the file is empty, the default severity is Error (16) and the default type is Backup Status (64).

If the file has only one parameter, it is used for the severity level. The default value of Backup Status (64) is used for the type.

Example

Assume you want to include all types of messages that have severity levels of warning, error, and critical. In this instance, the entry is:

56 255

Where:

56 = severity= the sum of warning, error, and critical (8 + 16 + 32)
255 = type = the sum of all types (1 + 2 + 4 + 8 + 16 + 32 + 64 +128)

The following is an example of a 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 meaning of each field is as follows (left to right):

severity = 16 (Error)
type = 4 (Backup)
jobid = 10797
job group ID = 1
server = cacao
client = bush
process = nbpem
text = backup of client bush, which exited with status 71
Troubleshooting the Administration Console for UNIX

Most errors in the NetBackup Administration Console for UNIX appear in the following: an attention dialog box or in an error message pane in the lower right area of the console. If they appear elsewhere, they are Java exception errors, which are not documented in this guide. They may appear in the status line (bottom) of the NetBackup Administration window. They also may appear in the log file that contains the stdout or the stderr messages that Java APIs or the NetBackup Administration Console write.

The following are the four kinds of error messages that appear in the NetBackup Administration Console:

- **NetBackup status codes and messages.**
  See “About NetBackup status codes and messages” on page 153.
  See “About media and device management status codes and messages” on page 421.
  Operations performed in the 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 message in the alphabetical listing of the following topic
  See “NetBackup Messages” on page 397.
  Then use the status code to find the full description of the message in the first half of that chapter.

- **NetBackup Administration Console: application server status codes and messages.**
  See “About NetBackup status codes and messages” on page 153.
  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:.
  A status code does not always accompany the message (see note).

- **Java exceptions**
  Either the Java APIs or NetBackup Administration APIs generate these. These messages begin with the name of the exception. For example:

  `java.lang.ClassCastException`
Java exceptions usually appear in one of the following three places:

- In the status line (bottom) of the NetBackup Administration window
- In the log file generated by the jnbSA or jbpSA commands
- When it is set up, in the output file of the Windows Display Console .bat file. More information is available about detailed debug logging. See “Enabling detailed debug logging” on page 125.

Operating system errors

If messages appear that do not match those documented in this manual, they probably are errors in the operating system.

Required disk space for logging and temporary files

The Administration Console requires disk space in the following locations for successful operation:

- On the host that is specified in the login 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, reduced functionality, and unexpected error messages.

The following are some of the results you may receive:

- No response during login
- "Cannot connect" socket errors during login to the NBJava application server
- Reduced functionality in the NetBackup interface, for example, only the Backup, Archive, and Restore and Files System Analyzer nodes appear in the tree
- An error dialog box with the "Unable to login, status: 35 cannot make required directory" message
- An error dialog box with "/bin/sh: null: not found (1) "message
- Empty warning dialog boxes
An error dialog box with the message "An exception occurred: vrts.nbu.admin.bpmgmt.CommandOutputException: Invalid or unexpected class configuration data: <the rest of the message will vary>"

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 login request from the login 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 and the user service is the bpjava-susvc or bpjava-usvc application.

To enable detailed debug logging

1. On the NetBackup client or server that is specified in the login dialog box, create the following: bpjava-msvc, bpjava-susvc (if a NetBackup server), and bpjava-usvc (if a NetBackup client) debug log directories in the /usr/openv/netbackup/logs directory (UNIX) or in install_path\NetBackup\logs (Windows). For more information on debug logs, see the following:

   See “Debug logs on servers” on page 83.

2. On the UNIX machine where you run the jnbSA or jbpSA commands, add the following line to the Debug.properties file in the /usr/openv/java directory.

   debugMask=2

   The log file name is displayed in the xterm window where you ran the jnbSA or jbpSA commands.
If you use the NetBackup Java Windows Display Console, add the following line to the Debug.properties file in the NetBackup Java installed folder (for example, C:\install_path\VERITAS\java):

debugMask=2

If you use the Windows Display Console on a host where NetBackup is not installed, you have to do the following: edit the nbjava.bat file located in the NetBackup Java-installed folder to redirect output to a file. See the nbjava.bat file for details.

**Query string overview**

Following are details on the -w (- where) **QueryString** option on the vxlogview command for unified logging.

Query string is a text expression similar to a database WHERE clause that 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 the logical operators such as AND and OR.

**Query String Syntax**

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

**Data types for fields**

Table 3-8 shows data types for fields with a description and an example.
<table>
<thead>
<tr>
<th>Field name</th>
<th>Type</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRODID or prodid</td>
<td>Integer or string</td>
<td>Provide the product ID or the abbreviated name of product.</td>
<td>PRODID = 100 or PRODID = 'NBU'</td>
</tr>
<tr>
<td>ORGID or orgid</td>
<td>Integer or string</td>
<td>Provide the originator ID or the abbreviated name of the component.</td>
<td>ORGID = 1 or ORGID = 'VxAM'</td>
</tr>
<tr>
<td>PID or pid</td>
<td>Long Integer</td>
<td>Provide the process ID</td>
<td>PID = 1234567</td>
</tr>
<tr>
<td>TID or tid</td>
<td>Long Integer</td>
<td>Provide the thread ID</td>
<td>TID = 2874950</td>
</tr>
<tr>
<td>STDATET or stdate</td>
<td>Long Integer or string</td>
<td>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'</td>
<td>STDATET = 98736352 or STDATET = '4/26/04 11:01:00 AM'</td>
</tr>
<tr>
<td>ENDATE or stdate</td>
<td>Long Integer or string</td>
<td>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'</td>
<td>ENDATE = 99736352 or ENDATE = '04/27/04 10:01:00 AM'</td>
</tr>
<tr>
<td>PREVTIME or prevtime</td>
<td>String</td>
<td>Provide the hours in 'hh:mm:ss' format. This field should be used only with operators =, &lt;, &gt;, &gt;= and &lt;=</td>
<td>PREVTIME = '2:34:00'</td>
</tr>
<tr>
<td>SEV or sev</td>
<td>Integer</td>
<td>Provide one of the following possible severity types:</td>
<td>SEV = 0 or SEV = INFO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- INFO or info</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- WARNING or warning</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ERR or err</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CRIT or crit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- EMERG or emerg</td>
<td></td>
</tr>
</tbody>
</table>
### Table 3-8 Data types (continued)

<table>
<thead>
<tr>
<th>Field name</th>
<th>Type</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSGTYPE or msgtype</td>
<td>Integer</td>
<td>Provide one of the following possible message types:</td>
<td>MSGTYPE = 1 or MSGTYPE = DIAG</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ DEBUG or debug - debug messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ DIAG or diag - diagnostic messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ APP or app - application messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ CTX or ctx - context messages.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ AUDIT or audit - audit messages</td>
<td></td>
</tr>
<tr>
<td>CTX or ctx</td>
<td>Integer or string</td>
<td>Provide the context token as string identifier or 'ALL' to get all the</td>
<td>CTX = 78 or CTX = 'ALL'</td>
</tr>
<tr>
<td></td>
<td></td>
<td>context instances to be displayed. This field should be used only with</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the operators = and !=.</td>
<td></td>
</tr>
</tbody>
</table>

### String constants

String constants should be given in single quotes. For example, prodid = 'NBU'

Start and end date can be provided as follows: either as a string constant of the regional display short date format or a long value of number of seconds that elapsed since midnight January 1, 1970.

### Query string examples

The following are some query string examples:

1. (PRODID == 100) && ((PID == 178964) || ((STDATE == '2/5/09 00:00:00 AM') && (ENDATE == '2/5/03 12:00:00 PM')))

2. ((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')))

3. (STDATE <= '04/05/09 0:0:0 AM') - This query will retrieve log messages, which are logged on or before 2009-05-04 for all the installed Symantec products.
Using NetBackup utilities

This chapter includes the following topics:

- About using NetBackup utilities
- Analysis utilities for NetBackup debug logs
- Network troubleshooting utilities
- NetBackup support utility (nbsu)
- NetBackup consistency check (NBCC)
- NetBackup consistency check repair (NBCCR)
- The nbcplogs utility

About using NetBackup 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.

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. A description of the two kinds of logging that are used, legacy logging and unified logging, is available.

See “About using logs and reports” on page 79.
To trace a NetBackup job requires that you 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.

The available utilities are as follows:

- **backuptrace** copies to standard output the debug log lines relevant to the specified backup jobs, including online (hot) catalog backups
- **restoretrace** copies to standard output the debug log lines relevant to the specified restore jobs
- **bpgetdebuglog** is a helper program for **backuptrace** and **restoretrace**
- **duplicatetrace** consolidates the debug logs for the specified NetBackup duplicate jobs and writes them to standard output.
- **importtrace** consolidates the debug log messages for the specified NetBackup import jobs and writes them to standard output.
- **verifytrace** consolidates the debug log messages for the specified verify job(s) and writes them to standard output.

### Installation requirements

The log analysis utilities are available for all platforms that are supported for NetBackup servers.

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

### Output format

The format of an output line is as follows:

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

The following is a short description of each part of the outline line format:

- **daystamp** The day of the log in yyyymmdd format.
- **millisecs** The number of milliseconds since midnight on the local machine.
- **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.

Limitations

While the log analysis utilities cover a variety of logs, the following exceptions occur:

- Media and device management logs are not analyzed.
- The legacy debug log files must be in standard locations on the servers and clients.
  
  /usr/openv/netbackup/logs/<PROGRAM_NAME>/log.mmddyy on UNIX and  
  <install_path>/NetBackup/Logs/<PROGRAM_NAME>/mmddyy.log on Windows. 
  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 time stamps outside the duration of the job from the following: bprd, nb pem, nbj m, nbrb, bp dbm, bp brm, bptm, bp dm, and bpcd.

How to run the log analysis utilities

This section describes each utility and the conditions for using it. For each command’s parameters, limitations, and examples of use, use the command with the `-help` option. All the following commands require administrative privileges.

See the *NetBackup Commands* manual.

**Table 4-1** is a description of each log analysis utility.
### Table 4-1 Log analysis utilities

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backuptrace</td>
<td>The <code>backuptrace</code> 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. <code>backuptrace</code> 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 <code>grep</code> by time stamp, program name, and server or client name. The <code>backuptrace</code> utility works with the nbpem, nbjm, and nbrb logs on the master server. You should enable debug logging for <code>bpbrm</code> and <code>bptm</code> or <code>bpdm</code> on the media server and for <code>bpbkar</code> on the client. For best results, set the verbose logging level to 5. Enable debug logging for the following: <code>bpdbm</code> and <code>bprd</code> on the master server and for <code>bpcd</code> on all servers and clients in addition to the processes already identified.</td>
</tr>
<tr>
<td>restoretrace</td>
<td><code>restoretrace</code> 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. <code>restoretrace</code> 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 <code>grep</code> by time stamp, program name, and server or client name. At a minimum, you must enable debug logging for <code>bprd</code> on the master server. Enable debug logging for <code>bpbrm</code> and <code>bptm</code> or <code>bpdm</code> on the media server and for <code>tar</code> on the client. For best results, set the verbose logging level to 5. Enable debug logging for <code>bpdbm</code> on the master server and for <code>bpcd</code> on all servers and clients.</td>
</tr>
<tr>
<td>bpgetdebuglog</td>
<td><code>bpgetdebuglog</code> is a helper program for <code>backuptrace</code> and <code>restoretrace</code>. It can also be useful as a stand-alone program and is available for all NetBackup server platforms. <code>bpgetdebuglog</code> prints to standard output the contents of a specified debug log file. If only the remote machine parameter is specified, <code>bpgetdebuglog</code> prints the following to standard output: the number of seconds of clock drift between the local machine and the remote machine.</td>
</tr>
</tbody>
</table>
Table 4-1  Log analysis utilities (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backupdbtrace</td>
<td>The <code>backupdbtrace</code> command consolidates the debug log messages for specified NetBackup database backup jobs and writes them to standard output. It sorts the messages by time. The command attempts to compensate for time zone changes and clock drift between remote servers and clients. At a minimum, you must enable debug logging for <code>admin</code> on the master server, and for <code>bptm</code> and <code>bpbkar</code> on the media server. For best results, set the verbose logging level to 5 and enable debug logging for the following: <code>bpdbm</code> on the master server and <code>bpcd</code> on all servers in addition to the processes already identified.</td>
</tr>
<tr>
<td>duplicatetrace</td>
<td>The <code>duplicatetrace</code> command consolidates the debug log messages for specified NetBackup duplicate jobs and writes them to standard output. It sorts the messages by time. The command attempts to compensate for time zone changes and clock drift between remote servers and clients. At a minimum, you must enable debug logging for <code>admin</code> on the master server and for <code>bptm</code> or <code>bpdm</code> on the media server. For best results, set the verbose logging level to 5 and enable debug logging for the following: <code>bpdbm</code> on the master server and <code>bpcd</code> on all servers and clients in addition to the processes already identified.</td>
</tr>
<tr>
<td>importtrace</td>
<td>The <code>importtrace</code> command consolidates the debug log messages for specified NetBackup import jobs and writes them to standard output. It sorts the messages by time. The command attempts to compensate for time zone changes and clock drift between remote servers and clients. At a minimum, you must enable debug logging for <code>admin</code> on the master server, and for <code>bpbrm</code>, <code>bptm</code> and <code>tar</code> on the media server. For best results, set the verbose logging level to 5 and enable debug logging for the following: <code>bpdbm</code> on the master server and <code>bpcd</code> on all servers and clients in addition to the processes already identified.</td>
</tr>
</tbody>
</table>
verifytrace consolidates the debug log messages for the specified verify job[s] and writes them to standard output. It sorts the messages by time. verifytrace 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 bpcm) 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.

Network troubleshooting utilities

A set of utility programs (commands) verifies various aspects of 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 two 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 including bptestcd and bptestnetconn verifies the NetBackup level settings. These settings include CONNECT_OPTIONS and CORBA endpoint selection.

<table>
<thead>
<tr>
<th>Table 4-2</th>
<th>Network configuration utilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>bptestnetconn</td>
<td>The bptestnetconn command performs several tasks that aid in the analysis of DNS and connectivity problems with any specified list of hosts, including the server list in the NetBackup configuration. To help troubleshoot connectivity problems between services that use CORBA communications, bptestnetconn can perform and report on CORBA connections to named services.</td>
</tr>
<tr>
<td>bptestbpcd</td>
<td>The bptestbpcd command 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.</td>
</tr>
</tbody>
</table>
Table 4-2  Network configuration utilities (continued)

| nbdna  | Network connectivity evaluation in a NetBackup domain is difficult because NetBackup domains can scale to hundreds of servers, and thousands of clients across complex network topologies. The NetBackup Domain Network Analyzer (nbdna) evaluates hostnames in the NetBackup Domain. The nbdna utility self-discovers the NetBackup domain and evaluates hostname information, then tests connectivity to these hostnames and validates their network relationship status. |

For more information on these utilities, refer to the *Commands* manual.

**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.

nbsu resides in the following location:
- On UNIX: `/usr/openv/netbackup/bin/support/nbsu`
- On Windows: `install_path\NetBackup\bin\support\nbsu.exe`

For a description of the nbsu command options, refer to the nbsu man page. More information is available.

See the *NetBackup Commands* manual.

**When to use nbsu**

&CompanyName; recommends that you run 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 &CompanyName; support.
nbsu progress display

By default, nbsu displays its progress to standard output. First it lists environment queries; then it lists the diagnostic commands that it runs.

Example nbsu output:

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\n
   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...

**nbsu output**

nbsu writes the information it gathers to text files in the following directory:

On UNIX:

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

On 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.

**Output files: format**

Each output file begins with a header that identifies the command(s) 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 4-1 shows the actual command(s) and output follow the header.

**Figure 4-1** 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 4-2 shows an example of part of the nbsu output file for the bpgetconfig command.

**Figure 4-2** 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)
```

**Output files: archiving and compression**

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:
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. &Company_Name; 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.

### Archiving by means of nbsu -xml

If no archive utility is installed on your system, do the following: use the -xml option of the nbsu command to 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 &Company_Name; support.

### nbsu and NetBackup status codes

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.

The commands that nbsu runs may be mentioned under "Recommended Actions" for a particular status code in either of the following: See “About NetBackup status codes and messages” on page 153.

See “About media and device management status codes and messages” on page 421.

For example, 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.

A description of the output files that nbsu generates is available.

See “Output files: format” on page 137.
To determine what information nbsu can collect for a particular status code, run nbsu with the -l option:

```
nbsu -l -nbu_e 25
```

**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.

### Notes on running nbsu

The following are items that can help you run the nbsu utility:

- For an nbsu description, examples, and how to gather diagnostic information to send to &CompanyName; support, refer to the nbsu command. See the *NetBackup Commands* manual.

- 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. `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.
  
  For a full description of the `-nbu_down` command line option, see the *NetBackup Commands* manual.

### If you encounter problems running nbsu

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:
    
    ```
    On UNIX: /usr/openv/netbackup/bin/support/nbsu 2>&1
    On Windows: install_path\NetBackup\bin\support\nbsu.exe 2>&1
    ```

  - To send all nbsu screen output including error messages to a file, enter:
    
    ```
    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 debug messages that relate to nbsu, enter:
  ```
  # nbsu -debug
  ```
  The messages are written to the `nbsu_info.txt` file. Information is available about the location of this file. See “nbsu output” on page 137.

### nbsu_info.txt file

The `nbsu_info.txt` file provides an overview of the environment where nbsu is run, and 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

This information 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, do the following: run nbsu with the `-debug` option to include additional debug messages in the `nbsu_info.txt` file.

### NetBackup consistency check (NBCC)

NBCC is a command line utility that is used to analyze the integrity of portions of the NetBackup configuration and catalog/database information as they pertain to tape media. This analysis includes review of NetBackup storage units, the EMM server, volume pools, tape media, and backup images associated with tape media.

NBCC does the following:

- Queries the operating system for configured Host Services and creates/reads the `nbcc-server-aliases` file for hostname normalization
- Through examination of the NetBackup configuration, identifies potentially tape based NetBackup media servers
- Gathers database/catalog information
- Analyzes the consistency of the gathered configuration and database/catalog information
- Creates a packaged bundle for &CompanyName; Technical Support review

NBCC resides in the following location:

- On UNIX: /usr/openv/netbackup/bin/support/NBCC
- On Windows: \install_path\NetBackup\bin\support\NBCC.exe

For a description of the NBCC command options, refer to the NBCC man page. More information is available.

See the NetBackup Commands manual.

When to use NBCC

&CompanyName; recommends that you run NBCC in the following circumstances:

- To check the consistency of the NetBackup configuration and catalog/database information from a tape media perspective
- To gather and create a package bundle when directed to do so by &CompanyName; Technical Support

NBCC progress display

By default, NBCC displays its progress numerically to standard output.

Example NBCC output that has been edited for brevity:

1.0 Gathering initial NBCC information
1.1 Querying configured network interfaces
1.2 Building hostname services information
   ...
1.3 Obtaining initial NetBackup configuration information
   ...
   If NBCC DOES NOT detect any catalog inconsistencies, would you like NBCC to create a support package? [Y/y,N/n] Y

2.0 Gathering required NetBackup configuration information

   Is the master server or any media server in a fail-over cluster? [Y/y,N/n] N

   Would you like NBCC to update the
   D:\Program Files\VERITAS\NetBackup\bin\support\config\nbcc-server-aliases file with additional hostnames and/or IP addresses that are detected during processing? [Y/y,N/n] Y
Would you like to verify each addition prior to the update? [Y/y,N/n] N

If NBCC is unable to determine the NetBackup version for ANY detected media server, is there a SINGLE version of NetBackup you would like associated to these media servers? [Y/y,N/n] Y

Please enter the NetBackup primary version number [3,4,5,6] 6

2.1 Reading the initial list of IP addresses and associated hostnames from the D:\Program Files\VERITAS\NetBackup\bin\support\config\nbcc-server-aliases file

2.2 Verifying the IP addresses and hostnames contained in the D:\Program Files\VERITAS\NetBackup\bin\support\config\nbcc-server-aliases file

2.3 Pinging primary hostnames...

2.4 Building NetBackup retention level list...

2.5 Building NetBackup storage unit list...

2.6 Obtaining EMM server names...

2.7 Obtaining tpconfig NDMP configuration information...
   The following NDMP Attach hosts were detected in EMM, but are not active in EMM:

2.8 Obtaining NetBackup unrestricted media sharing status...
   Configuration state = NO

2.9 Obtaining NetBackup Media Server Groups...
   No Server Groups configured

3.0 Gathering required NetBackup catalog information
   Start time = 2009-01-14 12:20:59

3.1 Gathering NetBackup EMM conflict table list
   Found 0 EMM conflict records

3.2 Building NetBackup Image database contents list
   ... Found 5890 images in the Image database

3.3 Obtaining NetBackup version from media servers
3.4 Building EMM database Media and Device configuration attribute lists
... Found 212 media records in the EMM database
3.5 Building EMM database Unrestricted Sharing Media attribute lists
 Found 0 Unrestricted Sharing media records in the EMM database
3.6 Building the EMM database Volume attribute list...
 Getting the EMM database Volume attributes from EMM server master1 ...
 Found 586 Volume attribute records in the EMM database
3.7 Building NetBackup volume pool configuration list
 Server master1
3.8 Building NetBackup scratch pool configuration list
 Server master1
3.9 Gathering NetBackup EMM merge table list
 Found 0 EMM merge table records

Summary of gathered NetBackup catalog information
...
 Catalog data gathering took 499 seconds to complete

***WARNING***
** It took more than 60 seconds to collect all of the DB data.
**
** If backups are running, there is a risk that the data collected
** might not be consistent, because the DBs may have been updated
** while the data was being collected.
**
** If backups are running and it is possible, please stop all
** backups and run NBCC again.
**
** If it is not possible to stop all backups, just let
** NBCC complete.
...

4.0 Verifying required catalog components were gathered

5.0 Beginning NetBackup catalog consistency check
 Start time = 2009-01-14 12:29:19

5.2 Processing EMM database Volume attribute records, pass 1 (of 2), 586 records to be processed
 Processed 586 EMM database Volume attribute records.
5.3 Checking for duplicate EMM server host names in Volume attribute data

5.4 Processing Image DB, pass 1 (of 2), 5890 to be processed
5890 images processed on pass 1

5.5 Processing EMM database Media attribute records, pass 1 (of 3),
212 records to be processed
Processed 212 EMM database Media attribute records.

5.7 Check for duplicate media server names in the EMM database Media attribute data

5.8 Processing EMM database Media attribute records, pass 2 (of 3),
212 records to be processed

CONSISTENCY_ERROR Oper_16_4

5.9 NetBackup catalog consistency check completed
End time = 2009-01-14 12:29:21

6.1 Processing detected NetBackup server entries
Summary of NBCC server processing...

Report complete, closing the
./output/nbcc/master2_NBCC_20090114_121931\nbcc-info.txt output file.

Server aliases file

NBCC generates the nbcc-server-aliases file that contains IP addresses and the related primary and associated alias hostnames. The nbcc-server-aliases file is created in the following directory.

On UNIX and Linux:

/usr/openv/netbackup/bin/support/config/

On Windows:

install_path\NetBackup\bin\support\config\n
The following example shows a sample server alias file listing.

# This file is used by NBCC as a basis for determining primary and
# associated alias hostnames as described in the NBCC -help output.
#
# List the primary IP address, all secondary IP addresses, the primary
# hostname and all aliases used for the same server by NetBackup in
# bpgetconfig SERVER related entries, storage units and Volume database
# hosts (eg, fully-qualified hostnames, hostnames associated with other
# network interfaces on the server, cluster node names) on a single line.
#
#
# Note: Any hostnames that contain upper-case characters are converted
to lower-case characters by NBCC for processing.
#
# Accurate representation of both primary and secondary IP addresses and
primary and associated hostnames are important for both the gathering
and consistency checking of the NetBackup catalog data.
#
# Format of entries in the "nbcc-server-aliases" file:
#
#   primary_IP [ secondary_IP ... ] primary_name alias [ alias ... ]
#
# Examples:
#
#   #.##.###.### #.##.###.## nbserver NBserver nbserver.lab.symantec.com
#   #.##.###.### #.##.###.## nbmaster-bkup nbmaster zeus zeus-bkup
#
# Any entries that are added to this file must NOT start with a '#'.
#
# All lines starting with a '#' are ignored by NBCC.
#
# Empty lines are ignored by NBCC.
#
10.10.100.10 nbu_server.com nbu_server
10.10.111.10 nbu_server1.com nbu_server1
10.10.112.10 nbu_server2.com nbu_server2

**NBCC output**

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

On UNIX and Linux:

```
/usr/openv/netbackup/bin/support/output/nbcc/hostname_NBCC_timestamp
```

On Windows:

```
install_path\NetBackup\bin\support\output\nbcc\hostname_NBCC_timestamp
```

**Output files: archiving and compression**

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.

**Notes on running NBCC**

The following are items that can help you run the NBCC utility:

- For an NBCC description, examples, and how to gather NetBackup catalog/database information to send to &Company Name; support, refer to the NBCC -help command, or do the following:
  See the *NetBackup Commands* manual.

- 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 it is going to process to STDOUT. As NBCC processes catalog/database components, it displays how many records have been processed. The number of records processed is in direct relationship to the size of the catalog/database being processed. If NBCC detects a failure, related information will be output to STDERR. Information to STDOUT or STDERR are also output to the nbcc-info.txt file (if available).

**If you encounter problems running NBCC**

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.

**nbcc-info.txt file**

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 was displayed to STDOUT or STDERR.

This information would indicate the processing that NBCC had done.

The “Processing detected NetBackup server entries” section of the *nbcc-info.txt* file contains a “Summary of NBCC server processing”. This information summarizes the results of the processing of detected server entries.

The following example show a successful summary of server processing from the *nbcc-info.txt* file.

```
+ Primary and associated alias hostnames: +
+ server_1 +
+ Primary and associated IP addresses: +
+ 100.100.10.1 +
+ Sources: +
+ config_file bpstulist nbemmcmd +
+ MediaDB host = up VolDB host = no Disk STU host = no +
+ Member of Server Group = no +
+ Media server NetBackup version = 6.5 +
+ Primary hostname ping results: +
+ Successful +
```

The following example shows a failed summary of server processing from the *nbcc-info.txt* file.

```
- Primary and associated alias hostnames: -
- server_2 -
- Primary and associated IP addresses: -
- 100.100.10.100 -
```
- Sources: +
  - config_file nbemncmd +
  - MediaDB host = down VolDB host = no Disk STU host = no +
  - Member of Server Group = no +
  - Media server NetBackup version = 6.X +
  - Primary hostname ping results: +
  - Failed - No IP address detected +

---

**NetBackup consistency check repair (NBCCR)**

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. &Company Name; Tech Support analyzes data 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, Tech 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 paired with an associated parameter.

The NBCCR utility executes each repair action in several stages:

- **Data collection.** NBCCR first collects information required to perform a repair.

- **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.

- **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. It implements the repairs with proven syntax, so ad hoc scripting occurs. 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:

- **On UNIX:** /usr/openv/netbackup/bin/support/NBCCR
- **On Windows:** install_path\NetBackup\bin\support\NBCCR.exe

For a description of the NBCCR command options, refer to the NBCCR man page. More information is available.

See the *NetBackup Commands* manual.
NBCCR files

NBCCR accepts one input file and creates two output files.

- NBCCR accepts as input the Suggested Repair Action (SRA) file named NBCCA.SRA.txt. The file resides in the same directory as the utility.
- NBCCR creates NBCCR.History.txt, a history file of all the repair actions attempted, and places it in the same directory as the utility.
- It also creates an output file, NBCCR.output.txt. See the two sample output files that follow.

While the NBCCR utility runs, the following file appears in the same location as the NBCCR utility:

KeepOnTruckin.txt

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.

Sample output files

The following are two sample contents of the NBCCR.output.txt file showing 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.

This sample shows that all images were found 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
```

The following sample show an unsuccessful repair action. NBCCR did not find one or more images on the tape, so the repair action is not performed.

```
MContents for ULT000 MediaServerExpireImagesNotOnTapeFlag
   ExpireImagesNotOnTape flag not set
   Did NOT find Backup ID winmaster_1234315163 Copy 1 AssignTime 2009-02-11 01:19:13 (1234315153) on ULT000
   Leaving winmaster_1234315163 Copy 1 on ULT000 in ImageDB
   ULT000 MContents - One or more images from images catalog NOT found on tape
   MContents ULT000 status: ActionFailed
```
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 &CompanyName; support can be difficult and time consuming.

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.

More information on the nbcplogs utility is available in the Commands manual.
Using NetBackup utilities

The nbcplogs utility
NetBackup status codes and messages

This chapter includes the following topics:

■ About NetBackup status codes and messages

About NetBackup status codes and messages

This chapter lists all the status codes and messages that NetBackup provides. Codes that relate to Media and device management are available.

See “Media and device management messages” on page 549.

This chapter is divided into two parts:

■ The first section lists the NetBackup status codes in numerical order and includes an explanation of what occurred along with recommended actions. See “NetBackup status codes” on page 154.

■ The second section lists the same status codes but sorts them alphabetically according to the message. See “NetBackup Messages” on page 397.

If you see a status code without its associated message text, use the `bperror` command to determine the message, its explanation, and recommended action.

On UNIX and Linux systems:

```
/usr/openv/netbackup/bin/admincmd/bperror -statuscode nstatuscode [-recommendation]
```

On Windows systems:
install_path\NetBackup\bin\admincmd\bperror -statuscode

where \texttt{statuscode} is the number of the message.

The following example shows how you use \texttt{bperror} to access error code information:

\textbf{On UNIX and Linux:} /usr/openv/netbackup/bin/admincmd/bperror -statuscode 150

\textbf{On Windows:} install_path\NetBackup\bin\admincmd\bperror -statuscode 150

\texttt{termination requested by administrator}

The process is terminating (or has terminated) as a direct result of a request from an authorized user or process.

The &\textit{Company Name}; Technical Support site has a wealth of information that can help you solve NetBackup problems. See the following site for comprehensive troubleshooting details:

\url{www.symantec.com/business/support/}

\section*{NetBackup status codes}

The following is a complete list of the NetBackup status codes that are listed in numerical order:

\begin{center}
\begin{tabular}{l}
\textbf{NetBackup status code: 0} \\
\textbf{Message:} the requested operation was successfully completed \\
\textbf{Explanation:} No problems were detected with the requested operation.
\end{tabular}
\end{center}

\begin{center}
\begin{tabular}{l}
\textbf{Recommended Action:} No action is needed, unless a database was backed up through a database extension product (for example, NetBackup for Oracle or NetBackup for SQL Server). In those instances, code 0 means the backup script (that started the backup) ran without error. However, you must check other status as explained in the related NetBackup manual to see if the database was successfully backed up.
\end{tabular}
\end{center}
NetBackup status code: 1

Message: the requested operation was partially successful

Explanation: A problem was detected that may require corrective action during the requested operation.

Recommended Action: Check the All Log Entries report and also the progress log (if there is one).

The following are some of the problems that can appear under status code 1:

- A file or a directory path is more than 1023 characters long.
  For NetBackup Snapshot Client, the maximum path name length is 1000 characters for snapshot backups, not 1023. When the snapshot is created, a new mount point is added to the beginning of the file path. If the new mount point plus the original file path exceeds 1023 characters, the backup fails with status code 1. The progress log includes the entry "ERR-Skipping long dir path."

- You cannot open a file.
  The file may have been locked for some reason.

- The following information applies only to UNIX and Linux systems:
  NetBackup cannot get the link name of a file.

- The following information applies only to UNIX and Linux systems:
  NetBackup cannot process a sparse file.

- A read error that was encountered in a file.

- File is of an unknown type, or may be hidden.

- The following information applies only to UNIX and Linux systems:
  The lstat system call fails on a file that is eligible to be backed up. This error may be a permission problem.

- The following information applies only to UNIX and Linux systems:
  A file cannot be locked that has mandatory locking enabled.

- A synthetic backup job may terminate with a status code 1 under the following conditions:
  - No images were found to synthesize (status code = 607).
  - TIR info has been pruned from component images (status code = 136).
  - Image format is unsupported (status code = 79).
The synthetic backup job logs the actual status code in the NetBackup error log. Refer to the documentation for the corresponding NetBackup error code for the corrective action to take.

■ A BMR job may terminate with status code 1 in the following situation:
  You save the BMR configuration and it returns an error even though the child jobs completed successfully. For information, examine the Detailed Status tab of the Job Details dialog box, or the `nbjm` unified log (originator ID 117).

■ A policy that contains multiple backup scripts starts a scheduled backup of a UNIX database extension client. If it fails with a status code 1, some of the backup scripts returned a failure status.

■ On clients using Windows Open File Backups (WOFB) to back up open or active files, the following may occur:
  Volume snapshots were not enabled successfully for the backup.
  The following logging messages should appear in the `bpbkar32` logs if volume snapshots were not successfully enabled.
  If multistreamed backup jobs are enabled, log messages similar to the following appear that indicate volume snapshots were not enabled for the multistreamed backup job:

```
11:05:44.601 AM: [1536.724] <4> tar_backup::V_AddToFI_XBSAObj: INF - Volume snapshots not enabled for: D:\Directory1
```

If multistreamed backups were not enabled, log messages similar to the following appear, which indicate volume snapshots were not enabled for the non-streamed backup job:

```
1:59:41.229 PM: [2076.2088] <4> V_Snapshot::V_Snapshot_CreateSnapshot: INF - Attempting to create snapshots for D:\Directory1
1:59:41.229 PM: [2076.2088] <4> V_Snapshot::V_Snapshot_CreateSnapshot: INF - CREATE request: \\
C:\Program Files\VERITAS\NetBackup\bin\bpfis create -fim VSP "D:\ Directory1"
1:59:41.799 PM: [2076.2088] <4> V_Snapshot::V_Snapshot_ParseBpfisOutput: INF - Snapshot creation, FIS_ID: 1058813981
1:59:41.799 PM: [2076.2088] <4> V_Snapshot::V_Snapshot_ParseBpfisOutput: INF - Snapshot creation EXECUTE
```

In this case, examine the bpfis logs for error messages regarding snapshot creation failures. More details are available on the bpfis logs. See the NetBackup Snapshot Client Administrator’s Guide.

In the bpfis logs, the following messages may appear when snapshot creation fails for Windows Open File Backup:

First message:

04:01:14.168 [376.2364] <32> onlfi_fi_split: VfMS error 11; see following messages:
04:01:14.168 [376.2364] <32> onlfi_fi_split: Fatal method error was reported
04:01:14.168 [376.2364] <32> onlfi_fi_split: VfMS method error 3; see following message:

Cause: VSP was not enabled because the VSP snapshot for the backup did not meet the specified minimum time in the Busy File Wait VSP setting. Either increase the Busy File Timeout VSP setting (recommended setting: 300 seconds or more) or submit the backup job when the volume has less activity.

Second message:

04:17:55.571 [1636.3224] <2> onlfi_vfms_logf: snapshot services: (null): There was an unexpected error while preparing the VSP snapshot transaction. Dumping the parameter array to provide more information: Error 112 from VSP_Prepare

Cause: VSP was not enabled for the backup because the client for the VSP Snapshot Cache files does not have enough free disk space. Free up disk space on the volumes being backed up.

Third message:

If Microsoft Volume Shadow Copy Service (VSS) is used as the Windows Open File Backup snapshot provider and snapshot creation fails, refer to the following: Event Viewer’s Application and System Logs for error information.
A snapshot error may have occurred. Also, you may have clients that use the Windows Open File Backup option to back up open or active files. In this case, a log message in the bpbkar32 debug log appears, which indicates that a snapshot error occurred.

The following is an example of a snapshot error:

8:51:14.569 AM: [1924.2304] <2> tar_base::V_vTarMsgW: ERR -  
Snapshot Error while reading test.file

See the recommended actions under status code 156.

The granular processing operation of an Exchange Granular backup job has failed to complete successfully. Check the bpbkar debug log for more information. A legacy (non-VSS) backup still truncates transaction logs if the job ends with status 1 because a granular processing operation failed. In this situation, the backup image is suitable for database recovery.

**NetBackup status code: 2**

**Message:** none of the requested files were backed up

**Explanation:** A backup or archive did not back up any of the files in the file list.

This status code applies primarily to automatic backups using Lotus Notes or SQL database agents, when all the backups that are job related have failed. Or, an Enterprise Vault backup has failed. It should not occur for standard file system backups.

Open a NetBackup support case (recommended in &CompanyName; document 276903.pdf) if you encounter this error for the following: a UNIX, Linux, or Windows file system backup, or for database agents other than SQL Server or Lotus Notes.

**Recommended Action:** Do the following, as appropriate:

- The following information applies only to Lotus Notes:
  This error occurs when archive style logging is not enabled for the Lotus Domino server on UNIX. It also occurs when another backup of the transaction logs is in progress.

- For troubleshooting guidance, such as a list of logs to gather, and for details on particular issues, refer to the &CompanyName; support document 276903.pdf.

- See the troubleshooting topic of the appropriate guide for a description of troubleshooting tools:
  - NetBackup for Microsoft SQL Server Administrator’s Guide
NetBackup status code: 3
Message: valid archive image produced, but no files deleted due to non-fatal problems
Explanation: The backup portion of the archive command reported problems so the files were not deleted.
Recommended Action: Examine the progress log or status of the archive on the client to determine if you need to retry the archive after correcting the problem. If the problem is not serious and the files were backed up, you can manually delete the files. To verify which files were backed up, use the NetBackup client-user interface in restore mode and browse the files in the archive.
A possible cause for files not being deleted is that you do not have the necessary permissions. NetBackup cannot delete files unless you are the user that owns the files, a superuser on UNIX, or an administrator on Windows.

NetBackup status code: 4
Message: archive file removal failed
Explanation: The backup portion of the archive completed was successful but the delete failed.
Recommended Action: Verify that you have permission to delete the files and that the read-only flag is not set for the files. On UNIX and Linux clients, verify that you have write permission to the directories that contain the files. Since the backup was successful, you can delete the files that were backed up. (If you do not have the necessary permissions, have the system administrator delete the files.)

NetBackup status code: 5
Message: the restore failed to recover the requested files
Explanation: Errors caused the restore to fail.
Recommended Action: Perform the following items in the order presented:
- Ensure that the client’s server list contains entries for the master server and any media servers that can be used during a backup or restore.
- Examine the status or the progress log on the client for messages on why the restore failed. Also, check the All Log Entries report on the server.
- Check ownership and permission on directories where files are restored.
Correct the problems that you find and retry the restore.

If you tried to restore files from a FlashBackup backup after a NetBackup patch was installed, the patch may not have been installed properly. Follow the installation instructions in the patch readme file and make sure the `libsfr.so` file is copied as instructed.

**NetBackup status code: 6**

**Message:** the backup failed to back up the requested files

**Explanation:** Errors caused the user backup to fail.

**Recommended Action:** Do the following as appropriate:

- Verify that you have read access to the files. Check the status or the progress log on the client for messages on why the backup failed. Correct problems and retry the backup.

- The following information applies only to Windows clients: Verify that the account used to start the NetBackup Client service has read access to the files.

- The following information applies only to Macintosh clients: This code can be due to multiple backups being tried simultaneously on the same client.
  
  Some possible solutions are as follows:

  - Adjust the backup schedules.

  - If the client is only in one policy, set the policy attribute, Limit jobs per policy, to 1.

  - Set the NetBackup global attribute, Maximum jobs per client, to 1 (note that this limits all clients in all policies).

- For a UNIX or Linux database extension client (for example, NetBackup for Oracle), this status code can indicate a problem with the script that controls the backup.

  Check the progress report on the client for a message such as `Script exited with status code = number` (the number varies). The progress log usually names the script.

  Check the script for problems. Also, check that the troubleshooting logs created by the database extension. See the NetBackup guide that came with the database extension for information on the scripts and the troubleshooting logs.
NetBackup status code: 7
Message: the archive failed to back up the requested files
Explanation: Errors caused the user archive to fail.
Recommended Action: Verify that you have read access to the files. Check the progress log or the status on the client for messages on why the archive failed. Correct problems and retry the archive.
On Windows clients, verify that the account used to start the NetBackup services has read access to the files.

NetBackup status code: 8
Message: unable to determine the status of rbak
Explanation: On DomainOS clients, rbak is used to do restores. If rbak does not exit with a status message, NetBackup cannot determine whether the restore worked or not.
Recommended Action: Check for a new core file to see if rbak quit abnormally. Check the ps output to see if rbak is hung. If so, cancel it and try again. Check the progress log for any unusual messages from rbak.

NetBackup status code: 9
Message: an extension package is needed, but was not installed
Explanation: A NetBackup extension product is required to perform the requested operation.
Recommended Action: Install the required extension product.

NetBackup status code: 10
Message: allocation failed
Explanation: The system memory allocation fails because of insufficient system memory available. A possible cause is that the system is overloaded with too many processes and not enough physical or virtual memory.
Recommended Action: Free up memory by terminating any unneeded processes that consume memory. Add more swap space or physical memory.

NetBackup status code: 11
Message: system call failed
**Explanation:** A system call has failed. This status code is used for a generic system call failure that does not have its own status code.

**Recommended Action:** Do the following, as appropriate:

- Check the All Log Entries and Problems reports to determine the system call that failed and other information about the error.

- `nbjm` and `nbproxy` return status code 11 when an exception is processed, such as when `nbproxy` obtains policy or configuration information. Examine the `nbjm` unified log (originator ID 117) or the `nbproxy` legacy log for more detail on the cause of the error.

- A frequent cause is that the server’s file system is full. For example, you may see a message similar to the following in the Problems report or `bpdbm debug` log:

  06/27/95 01:04:00 romb romb db_FLISTsend failed: system call failed (11)
  06/27/95 01:04:01 romb romb media manager terminated by parent process

  06/27/95 01:05:15 romb romb backup of client romb that exited with status 11 (system call failed)

  On UNIX and Linux systems, run a `df` command on the `/usr/openv/netbackup/db` directory.

  If the `df` command does not reveal the problem, check the `bpdbm debug` logs or do a `grep` for the message `system call failed` in relevant files under the directory `/usr/openv/netbackup/db/error/`

  On Windows systems, verify that the disk partition where NetBackup is installed has enough room.

- Verify that the system is not running out of virtual memory. If virtual memory is the problem, turn off unused applications or increase the amount of virtual memory.

  To increase virtual memory on Windows, do the following in the order presented:

  - Display the Control Panel.
  - Double-click **System**.
  - On the **Performance** tab, set Virtual Memory to a higher value.

  The following information applies only to UNIX and Linux clients:
Check for a semaphore problem. This error may occur because the system does not have enough allocated semaphores. It is most commonly seen on Solaris servers when an RDBMS is also running.

The symptoms of the problem vary. In some cases, error messages in the NetBackup log indicate a backup failure due to an error in semaphore operation. Another symptom is the inability of the NetBackup device manager daemon, ltid, to acquire a needed semaphore.

System requirements vary; thus, no definite recommendations can be made. One customer running NetBackup and ORACLE on a Solaris server made the following changes to the /etc/system file and then rebooted the system (boot -r). The changes were adequate.

```
set semsys:seminfo_semmni=300
set semsys:seminfo_semmns=300
set semsys:seminfo_semmsl=300
set semsys:seminfo_semmnu=600
```

Set these attributes to a value great enough to provide resources to all applications on your system.

- Examine other debug logs or the progress log or status on the client. Examine the nbjm unified log (originator ID 117) for more detail on the cause of the error.

**NetBackup status code: 12**

**Message:** file open failed

**Explanation:** An open of a file failed.

A disk storage unit tries to write to or create a directory on the root device of the NetBackup server or media server. In this case, the Activity Monitor job details log contains the message "not permitted to root device." By default the absolute path or specified directory for a disk storage unit cannot be on the root file system (or system disk). You must explicitly enable them to be there when the storage unit is created.

**Recommended Action:** Do the following as appropriate:

- If you want the path for the disk storage unit to reside in the root file system: Open the Change Storage Unit dialog box in the Administration Console and select the check box: "This directory can exist on the root file system or system disk."

- If the specified path for the disk storage unit is not in the root file system or system device, do the following: Verify that the path is in a mounted file system.
If the specified path for the disk storage unit is in the root file system or system device but does not need to be: Use the Change Storage Unit dialog box to specify a different (non-root) path in a mounted file system.

Check the NetBackup Problems report. Try to determine the file and why the error occurred. A possible cause is a permission problem with the file. For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then, retry the operation and check the resulting debug log.

For NetBackup Lotus Notes, point-in-time restore jobs may fail with a status 12. These jobs are initiated from the master server by using either the NetBackup Administration Console or the Backup, Archive, and Restore interface. Their failure is reported in the NetBackup tar log file. (For Windows, this file is located in the `install_path\NetBackup\logs\tar` folder. For UNIX and Linux, it is located in the `/usr/openv/netbackup/logs/tar` folder.) If the install path of the NetBackup master server is different from the install path of the NetBackup client, the following occurs: The automatic restore of Lotus transaction log extents during recovery of the Lotus database fail. Note that the Activity Monitor shows a status 0 (successful). The tar log on the client, however, shows success for the restore but a failure (status 12) for the Lotus database recovery.

Perform the restore job from the Backup, Archive, and Restore interface on the NetBackup client.

For NetBackup Snapshot Client, status code 12 may appear in the `/usr/openv/netbackup/logs/bptm` or `bpdm` log with the following:

```
tpc_read_config failed: cannot open file /usr/openv/volmgr/database/3pc.conf
```

This status code may indicate that the policy is configured with either of the following: The NetBackup media server or Third-Party Copy Device as the off-host backup method, but the `3pc` file does not exist or is in the wrong location.

Instructions are available on how to create the `3pc` file.
See the *NetBackup Snapshot Client Administrator’s Guide*.

For a FlashBackup policy, if the `CACHE=` entry follows the source data entry, the backup fails with status code 12. Messages such as the following appear in the `/usr/openv/netbackup/logs/bpbkar` logs on the client:

```
09:55:33.942 [6092] <32> bpfsmap: FTL - bpfsmap: can't open snapshot disk /dev/rdsk/c4t1d0s3 errno 0
```
Change the order of the backup selections list so that the CACHE entry precedes the source data entry. (The source data entry specifies the raw partition that contains the file system to be backed up.)

**NetBackup status code: 13**

**Message:** file read failed

**Explanation:** A read of a file or socket failed.

The possible causes include as follows:

- A network communication problem has occurred on the master server, media server, or one of the clients.
- An I/O error that occurred during a read from the file system.
- Read of an incomplete file or a corrupt file.
- A socket read failure that is caused by a network problem or a problem with the process that writes to the socket.
- A problem specific to NetBackup Snapshot Client (see recommended actions).
- The first EV-SQL backup after a NetBackup installation failed. See the Troubleshooting section of the *NetBackup for Enterprise Vault Agent Administrator’s Guide*.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for clues on where and why the problem occurred.
- Check that network communication works properly. See “Resolving network communication problems” on page 40.
- For a FlashBackup client, check the /var/adm/messages log for errors like the following:

```
Mar 24 01:35:58 bison unix: WARNING: sn_alloccache: cache /dev/rdsk/c0t2d0s3 full - all snaps using this cache are now unusable
```
This error indicates that the cache partition is not large enough. If possible, increase the size of the cache partition. Or, if multiple backups use the same cache, reduce the number of concurrent backups. To reduce the number, reschedule some of them or reschedule the entire backup to a time when the file system is less active.

- For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.
- Ensure that the latest service packs for all products and components (SQL, Exchange, Notes, etc.) have been installed.
- Ensure that all the network hardware (NICs, hubs, switches, routers, etc.) throughout the environment are set to full duplex, not half duplex.
- Check the following items regarding the NICs in your system:
  - Upgrade to the latest NIC drivers throughout the system.
  - Ensure that all NICs are set to full duplex, not half duplex. See “Backup performance and NIC cards” on page 71.
  - Increase the timeout settings on the NIC.
  - If NIC teaming is implemented, deactivate for testing purposes.
  - Replace the NIC itself on the affected client or server.
- For NetBackup Snapshot Client, status code 13 may appear in the /usr/openv/netbackup/logs/bpbkar log.

The log can indicate the following:

- The files to back up reside on an IDE drive as opposed to SCSI. The off-host backup method was set to either NetBackup media server or Third-Party Copy Device. If you use off-host backup, the disk that contains the client files must be a SCSI or Fibre Channel device.
  If the disk is an IDE drive, you may see the following in the /usr/openv/netbackup/logs/bpfis log:

```
get_disk_info: FTL - /var/tmp/caa026fEU disk_inquiry failed.
Errno = 25: Inappropriate ioctl for device
```

The following listing may appear in the
/usr/openv/netbackup/logs/bpbkar log:

```
bpbkar: INF - Processing /var
bpbkar: ERR - get_disk_info() failed, status 13
bpbkar: ERR - tpc_get_disk_info() failed: err 13
```
The files to back up exist on a file system that is not mounted. The file system that is specified as the snapshot source must be mounted. If the snapshot source is not mounted but the mount point is present, NetBackup may do the following: Try to take a snapshot of the directory preceding the directory that was specified as the snapshot source.

For the NetBackup media server method, you may need to increase the client read timeout value. In some environments, NetBackup may require more read time than the default value allows. If the client read timeout is insufficient, the backup may fail, which causes this error.

To increase the client read timeout for all clients, do the following: In the NetBackup Administration Console, go to **Host Properties > Master Servers** > double-click the master server, then go to **Properties > Timeouts**. Then increase the client read timeout.

**NetBackup status code: 14**

**Message:** file write failed

**Explanation:** A write to a file or socket failed.

Possible causes include the following:

- An I/O error that occurred during a write to the file system.
- Write to a socket failed. Cause of this failure: A network problem or a problem with the process that reads from the socket.
- Writing to a full disk partition.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for clues on where and why the problem occurred.
- For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.
- Make sure that routers, bridges, and other network devices are all at "full" duplex.
  See “Backup performance and NIC cards” on page 71.
- Use a "sniffer" program to determine the number of packets being rejected or re-requested.
On Windows systems, the client bpbkar log may contain a 10054 "Connection Reset Error" error (usually indicates a hardware error). Somewhere between the NetBackup client and server, the connection was reset. When NetBackup receives this error, it cannot continue the backup. This error has been attributed to the following:

- A hiccup in the network.
- A bad network interface card on a NetBackup client.
- A bad network interface card on the NetBackup server.
- Faulty routers.
- Any other applications that interfere with NetBackup connections.

On Novell systems, status code 14 has also been attributed to network issues. Try a "sniffer" program.

The error occurs while you use the NetBackup-Java interface: The application server (bpjava processes) for the NetBackup-Java interface probably ran out of disk space in the file system containing /usr/openv/netbackup/logs/user_ops. The application server writes temporary files into directories in the /user_ops directory. Try clearing up disk space in the file system.

**NetBackup status code: 15**

Message: file close failed

Explanation: A close of a file or socket failed.

Recommended Action: Check the NetBackup Problems report for clues on where and why the problem occurred. For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.

**NetBackup status code: 16**

Message: unimplemented feature

Explanation: The specified operation is not implemented. This error should not occur through normal use of NetBackup.

Recommended Action: Save all error information and call customer support.

**NetBackup status code: 17**

Message: pipe open failed
**Explanation:** Occurs in NetBackup client menu and Vault areas.

**Recommended Action:** Save all error information and call customer support.

**NetBackup status code: 18**

**Message:** pipe close failed

**Explanation:** A pipe close failed when one process tries to start a child process.

**Recommended Action:** Check the NetBackup Problems report for clues on why the failure occurred. For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.

**NetBackup status code: 19**

**Message:** getservbyname failed

**Explanation:** A call to `getservbyname()` failed. The `getservbyname()` function uses the name of the service to find a service entry in the `services` file. (Or NIS services map on UNIX and Linux if it is configured.)

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for clues on why the failure occurred.
- On a UNIX or Linux system, check that `/etc/services` and NIS services map (if applicable) have entries for the NetBackup services: `bpcd`, `bpdbm`, and `bprd`.
- On a Windows system, verify that the `%SystemRoot%\system32\drivers\etc\services` file shows the correct entries for the NetBackup Internet processes: `bpcd`, `bpdbm`, and `bprd`. Ensure that the following numbers match the settings in the `services` file: The NetBackup Client Service Port number and NetBackup Request Service Port number on the Network tab in the NetBackup Client Properties dialog box. To display this dialog box, start the Backup, Archive, and Restore interface and click **NetBackup Client Properties** on the **File** menu. The values on the **Network** tab are written to the `services` file when the NetBackup Client service starts. See “Verifying host name and service entries” on page 48.
- Check the level of network activity. An overloaded network can cause this error.
- If these actions do not reveal the problem, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.
NetBackup status code: 20

Message: invalid command parameter

Explanation: One or more command parameters were not valid. This error can occur when incompatible levels of NetBackup are installed on a master and its media server(s) or client(s). For example, a NetBackup master server has NetBackup 7.0 and the media server or the client has NetBackup 6.0.

This error can also occur if the wrong parameters are used when you run a command line.

Recommended Action: Do the following, as appropriate:

- Check the NetBackup Problems report for clues.
- If the error occurs when you run a command on the command line, verify that the parameters are valid.
- This status code may occur if nbjm passes parameters but does not have a required parameter. Check the nbjm unified logs (originator ID 117) for the list of parameters that were passed.
- The following information pertains to NetBackup Snapshot Client.
  - If the following appears in the /usr/openv/netbackup/logs/bptm log as enabled on a third-party copy backup, multiplexing was enabled on a third-party copy backup:

    bptm: cannot perform Third-Party-Copy for multiplexed backups
    send_brn_msg: ERROR 20
    bptm: EXITING with status 20
    The Third-Party Copy Device off-host backup method is incompatible with multiplexing (the writing of two or more concurrent backup jobs to the same storage device). You must disable multiplexing for any third-party copy backups. If multiplexing is enabled, the backup fails.
  - The media server may not have the correct 3pc. file entry for the client disk that is needed for the backup.
    The following appears in the /usr/openv/netbackup/logs/bpbkar log:

    14:45:00.983 [15773] <4> bmap_mm_get_devid: GET_DEVICE_INDEX 1
    EMC:SYMMETRIX:601092014000
    14:45:00.986 [15773] <4> bpbkar child_send_keepalives: keepalive child started, pid = 15822
    14:47:02.029 [15773] <4> bmap_mm_get_devid: keepalive child: 15822 killed
    14:47:02.030 [15773] <4> bmap_mm_get_devid: DEVICE_INDEX -1
This shows that a particular device cannot be found in the 3pc. file on the media server (14:47:02.031 [15773] <16> bpmap_send_extend: ERR - can't obtain device id string EMC:SYMMETRIX:601092014000).

The problem is one of the following:

- The 3pc. file on the media server is outdated. Recreate the 3pc. file.
- The media server is not on the same Fibre Channel network as the third-party copy device and client disk. As a result, the 3pc. file does not have a correct entry for the client disk. Run the bptpcinfo command with the -x client_name option; this option adds the client disk to the 3pc. file. For each disk that is added to the file by means of bptpcinfo -x client_name, you may need to add the device’s worldwide name (wwn=).

See the NetBackup Snapshot Client Configuration online document. See "Snapshot Client Assistance" in the NetBackup Snapshot Client Administrator’s Guide.

- The HP VxFS snapshot mechanism requires a dedicated cache partition for each snapshot. A check is made in the mount table to make sure that the cache partition is not already in use. If the cache partition is already in use, status code 20 occurs.

Check the /usr/openv/netbackup/logs/bpbkar log for a message similar to the following:

bpfsmap: FTL - bpfsmap: snapshot cache already in use, /dev/arrayvg/vol14c
bpbkar Exit: ERR - bpbkar FATAL exit status = 20: invalid command parameter
bpbkar Exit: INF - EXIT STATUS 20: invalid command parameter

If the snapshot cache partition is already in use, do one of the following: Set up your policy schedules to run at different times or use different cache partitions for each backup.
If the Allow multiple data streams option is enabled, each stream must have its own dedicated cache partition.

- Compare the NetBackup version level on the server to the version level on the clients by doing the following:
  - On UNIX or Linux NetBackup servers and clients, check the 
    /usr/openv/netbackup/bin/version file.
  - On Windows NetBackup servers, check the 
    install_path\Netbackup\version.txt file or the About NetBackup item 
    on the Help menu.
  - On Microsoft Windows clients, check the About NetBackup item on the 
    Help menu.
  - On NetWare target clients, check the Version entry in the bp.ini file.
  - On Macintosh clients, check the version file in the bin folder in the 
    NetBackup folder in the Preferences folder.
  - If a Java interface displays the error, tell them how to enable the debug 
    print manager in the Java startup file. Retry and compare the parameters 
    that were logged on the Java log with the parameters listed in the commands 
    usage statement.

- If these actions do not reveal the problem, do the following: Create a debug 
  log directory for the process that returned this status code (if the process uses 
  legacy logging). Then retry the operation and check the resulting log.

**NetBackup status code: 21**

**Message:** socket open failed

**Explanation:** A socket was not opened.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for clues on where and why the failure 
  occurred. If you cannot determine the cause from the Problems report, create 
  debug log directories for the processes that returned this status code. Then, 
  retry the operation and check the resulting debug logs.

- The following information applies only to Sun Solaris: 
  Verify that all operating system patches are installed. 
  See the Operating Notes section of the NetBackup Release Notes.

- The following information applies only to Windows systems: 
  Verify that the recommended service packs are installed.
NetBackup status code: 22

Message: socket close failed

Explanation: A socket was not closed.

Recommended Action: Do the following, as appropriate:

- Check the NetBackup Problems report for clues on where and why the failure occurred. If you cannot determine the cause from the Problems report, create debug log directories for the processes that could have returned this status code. Then, retry the operation and check the resulting debug logs.

- The following information applies only to Sun Solaris:
  Verify that all operating system patches are installed.
  See the Operating Notes section of the NetBackup Release Notes.

- The following information applies only to Windows systems:
  Verify that the recommended service packs are installed.

NetBackup status code: 23

Message: socket read failed

Explanation: A read operation from a socket failed.

Recommended Action: Do the following, as appropriate:

- Check the NetBackup Problems report for clues on where and why the failure occurred. If you cannot determine the cause from the Problems report, create debug log directories for the processes that could have returned this status code. Then, retry the operation and check the resulting debug logs.

- Corrupt binaries are one possible cause for this error.
  Load a fresh bptm from the install media to try to resolve the problem.

- The following information applies only to Sun Solaris:
  Verify that all operating system patches are installed.
  See the Operating Notes section of the NetBackup Release Notes.

- The following information applies only to Windows systems:
  Verify that the recommended service packs are installed.

- This error may occur during a restore to a Novell client.
  Note the following possible actions:

  - By default, the value for Novell "Maximum Concurrent Disk Cache Writes" may be too low (for example, 50); Novell recommends setting it to 100. A value of 100 increases the speed and efficiency of the disk cache writes. It increases the number of write requests to be run at one time.
- Change to or add the following settings in the Novell sys:system\autoexec.ncf file:
  ```
  SET Maximum Packet Receive Buffers = 4000
  SET Maximum Directory Cache Buffers = 4000
  SET Maximum Concurrent Disk Cache Writes = 2000
  SET Maximum Concurrent Directory Cache Writes = 2000
  SET Maximum Physical Receive Packet Size = 1514
  ```

- On Windows master servers, check the LIST_FILES_TIMEOUT value and ensure that this value is at least 1800.

**NetBackup status code: 24**

**Message:** socket write failed

**Explanation:** A write operation to a socket failed.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for clues on where and why the failure occurred. If you cannot determine the cause from the Problems report, create debug log directories for the processes that could have returned this status code. Then retry the operation and check the resulting debug logs.

- A possible cause is a high network load. For example, this problem occurs with `Cannot write to STDOUT` when a Windows system that monitors network load detects a high load. It then sends an ICMP packet to other systems to inform them that the route those systems use was disconnected. The log messages were similar to the following:

  ```
  01/31/96 14:05:23 ruble crabtree.null.com from client crabtree.null.com: ERR - Cannot write to STDOUT. Err no= 242: No route to host
  01/31/96 14:05:48 ruble crabtree.null.com successfully wrote backup id crabtree.null.com_0823125016, copy 1, fragment 1, 440864 Kbytes at 628.538 Kbytes/sec
  01/31/96 14:05:51 netbackup crabtree.null.com CLIENT crabtree.null.com POLICY Remote3SysFullW SCHED Sirius EXIT STATUS 24 (socket write failed)
  ```

- The following information applies only to Sun Solaris:
  Verify that all operating system patches are installed.
  See the Operating Notes section of the *NetBackup Release Notes*.

- The following information applies only to Windows systems:
Verify that the recommended service packs are installed.

- This error may occur during a restore to a Novell client.

Note the following possible actions:

- By default, the value for Novell "Maximum Packet Receive Buffers" may be too low (such as 100). To improve the restore performance, change this value to 2000. To change it, issue "SET Maximum Packet Receive Buffers=<value>" at the console, or enter the value in either of the following Novell files: sys:system\startup.ncf or sys:system\autoexec.ncf.

- Change to or add the following settings in the Novell sys:system\autoexec.ncf file:

  SET Maximum Packet Receive Buffers = 4000
  SET Maximum Directory Cache Buffers = 4000
  SET Maximum Concurrent Disk Cache Writes = 2000
  SET Maximum Concurrent Directory Cache Writes = 2000
  SET Maximum Physical Receive Packet Size = 1514

**NetBackup status code: 25**

**Message:** cannot connect on socket

**Explanation:** A process that timed out while it connects to another process for a particular operation. This problem can occur in the following situation: when a process tries to connect to the NetBackup request daemon (bpud) or database manager daemon (bpdbm) and the daemon is not running. (On Windows, these daemons are the NetBackup Request Manager and NetBackup database manager services.)

It can also occur in the following situations: the network or server is heavily loaded and has slow response time or an evaluation license key for NetBackup expired. However, the most common cause of this error is a host name resolution problem.

The following are other possible causes of this error caused by network connectivity issues or a required process such as pbx_exchange not running.

- `nbjm` is unable to connect to `bpcd` on the media server
- `nbpem` is unable to connect to `nbproxy`
- `bptm` on the media server is unable to connect to `nbjm` on the master server.
- You cannot perform an immediate backup operation.

These errors are

**Recommended Action:** Do the following, as appropriate:
Verify that `bpcompatd`, `vnetd`, and Private Branch Exchange (PBX) are running. Information on how to start PBX is available. See “Resolving PBX problems” on page 66.

If necessary, stop and restart NetBackup.

- On UNIX and Linux systems, enter the following:
  ```
  /usr/openv/netbackup/bin/bp.kill_all
  /usr/openv/netbackup/bin/bp.start_all
  ```

- On Windows systems, enter the following:
  ```
  install_path\NetBackup\bin\bpdown
  install_path\NetBackup\bin\bpup
  ```

The following information applies only to a UNIX or Linux NetBackup master server:
Verify that the `bprd` and the `bpdbm` processes are running. If these processes are not running, start them. On a Windows master server, verify that the NetBackup Request Manager and NetBackup database manager services are running. If these services are not running, start them.
If these processes or services are running, examine the All Log Entries report for the time of the failure to determine where the failure occurred.
Do one of the following:

- If you cannot view the report or you get a `cannot connect on socket` error when you try to view it, do the following: Verify again that the NetBackup database manager service or daemon is running. Then, create a debug log directory for `bpdbm`, retry the operation, and check the resulting debug log.

- If you can view the report and have not found an entry that is related to this problem: Create debug log directories for the related processes that were running when the error first appeared. (This process frequently is `bpbrm`.) Then, retry the operation and check the resulting debug logs.

Verify that the server list specifies the correct master server.

The following information applies only to Windows systems:
The master server is designated in the Server to use for backups and restores drop-down in the Specify NetBackup Machines and Policy Type dialog box. To display this dialog box, start the Backup, Archive, and Restore interface and click Specify NetBackup Machines and Policy Type on the File menu.
The following information applies only to UNIX, Linux, and Macintosh systems:

- The master server is the first SERVER entry in the bp.conf file.

- On NetWare target clients: The master server name is the first SERVER entry in the bp.ini file.

- Check the following &Company; support Web site to ensure that all recommended NetBackup patches are installed:
  www.symantec.com/business/support/
  Then select "NetBackup" followed by "files and updates."

- If failure occurs when you run a user-directed backup from a client, make sure that a user-directed backup schedule exists at the master server.

- With NetBackup database extensions: Make sure that the applicable database product has the correct permissions allowing NetBackup to write to the progress log on the client.

The following information applies only to UNIX and Linux systems:

- If bpdbm has quit when the shutdown script runs on a media server, carefully read the K77netbackup script. It contains details on how to prevent this problem. The script is in /usr/openv/netbackup/bin/goodies.

If you change the server list on a master server, stop, and restart the following: The NetBackup database manager and request daemons (UNIX and Linux) or the NetBackup database manager and NetBackup Request Manager services (Windows).

- Check the services file.

- The following information applies only to UNIX and Linux systems:
  Verify that the /etc/services file (and NIS services if NIS is used) has entries for the NetBackup services: bpcd, bpdbm, and bprd.

On Windows, verify that the %SystemRoot%\system32\drivers\etc\services file has the correct entries for bpcd, bpdbm, and bprd.

Also, verify that the following numbers match the settings in the services file: The NetBackup Client Service Port and the NetBackup Request Service Port on the Network tab in the NetBackup Client Properties dialog box. To display this dialog box, start the Backup, Archive, and Restore interface and click NetBackup Client Properties on the File menu. The values on the Network tab are written to the services file when the NetBackup Client service starts.

See “Verifying host name and service entries” on page 48.

- On Sun Solaris, verify that all operating system patches are installed

See the Operating Notes section of the NetBackup Release Notes.
On Windows, verify that the recommended service packs are installed.

When the base NetBackup license key expires, daemons (such as bprd and bpdbm) terminate on the NetBackup server. If these daemons are not running, you are likely to encounter status code 25 errors in the Administration console. Install a valid base NetBackup license key, restart the daemons, and restart the console.

For NetBackup Snapshot Client, the following applies: When many devices are configured on a media server, it may take a long time for the bptpcinfo command to generate the file 3pc. When the backup is run for the first time, the backup may fail with status 25. Make sure that the /usr/openv/volmgr/database/3pc.conf file exists. If it does, rerun the backup. If the backup fails again, run the bptpcinfo manually to generate the file 3pc., then try the backup again.

NetBackup status code: 26

Message: client/server handshaking failed

Explanation: A process on the server encountered an error when it communicated with the client. This error indicates that the client and server were able to initiate communications, but encountered difficulties and the communications did not complete. This problem can occur during a backup or a restore.

Recommended Action: Determine which activity encountered the handshake failure by examining the All Log Entries report for the appropriate time period. Determine the client and server that had the handshake failure.

For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.

NetBackup status code: 27

Message: child process killed by signal

Explanation: A child of the process that reported this error was terminated. This error may occur if the backup job was terminated or another error terminated the child process. This problem may also occur if a NetBackup process was terminated through Task Manager or another utility.

Recommended Action: Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create a debug log directory for the process that you think may have returned this status code. Then, retry the operation and check the resulting debug log.
NetBackup status code: 28

Message: failed trying to fork a process

Explanation: A fork of a child process failed (on UNIX and Linux) or a CreateProcess failed (on Windows).

This failure may be due to the following:

■ An overloaded system
■ Insufficient swap space or physical memory
■ Too many processes are running on the system

Recommended Action: Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create debug log directories for the processes that think may have returned this status code. Then, retry the operation and check the resulting debug logs.

NetBackup status code: 29

Message: failed trying to exec a command

Explanation: A command was not run. This error can occur because the permissions of the command do not allow it to be run. Or it occurs due to a lack of system resources such as memory and swap space.

Recommended Action: Do the following, as appropriate:

■ Check the NetBackup All Log Entries report for clues on where and why the failure occurred.
■ Check the permissions on the command to be run.
■ For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.

NetBackup status code: 30

Message: cannot get passwd information

Explanation: Could not get the passwd entry for a user.

Recommended Action: Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create a debug log for the process that you think may have returned this status code. Then, retry the operation and check the resulting debug log.
NetBackup status code: 31

Message: could not set user id for process

Explanation: Could not set the user ID of a process to the user ID of the requesting user. NetBackup runs client processes as the requesting user.

Recommended Action: Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create a debug log directory for the process that you think may have returned this status code. Then, retry the operation and check the resulting debug log.

NetBackup status code: 32

Message: could not set group id for process

Explanation: Could not set the group ID of a process to the requesting user group. NetBackup runs client processes with the group ID of the requesting user.

Recommended Action: Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create a debug log directory for the process that you think may have returned this status code. Then, retry the operation and check the resulting debug log.

NetBackup status code: 33

Message: failed while trying to send mail

Explanation: An email notification about backup, archive, or restore results has failed. The email was not sent to the administrator’s address as specified by the email global attribute. On a UNIX or Linux client, the email was not sent to an email address that is specified with USEMAIL in the client’s bp.conf file.

Recommended Action: Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create a debug log directory for the process that you think may have returned this status code. Then, retry the operation and check the resulting debug log.

NetBackup status code: 34

Message: failed waiting for child process

Explanation: A NetBackup process encountered a failure while it waited for a child process to complete.

Recommended Action: Check the NetBackup All Log Entries report for clues on where and why the failure occurred. For detailed troubleshooting information, create a debug log for the process that you think may have returned this status code. Then, retry the operation and check the resulting debug log.
NetBackup status code: 35

Message: cannot make required directory

Explanation: Could not create a required directory.

Possible causes are the following:
- A process does not have permission to create the directory
- The path to the directory is not valid
- An IO error occurs
- No space is available on the device that contains the directory

Recommended Action: Do the following, as appropriate:
- Check the NetBackup All Log Entries report to determine which directory was not created and why it was not created. In particular, check for a full disk partition.
- Check the permissions on the parent directory. Verify that NetBackup services are started with a "Logon as" account that has permission to create the directory.
- For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.

NetBackup status code: 36

Message: failed trying to allocate memory

Explanation: Allocation of system memory failed. This error occurs when an insufficient system memory is available. This cause of this error may be that the system is overloaded with too many processes and it does not enough physical and virtual memory.

Recommended Action: Free up memory by terminating any unneeded processes that consume a lot of memory. Add more swap space or physical memory.

NetBackup status code: 37

Message: operation requested by an invalid server

Explanation: An invalid media server or Windows NetBackup Remote Administration Console made a request to the NetBackup request daemon (bprd) or NetBackup database manager daemon (bpdbm). On Windows, these daemons are the NetBackup Request Manager and NetBackup database manager services.
**Recommended Action:** Examine the NetBackup All Log Entries report for the time of this error to determine which system tried to connect to the master server.

If the server is a valid media server, verify that the storage unit for the media server is defined. Also, verify that the server or Windows NetBackup Remote Administration Console has a server list entry on the master server.

If necessary, update the server list.

On a UNIX or Linux master server, add a `SERVER = media_server_name` to the `bp.conf` file. `media_server_name` is the host name of the media server. On a Windows master server, add the media server to the list on the Servers tab in the Master Server Properties dialog box.

See “Using the Host Properties window” on page 60.

If a server or Windows NetBackup Remote Administration Console has more than one host name (for example, it has multiple network interfaces), do the following: verify that the master server has a server list entry for each of them.

If you change the server list on a UNIX or Linux master server, for the changes to take effect do the following: stop and restart the NetBackup Request daemon (`bprd`) and NetBackup database manager daemon (`bpdbm`). If you change the server list on a Windows master server, stop, and restart the NetBackup Request Manager and NetBackup database manager services.

**NetBackup status code: 38**

**Message:** could not get group information

**Explanation:** Could not get the group entry that describes a UNIX or Linux user group.

**Recommended Action:** Check the NetBackup Problems report for clues on why the error occurred. For detailed troubleshooting information, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.

**NetBackup status code: 39**

**Message:** client name mismatch

**Explanation:** The client used a name in a request to the NetBackup server that did not match the configured name in the policy on the server.

**Recommended Action:** Change one of the following so the two match: the NetBackup client name setting on the client (see the applicable NetBackup users guide) or the one in the policy configuration on the server.
NetBackup status code: 40

Message: network connection broken

Explanation: The connection between the client and the server was broken. This status code can also appear if the connection is broken between the master and the media server during a backup.

Recommended Action: Do the following, as appropriate:

- Try pinging the client from the server. If pinging is not possible, check for loose connections or other network problems.
- Verify that the server list settings are correct on both the client and the server. If the backup involves a media server, verify that these entries are correct on both the master and the media server. For example, if a media server does not have a server list entry for the master, it does not accept connections from the master.
  - On Windows, the master server is designated on the Servers tab in the Master Server Properties dialog box. See “Using the Host Properties window” on page 60.
  - On UNIX, Linux, and Macintosh systems the master server is the first SERVER entry in the bp.conf file.
  - On NetWare target clients the master server name is the first SERVER entry in the bp.ini file.
- If you change the server list on a UNIX or Linux master server, for the changes to take effect you must do the following: Stop and restart the NetBackup Request daemon (bprd) and NetBackup database manager daemon (bpdbm). On Windows, stop and restart the NetBackup Request Manager and NetBackup database manager services.
- Status code 40 can also be due to denial of a mount request by the operator.
- This status code may occur if nbjm was unable to connect to bpbrm or to bpmount. Examine the nbjm unified log (originator ID 117) or the bpbrm or the bpmount legacy logs for more detail on the cause of the error.

NetBackup status code: 41

Message: network connection timed out

Explanation: The server did not receive any information from the client for too long a period of time.

Recommended Action: Do the following, as appropriate:
On UNIX, Linux, or Windows clients, check for the following problems with the `bpbkar` client process.

On Windows clients: The `bpbkar` client process is not hung. Due to the files and directories it scans, it has not replied to the server within the **Client read timeout** or **Client connect timeout** period. This error occurs during incremental backups when directories have thousands of unmodified files. For this case, use Host Properties on the NetBackup server to change **Client connect timeout** or **Client read timeout**. These settings are on the Timeouts and Universal Settings tabs, respectively, in the **Master Server Properties** dialog box. The default for these timeouts is 300 seconds.

See “Using the Host Properties window” on page 60.
You can also monitor CPU utilization to determine if this condition exists.

The following information applies only to UNIX or Linux clients:

- The `bpbkar` client process is hung on a file that has a mandatory locking set. For this case, add the following to the client’s `bp.conf` file:

  `VERBOSE`

  And as root on the client run the following:

  ```bash
touch /usr/openv/netbackup/bpbkar_path_tr
/usr/openv/netbackup/logs/bpbkar
```

  Then retry the operation. The names of the files are logged on the debug log file in the `/usr/openv/netbackup/logs/bpbkar` directory before `bpbkar` processes them. The last file in the log is the file that causes problems.

**Note:** Also, use these procedures for other "unknown" `bpbkar` hangs.

If the problem is due to mandatory file locking, have NetBackup skip the locked files. Set `LOCKED_FILE_ACTION` to `SKIP` in the `/usr/openv/netbackup/bp.conf` file on the client.

- The `bpbkar` client process is not hung. Due to the files and directories it scans, it has not replied to the server within **CLIENT_READ_TIMEOUT** or **CLIENT_CONNECT_TIMEOUT**. This error occurs during backups when directories have thousands of unmodified files or during restores of the sparse files that have thousands of holes. For this case, try to add or modify the **CLIENT_READ_TIMEOUT** and **CLIENT_CONNECT_TIMEOUT** values in the server’s `/usr/openv/netbackup/bp.conf` file. The default for the **CLIENT_READ_TIMEOUT** and **CLIENT_CONNECT_TIMEOUT** is 300 seconds if it is not specified.
Use your system’s `ps` command and monitor CPU utilization to help decide which of these conditions exist.

When you finish the investigation of the problem, delete the `/usr/openv/netbackup/logs/bpbkar` directory, since the log files can become quite large and are not deleted automatically. Also delete `/usr/openv/netbackup/bpbkar_path_tr` so you do not generate larger log files than needed the next time you create directory `/usr/openv/netbackup/logs/bpbkar`.

- On Windows systems, try the following:
  - Disable the following file:
    ```bash
    install_path\VERITAS\NetBackup\bin\tracker.exe
    ```
  - Repair hard drive fragmentation. Try an application that is called Diskeeper Lite, which is part of the Windows Resource Kit.
  - Make sure that enough space is available in \temp.

- If the server cannot connect to the client, do the following: Create `bpcd` or `bpbkar` (UNIX, Linux, and Windows only) debug log directories on the client. Then retry the operation and check the resulting logs. If these logs do not provide a clue, create a `bpbrm` debug log on the server. Then retry the operation and check the resulting debug log.

  If the `bpbrm` log has entries similar to the following, the problem is in the routing configuration on the server:

  ```bash
  bpbrm hookup_timeout: timed out waiting during the client hookup
  bpbrm Exit: client backup EXIT STATUS 41: network connection timed out
  ```

  Verify that the client IP address is correct in the name service that is used. On UNIX and Linux clients, if both the NIS and the DNS files are used, verify that they match.

  See “Resolving network communication problems” on page 40.

- If you use an AIX token ring adapter and the `routed` daemon is running, the timeout occurs because the token ring adapter creates dynamic routes. It then causes the `routed` daemon to crash.

- For a FlashBackup client, this error occurs if the file system being backed up is very large and has a very large number of files. It can also occur if a large number of concurrent data streams are active at the same time. To correct it, add `CLIENT_READ_TIMEOUT` to the `/usr/openv/netbackup/bp.conf` file and set it to increase the timeout interval.
- Make sure all recommended NetBackup patches are installed. Check the following support Web site for current patch information: www.symantec.com/business/support/
  Then select "NetBackup" followed by "files and updates".

- Add the CLIENT_READ_TIMEOUT values to the master server, media server, and client when a NetBackup database extension product is installed. The values should all be the same for each server. The value set is dependent on the size of the database being backed up. More information on CLIENT_READ_TIMEOUT is available.
  See the NetBackup Administrator's Guide, Volume II.

- Make sure that enhanced authentication is configured correctly. For example, the following may result in status code 41: Host A is configured to use enhanced authentication with host B, but host B is not configured to use enhanced authentication with host A. In this case, connections from host B to host A are likely to fail with status code 41. Connections from host A to B are likely to fail with authentication errors (status code 160).

**NetBackup status code: 42**

**Message:** network read failed

**Explanation:** An attempt to read data from a socket failed.

**Recommended Action:** Do the following, as appropriate:

- Verify that both the client and the server are operational.
- Resolve any network communication problems.
  See “Resolving network communication problems” on page 40.
- Check the Problems report for clues.

**NetBackup status code: 43**

**Message:** unexpected message received

**Explanation:** The client and the server handshake were not correct.

**Recommended Action:** Do the following, as appropriate:

- Verify that the correct version of software is running on the client and the server.
- To enable detailed debug logging, do the following:
  - On the server, create a `bpbrm` debug log directory.
  - On clients, create a `bpcd` debug log directory (created automatically on Macintosh clients).
- Increase the amount of debug information to include in the logs. See “About using logs and reports” on page 79.

- Retry the operation and examine the logs. If you use `bpstart_notify` scripts on UNIX, Linux, or Windows clients, verify that messages are not written to `stdout` or `stderr`.

### NetBackup status code: 44

**Message:** network write failed

**Explanation:** An attempt to write data to a socket failed.

**Recommended Action:** Do the following, as appropriate:

- Check the Problems report for information about the error.
- Verify that the client and servers are operational and connected to the network.
- Create a debug log directory for the process that reported the problem and the operation. Examine the resulting debug log file for detailed troubleshooting information. See “Resolving network communication problems” on page 40.

### NetBackup status code: 45

**Message:** request attempted on a non reserved port

**Explanation:** A try was made to access a client from a non-reserved port.

**Recommended Action:** Verify that the latest software is installed on the client and server.

- On UNIX and Linux NetBackup servers and clients, check the `/usr/openv/netbackup/bin/version` file.
- On Windows NetBackup servers, check the `install_path\netbackup\version.txt` file or the About NetBackup item on the Help menu.
- On Microsoft Windows clients, check the About NetBackup item on the Help menu.
- On NetWare target clients, check the Version entry in the `bp.ini` file.
- On Macintosh clients, check the version file in the bin folder in the NetBackup folder in the Preferences folder.

### NetBackup status code: 46

**Message:** server not allowed access
Explanation: The server tries to access a client, but access is blocked. Possible causes are as follows:

- The server is not listed on the client as a valid server.
- The client was configured to require encrypted backups, but the encryption attribute for the backup policy on the server was not selected.
- The evaluation license for the NetBackup Encryption product has expired on the server, but the NetBackup client was configured to require encrypted backups. As a result, the server tries to make a non-encrypted backup of the client. Since the client is configured to require encryption, the backup failed.

Recommended Action: Do the following, as appropriate:

- If the server is a valid server but is not listed on the client, add its name to the client’s server list:
  - On Windows clients in the Specify NetBackup Machines and Policy Type dialog box, do the following: Add the server in the Server to use for backups and restores drop-down list. To display this dialog box, start the Backup, Archive, and Restore interface on the client. Then click Specify NetBackup Machines and Policy Type on the File menu.
  - On UNIX, Linux, and Macintosh clients, add a SERVER entry in the bp.conf file.
  - On NetWare target clients, add a SERVER entry in the bp.ini file.

- To make non-encrypted backups of the client, set CRYPT_OPTION on the client to allowed or denied.
  Refer to the NetBackup Encryption Administrator’s Guide.

- If the NetBackup encryption evaluation license has expired on the server and you want to continue encrypting backups of the client, do the following:
  - Purchase a permanent encryption license key and add it to the server. After you add the permanent encryption license key, check the attributes of the backup policy to make sure that encryption is selected.
  - To check the validity of an evaluation license key, do the following:
    - On Windows, go to the Help menu on the NetBackup Administration window on the NetBackup server and select License Keys. If the evaluation key is not listed in the NetBackup License Keys window, the key has expired. Use this window to add the new permanent encryption key.
    - On UNIX and Linux, use the following command on the server:
      /usr/openv/netbackup/bin/admincmd/get_license_key
Select option 8 to list the active license keys and features. If the evaluation key is not listed, the key has expired. Use this command to add the new permanent encryption key.

**NetBackup status code: 47**

**Message:** host is unreachable

**Explanation:** An attempt to connect to another machine failed.

**Recommended Action:** Do the following, as appropriate:

- Verify that the name service (or services) used by the client are configured to resolve the host names of the NetBackup server correctly.
- Verify that the name service (or services) used by the server are configured to resolve the host name of the NetBackup client correctly.
- Try to ping the client from the server and the server from the client.
- If you continue to have problems, do the following:
  See “Resolving network communication problems” on page 40.

**NetBackup status code: 48**

**Message:** client hostname could not be found

**Explanation:** The system function `gethostbyname()` failed to find the client’s host name.

**Recommended Action:** Verify that the client name is correct in the following:

- The NetBackup policy configuration on the master server.
- The General tab in the following dialog boxes: NetBackup Client Properties and Specify NetBackup Machines and Policy Type (on Microsoft Windows and NetWare nontarget clients). To display these dialog boxes, start the Backup, Archive, and Restore interface on the client. For the General tab, click **NetBackup Client Properties** on the File menu; click **Specify NetBackup Machines and Policy Type** on the File menu.
- The `bp.conf` file on UNIX, Linux, and Macintosh clients.
- The `bp.ini` file on NetWare target clients.
- On clients and servers, verify that the name service is set up to resolve the NetBackup client names correctly.

On UNIX and Linux clients, verify that the client’s host name is in the `/etc/hosts` file or the YP hosts file or NIS maps.
**NetBackup status code: 49**

**Message:** client did not start

**Explanation:** The client failed to start up correctly.

**Recommended Action:** Do the following, as appropriate:

- Make sure that software is installed on the client and it is the correct version. If necessary, reinstall the client software.
- Check for full file systems on the client.
- Enable detailed debug logging on the client by doing one of the following:
  - Create `bpcd` and `bpkar` (UNIX, Linux, and Windows only) debug log directories.
  - On a UNIX or Linux client, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.
  - On PC clients, increase the debug or log level. See “How to set logging levels on UNIX clients” on page 116. See “How to set logging levels on PC clients” on page 120. Retry the operation and examine the resulting logs.
- On UNIX or Linux systems, use the UNIX `sum` command to check for corrupt binaries.

**NetBackup status code: 50**

**Message:** client process aborted

**Explanation:** The client backup terminated abnormally. For example, this error occurs if a NetBackup master or media server is shut down or rebooted when a backup or restore is in progress.

**Recommended Action:** Do the following, as appropriate:

- Enable detailed debug logging.
  - Create a `bpkar` debug log directory (UNIX, Linux, and Windows clients only).
  - Create a `bpcd` debug log directory. (This log is created automatically on Macintosh clients.)
  - On UNIX and Linux clients, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.
  - On PC clients, increase the debug or log level. See “How to set logging levels on UNIX clients” on page 116.
See “How to set logging levels on PC clients” on page 120. Retry the operation and examine the resulting logs.

- This error may occur if *nbjm* terminated while a backup job was running. Examine the unified logging files on the NetBackup server for *nbjm* (117) for more detail on the error. All unified logging is written to `/usr/openv/logs` (UNIX and Linux) or `install_path\NetBackup\logs` (Windows).

- On UNIX and Linux clients, check for core files in the `/` directory.

- On UNIX and Linux clients, check the system log (`/usr/adm/messages` on Solaris) for system problems.

- This problem can sometimes be due to a corrupt binary. On UNIX and Linux clients, use the UNIX `sum` command to check the `bpcd`, `bpbkar`, and `tar` binaries, which are located in `/usr/openv/netbackup/bin` on the client. Reinstall them if they are not the same as in the client directory under `/usr/openv/netbackup/client` on the server.

  On a Windows client, check the `bpinetd.exe`, `bpcd.exe`, `bpbkar32.exe`, and `tar32.exe` files, which are located in the `install_path\NetBackup\bin` folder on the client.

  Reinstall the client if these files are as follows:
  - Not the same size as on other Windows clients
  - Not at the same release level
  - Do not have the same NetBackup patches as other Windows clients

**NetBackup status code: 51**

**Message:** timed out waiting for database information

**Explanation:** The catalog process did not respond within five minutes.

**Recommended Action:** Do the following, as appropriate:

- Verify that the NetBackup database manager service or daemon is running.

- Verify that the file system that contains the NetBackup catalogs has enough space.

- Create `bpbrm` and `bpdbm` debug log directories on the server and retry the operation.

- Look in the debug log files to find more information on the problem.
NetBackup status code: 52

Message: timed out waiting for media manager to mount volume

Explanation: The requested volume was not mounted before the timeout expired. This error can also occur if the volume is a cleaning tape but was not specified as a cleaning tape.

Another possible cause: the last available drive has a mount request for a non-backup (such as a restore). Then a backup that requires the same drive is initiated before the mount completes. This error is due to the drive not being reported as busy until the mount completes.

Recommended Action: Do the following, as appropriate:

- Verify that the requested volume is available and an appropriate drive is ready and in the UP state.
- If this error occurs during a read operation (restore, duplicate, verify), the drives could be busy. Increase the timeout for the media mount that the NetBackup global attribute specifies, to allow more time to mount and position the media.
- Verify that the tape is not a cleaning tape that is configured as a regular volume.
- When an Automated Cartridge System controls the robot, verify that the ACSLS system is up.
- If it is an initial installation, a procedure is available.
  See “Resolving common configuration problems” on page 28.
- On Windows, check the Event Viewer Application log for the error messages that indicate why the tape mount did not complete. On UNIX and Linux, check the system log.

NetBackup status code: 53

Message: backup restore manager failed to read the file list

Explanation: The backup and restore manager (bpbrm) did not read the list of files to back up or restore.

Recommended Action: Verify that the server software was installed correctly on all NetBackup servers. If that is not the problem, do the following:

- Create bpbrm debug log directories on the server.
- On a UNIX or Linux NetBackup server, add the VERBOSE option to the bp.conf file. On a Windows NetBackup server, set the Global logging level option on the Logging tab in the Master Server Properties dialog box.
  To display this dialog box, refer to the following topic:
See “Using the Host Properties window” on page 60. Increase the unified logging levels by using the `vxlogcfg` command as explained in the following procedure:
See “Configuring and using unified logging” on page 93.

- Retry the operation and check the resulting debug logs for detailed troubleshooting information.

**NetBackup status code: 54**

**Message:** timed out connecting to client

**Explanation:** The server did not complete the connection to the client. The accept system or winsock call timed out after 60 seconds.

Some third-party software packages (for example, a personal firewall product) can affect the TCP/IP stack in Windows. This action can cause a loss of connection between the NetBackup server and the `bpcd` process on the client. NetBackup tries to set SO_REUSEADDR (allow local address reuse) on the inbound socket connection so that the port can be handed off from bpinetd.exe (the NetBackup Client Service) to bpcd.exe. Some products may not allow this functionality due to the various methods that can be used to violate system security.

**Recommended Action:** Do the following, as appropriate:

- For a Macintosh or NetWare target client: Verify that the server does not try to connect when a backup or restore is already in progress on the client. These clients can handle only one NetBackup job at a time.
  On a Macintosh, check for activity by examining the `NetBackupListen` file in the following folder on the startup disk of the Macintosh client:

  ```
  ```

- Perform the following procedure:
  See “Resolving network communication problems” on page 40.

- On UNIX and Linux clients, verify that the `/usr/openv/netbackup/bin/bpcd` binary exists and that it is the correct size.

- Check the `/etc/inetd.conf` file to make sure the `bpcd` path is correct in the following entry:

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

- On the systems that include the following, make sure that the client name is in the master's `/etc/hosts` file: NetBackup master, media, and clients (with NetBackup database extension products installed on one or more clients).
- Completely uninstall the third-party software package on the client that causes the failure. Or, contact the software manufacturer to investigate if other configuration options or workarounds are possible.

**NetBackup status code: 55**

**Message:** permission denied by client during rcmd

**Explanation:** The UNIX or Linux client does not have the server's name in its `.rhosts` file.

**Recommended Action:** Add the server name to the `.rhosts` file on the UNIX or Linux client.

**NetBackup status code: 56**

**Message:** client’s network is unreachable

**Explanation:** An error reported that the client could not reach the host (WSAENETUNREACH on Windows or ENETUNREACH on UNIX and Linux) on a system call.

**Recommended Action:** Try to ping the client from the server. Check the IP address for the client. If you still have problems, talk to your network administrator.

**NetBackup status code: 57**

**Message:** client connection refused

**Explanation:** The client refused a connection on the port number for `bpcd`.

This error can occur because of the following:

- No process listening activity occurs on the `bpcd` port
- The number of connections to the `bpcd` port is more than the network subsystem can handle with the `listen()` call

**Recommended Action:** Do the following, as appropriate:

- For Windows NetBackup servers:
  - Make sure the NetBackup client software is installed.
  - Verify that the `bpcd` and `bprd` port numbers in the `%SystemRoot%\system32\drivers\etc\services` file on the server matches the setting on the client.
  - Verify that the **NetBackup Client Service Port** number and **NetBackup Request Service Port** number on the **Network** tab in the **NetBackup Client Properties** dialog match the `bpcd` and `bprd` settings in the `services` file.
To display this dialog, start the Backup, Archive, and Restore interface on the server and click **NetBackup Client Properties** on the **File** menu. The values on the Network tab are written to the **services** file when the NetBackup Client service starts.

- Verify that the NetBackup client service is running.
- Use the following command to see if the master server returns correct information for the client:

  \[install_path\VERITAS\NetBackup\bin\bpclntcmd -pn\]

- On UNIX and Linux servers, do the following:
  - Make sure the NetBackup client software is installed.
  - Verify that the **bpcd** port number on the server (either NIS services map or in `/etc/services`) matches the number in the client’s services file.

- For a Macintosh or NetWare target client, verify that the server is not trying to connect when a backup or restore is already in progress on the client. These clients can handle only one NetBackup job at a time.

- Additional help is available.
  See “Resolving network communication problems” on page 40.

**NetBackup status code: 58**

**Message:** can’t connect to client

**Explanation:** The server was unable to connect to the client.

**Recommended Action:** Resolve network communication problems.

See “Resolving network communication problems” on page 40.

**NetBackup status code: 59**

**Message:** access to the client was not allowed

**Explanation:** The master or the media server tries to access the client, but the client does not recognize the server as a valid server.

For the Enterprise Vault Agent: The names of all of the media servers among the Enterprise Vault servers are not specified in the client configuration.

**Recommended Action:** Do the following, as appropriate:

- If the server is a valid server, verify that it is in the server list on the client. If necessary add it as follows:
On Windows clients: Add the server on the **Server to use for backups and restores** drop-down in the **Specify NetBackup Machines and Policy Type** dialog box. To display this dialog box, start the Backup, Archive, and Restore interface on the client. Then click **Specify NetBackup Machines and Policy Type** on the **File** menu.

On UNIX and Linux, and Macintosh clients: add a **SERVER** entry in the **bp.conf** file.

On NetWare target clients: add a **SERVER** entry in the **bp.ini** file.

If you change the server list on a UNIX or Linux master server, do the following for the changes to take effect: stop and then restart the NetBackup Request daemon (**bprd**) and NetBackup database manager daemon (**bpdbm**). On Windows, stop and restart the NetBackup Request Manager and NetBackup Database Manager services.

On Windows clients, enable **bpinetd** debug logging as follows:

- Create a **bpinetd** debug log directory on the client.
- Increase the debug or log level.
  
  See “How to set logging levels on UNIX clients” on page 116.
  
  See “How to set logging levels on PC clients” on page 120.
- Retry the backup and examine the resulting logs to determine the cause of the failure.

On all clients, enable **bpcd** debug logging as follows:

- Create a **bpcd** debug log directory on the client.
- On a UNIX or Linux client, add the **VERBOSE** option to the
  
  ```bash
  /usr/openv/netbackup/bp.conf
  ```
- On PC clients, increase the debug or log level as explained in the debug log topics in Chapter 3.
- Retry the backup and examine the resulting logs to determine the cause of the failure.
- Check the **bpcd** debug log to determine the server’s peer name and what comparisons are made.
  
The **bpcd** process compares NetBackup server list entries to the peer name of the server that tries the connection. It rejects the connection if the names are different. If necessary, change the server list entry on the client to match the peer name.

On Windows clients, check the following:
Verify that NetBackup for Windows software was installed under a Windows administrator account. If NetBackup is under another type of account, reinstall it under an administrator account. The installation completes successfully under a non-administrator account except for the following: the NetBackup Client service is not added to Windows and the NetBackup server cannot access the client.

Verify that the Windows TCP/IP service specifies the domain server that resolves names for the subnet that contains the NetBackup servers. UNIX, Linux, and Windows clients are frequently not on the same subnet and use different domain servers. When this condition exists, NetBackup servers and Windows clients may be able to ping one another, but the server still cannot access the Windows client.

The preceding items may not resolve this problem. See “Resolving network communication problems” on page 40.

If NetBackup use multiple network interfaces with media servers, make sure the interface names appear in the client’s /usr/openv/netbackup/bp.conf file.

For the Enterprise Vault Agent: See the Troubleshooting section of the NetBackup for Enterprise Vault Agent Administrator’s Guide.

**NetBackup status code: 60**

**Message:** client cannot read the mount table

**Explanation:** The backup process on the client did not read the list of mounted file systems.

**Recommended Action:** Do the following, as appropriate:

- Run a `df` to see if the system can read the mount table.
- On an SCO system, code 60 can occur because the mount-point path name exceeds 31 characters (the maximum number on an SCO system). The `bpbkar` debug log on the client shows a message similar to the following:

  ```
  bpbkar build_nfs_list: FTL - cannot statfs net Errno: 42406
  ```

  To eliminate these errors for future backups, create a mount point with a shorter name and symbolically link the long name to the short name.

- For detailed troubleshooting information, create a `bpbkar` debug log directory. Then retry the operation and check the resulting log.
NetBackup status code: 63
Message: process was killed by a signal
Explanation: A kill signal was sent to the client process.
Recommended Action: The usual cause for this error is that someone intentionally terminated a backup.

NetBackup status code: 64
Message: timed out waiting for the client backup to start
Explanation: The client did not send a ready message to the server within the allotted time.
Recommended Action: Do the following, as appropriate:
  ■ On all clients, enable bpcd debug logging as follows:
    ■ Create a bpcd debug log directory on the client.
    ■ On a UNIX or Linux client, add the VERBOSE option to the
      /usr/openv/netbackup/bp.conf file.
    ■ On PC clients, increase the debug or log level.
      See “How to set logging levels on PC clients” on page 120.
  ■ On a UNIX, Linux, or Windows client, create the bpbkar debug log directory
    on the client.
  ■ On Windows clients, verify that the NetBackup Client service is running.
  ■ On a UNIX or Linux client, use the ps command to check for a client process
    that uses too much CPU time.
  ■ Retry the backup and examine the debug logs for clues on the cause of the
    failure.

NetBackup status code: 65
Message: client timed out waiting for the continue message from the media
manager
Explanation: The tape manager, bptm, reported that the media did not load and
position within the allotted time.
Recommended Action: Verify that the requested volume is available and the
required device is in an UP state.
  ■ Create a bptm debug log directory on the server.
On a UNIX or Linux NetBackup server, add the `VERBOSE` option to the `bp.conf` file. On a Windows NetBackup server, set the **Verbose logging level** option on the Logging tab in the Master Server Properties dialog box. See “Using the Host Properties window” on page 60.

Retry the operation and check the `bptm` debug log file for information on the drive, robot, and tape that causes the timeout.

On a Windows NetBackup server (master or media): check the Event Viewer Application log for the error messages that indicate why the tape mount did not complete.

**NetBackup status code: 66**

**Message:** client backup failed to receive the CONTINUE BACKUP message

**Explanation:** The client `bpbkar` process did not receive the message from the server that indicates that the server is ready to continue.

**Recommended Action:** Do the following, as appropriate:

- Verify that the server did not crash.
- On UNIX, Linux, and Windows clients, enable `bpbkar` debug logging.
  - Create a `bpbkar` debug log directory.
  - On a UNIX or Linux client, add the `VERBOSE` option to the `bp.conf` file. On a Windows client, set **Verbose** on the **TroubleShooting** tab in the NetBackup Client Properties dialog box. To display this dialog box, start the Backup, Archive, and Restore interface on the client. Then select **NetBackup Client Properties** from the **File** menu.
- On other PC clients except Macintosh, create a debug log directory for `bpcd` (the `bpcd` log is created automatically on Macintosh).
  Increase the amount of information that appears in the logs.

  See “How to set logging levels on UNIX clients” on page 116.
  See “How to set logging levels on PC clients” on page 120.

- On the master server, create `bpbrm` debug log directories. Increase the logging level for the diagnostic and debug logs for nbpem, nbjm, and nbrb.
  Use the `vxlogcfg` command as described in the following topic:

  See “Configuring and using unified logging” on page 93.

- Retry the operation and check the resulting debug logs.

**NetBackup status code: 67**

**Message:** client backup failed to read the file list
**Explanation:** The client did not read the list of files to back up.

**Recommended Action:** Do the following, as appropriate:

- Verify that the server did not crash.
- Set up debug logging.
  - On the server, create a `bpbrm` debug log directory.
  - On UNIX, Linux, and Windows clients, create a `bpbkar` debug log directory.
  - On other PC clients except Macintosh, create a debug log directory for `bpcd` (the `bpcd` log is created automatically on Macintosh).
  - Increase the amount of information that appears in the logs.
    - See “How to set logging levels on UNIX clients” on page 116.
    - See “How to set logging levels on PC clients” on page 120.
- Retry the operation and check the resulting debug logs.

**NetBackup status code: 68**

**Message:** client timed out waiting for the file list

**Explanation:** The client did not receive the list of files to back up within the allotted time. This list comes from the server.

**Recommended Action:** Do the following, as appropriate:

- Verify that the server did not crash.
- Set up debug logging.
  - On the server, create a `bpbrm` debug log directory.
  - On UNIX, Linux, and Windows clients, create a `bpbkar` debug log directory.
  - On other PC clients except Macintosh, create a debug log directory for `bpcd` (the `bpcd` log is created automatically on Macintosh).
  - Increase the amount of information that appears in the logs.
    - See “How to set logging levels on UNIX clients” on page 116.
    - See “How to set logging levels on PC clients” on page 120.
- Retry the operation and check the resulting debug logs.

**NetBackup status code: 69**

**Message:** invalid filelist specification

**Explanation:** The file list from the server had invalid entries.
For the Enterprise Vault Agent: A policy contains directives that cannot be specified together in the same policy.

**Recommended Action:** Do the following, as appropriate:

Check the policy file list. If wildcards are used, verify that the bracket characters ([ and ]) in the list match. If the file list contains UNC (Universal Naming Convention) names, ensure they are properly formatted.

This error can occur if nbjm was running and a Sharepoint job re-discovery returns a 0 or 1 and the policy file list is empty. Examine the nbjm unified log (originator ID 117) for more detail on the cause of the error.

For NetBackup Snapshot Client only:

In an off-host backup (**NetBackup Media Server** or **Third-Party Copy Device**), code 69 may indicate that the file list contains the ALL_LOCAL_DRIVES entry. NetBackup does not support the ALL_LOCAL_DRIVES entry for off-host backup. Remove the ALL_LOCAL_DRIVES entry from the file list.

For the Enterprise Vault Agent only:

See the Troubleshooting section of the *NetBackup for Enterprise Vault Agent Administrator’s Guide*.

**NetBackup status code: 70**

**Message:** an entry in the filelist expanded to too many characters

**Explanation:** The wildcards, which were used in one of the file list entries, specified too many files.

**Recommended Action:** Change the wildcards in the file list to specify fewer files.

**NetBackup status code: 71**

**Message:** none of the files in the file list exist

**Explanation:** The files in the file list did not match any of the files on the client. This error can occur with only one file in the file list and the file cannot be backed up due to an I/O error.

**Recommended Action:** Do the following, as appropriate:

- Verify that the correct file list is specified for this client.

- On Windows clients, verify that the account used to start the NetBackup Client service has read access to the files.

  If you back up a network drive or a UNC (universal naming convention) path, do the following: use the Services application in the Windows Control Panel...
to verify that the NetBackup Client service does not start under the SYSTEM account. The SYSTEM account cannot access network drives.

To back up network drives or UNC paths: change the NetBackup Client service startup to log in as a user that has permission to access network drives.

- Check the All Log Entries report for clues.

- To set up debug logging, do one of the following:
  - On UNIX, Linux, and Windows clients, create a debug log directory for `bpbkar`.
  - On other PC clients except Macintosh, create a debug log directory for `bpcd` (the `bpcd` log is created automatically on Macintosh).

- Increase the amount of information that appears in the logs.
  See “How to set logging levels on UNIX clients” on page 116.
  See “How to set logging levels on PC clients” on page 120.

- Retry the operation and check the resulting debug logs.

- On Novell systems, do one of the following:
  - For the nontarget version of NetBackup for NetWare, the backup policy type must be "NetWare," and the files list should include a forward slash (/) only. There should be nothing else in the files list.
    To check the policy type and files list, start Backup Policy Management and right-click the name of a policy. Click the Attributes tab to check the policy type; click the Files tab to check the contents of the files list.
  - For the target version, the backup policy type must be "Standard," and the policy files list must be formatted as follows: `/target_name` where a forward slash precedes the variable `target_name`.
    To check the policy type and files list, start Backup Policy Management and right-click the name of a policy. Click the Attributes tab to check the policy type; click the Files tab to check the contents of the files list.
    For the target version, the following NetWare message may be another indicator of incorrect policy type (this message appears in the Novell client’s bpcd log):
    ```
    unable to connect to service, scheduled access not specified
    ```
    Make sure the policy type is set to "Standard."
  - For either the target or the nontarget version of NetBackup for NetWare, make sure that the following are all at the same version: the NetWare loadable modules (NLMs) SMDR and TSAxxx (such as TSAFS and TSANDS).
    If they are not at the same version, status 71 may occur.
NetBackup status code: 72
Message: the client type is incorrect in the configuration database
Explanation: The policy type attribute in the policy configuration indicates that the client is one type, but the installed software is for another type.
Recommended Action: Verify that the policy type attribute for the policy is correct.

NetBackup status code: 73
Message: bpstart_notify failed
Explanation: The bpstart_notify script returned a nonzero exit code.
Recommended Action: Check the bpstart_notify script on the client to see if it performs as expected.

NetBackup status code: 74
Message: client timed out waiting for bpstart_notify to complete
Explanation: The bpstart_notify script on the client takes too long.
Recommended Action: Try to speed up the bpstart_notify script or set the BPSTART_TIMEOUT on the server to a value that is larger than the default. Set BPSTART_TIMEOUT in the bp.conf file on a UNIX or Linux NetBackup server. On a Windows NetBackup server, use Host Properties to set Backup Start Notify Timeout.

See “Using the Host Properties window” on page 60.

NetBackup status code: 75
Message: client timed out waiting for bpend_notify to complete
Explanation: The bpend_notify script on the client takes too long.
Recommended Action: Try to speed up the bpend_notify script or set the BPEND_TIMEOUT on the server to a value that is larger than the default. Set BPEND_TIMEOUT in the bp.conf file on a UNIX or Linux NetBackup server. On a Windows NetBackup server, use Host Properties to set Backup End Notify Timeout.

NetBackup status code: 76
Message: client timed out reading file
Explanation: A fifo was specified in the file list and no data was produced on the fifo within the allotted time.
**Recommended Action:** Make sure that the process that is to produce the data on the named fifo is started correctly. Add an entry to the /usr/openv/netbackup/bp.conf file on the server to set CLIENT_READ_TIMEOUT to a larger value than the default.

**NetBackup status code: 77**

**Message:** execution of the specified system command returned a nonzero status

**Explanation:** An immediate command returned a nonzero status.

**Recommended Action:** Do the following, as appropriate:

- Verify that the command is specified correctly.

- For NetBackup Snapshot Client only, do the following: The policy file list may contain the files that do not reside within a file system that was designated as the snapshot source. To apply a snapshot method to the backup of individual files, the snapshot source must be a file system. (It cannot be a raw partition or Volume Manager volume.) The files in the policy file list must reside within that file system.

- Run the command manually to see if the wanted result is produced.

- For detailed troubleshooting information, set up debug logging, as follows:
  - On UNIX, Linux, and Windows clients, create a debug log directory for bpbkar.
  - On other PC clients except Macintosh, create a debug log directory for bpcd (the bpcd log is created automatically on Macintosh).
  - Increase the amount of information that appears in the logs. See “How to set logging levels on UNIX clients” on page 116. See “How to set logging levels on PC clients” on page 120.
  - Retry the operation and check the resulting debug log.

**NetBackup status code: 78**

**Message:** afs/dfs command failed

**Explanation:** Indicates an AFS vos command failure.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems Report for additional information on why the command failed.

- The bpbkar debug log shows the command that was run. Create a debug log directory for bpbkar. Retry the operation and retry the resulting debug log.
Try running the vos command manually to duplicate the problem.

**NetBackup status code: 79**

**Message:** unsupported image format for the requested database query

**Explanation:** One or more of the images to be synthesized was encrypted. These images cannot be synthesized.

**Recommended Action:** Ensure that none of the images was encrypted.

**NetBackup status code: 80**

**Message:** Media Manager device daemon (ltid) is not active

**Explanation:** If the server is UNIX or Linux, the NetBackup device manager daemon, ltid, is not running. If the server is Windows, the NetBackup Device Manager service is not running.

**Recommended Action:** Do the following, as appropriate:

- On Windows, use the Activity Monitor or the Services application in the Windows Control Panel to see if the NetBackup Device Manager service is running. If it is not running, start it. To enable verbose logging, place VERBOSE on a line by itself in the install_path\Volmgr\vm.conf file before you start the service.

- On UNIX and Linux, use vmps to see if ltid is running and if necessary start ltid in verbose mode with the following command:

  ```
  /usr/openv/volmgr/bin/ltid -v
  ```

  Or, add a VERBOSE entry to the /usr/openv/volmgr/vm.conf file. Create the vm.conf file if necessary.

- On UNIX and Linux, check the system logs to verify that ltid starts.

**Note:** On UNIX and Linux systems, ltid, and on Windows systems, the NetBackup Device Manager service, is used only if devices are attached to the system.

**NetBackup status code: 81**

**Message:** Media Manager volume daemon (vmd) is not active

**Explanation:** The tape manager (bptm) did not communicate with the NetBackup Volume Manager (vmd). This communication is required for most operations.
**Recommended Action:** On UNIX and Linux, verify that the Media Manager device daemon (`ltid`) and the NetBackup Volume Manager (`vmd`) are running. Start them if necessary.

On Windows, verify that both the NetBackup Device Manager service and the NetBackup Volume Manager service are running. Start them if necessary.

---

**Note:** `ltid` or the NetBackup Device Manager service is used only if devices are attached to the system.

---

**NetBackup status code: 82**

**Message:** media manager killed by signal

**Explanation:** Another process or a user terminated the tape manager (`bptm`) or disk manager (`bpdm`).

**Recommended Action:** This error should not occur in normal operation. If you want to terminate an active backup, use the NetBackup Activity Monitor.

When you back up a DomainOS client, this error occurs after the server has not received anything on the socket for at least 300 seconds. It causes a client read timeout and breaks the connection. The `bpbkar` debug log has an entry similar to the following:

```
Connection reset by peer (UNIX/errno status)
```

To resolve the problem, increase the `CLIENT_READ_TIMEOUT` value. In this instance, set the value to 900.

---

**NetBackup status code: 83**

**Message:** media open error

**Explanation:** The tape manager (`bptm`) or disk manager (`bpdm`) did not open the device or file that the backup or restore must use.

**Recommended Action:** For additional information, check the following:

- NetBackup Problems report
- Event Viewer Application log (Windows)
- System log (UNIX and Linux)
- Typically, this status code indicates a drive configuration problem that allows more than one process at a time to open the device. On UNIX and Linux, the problem may be due one or more of the following:
■ Two (or more) devices were configured that are the same physical device (for different densities perhaps). Verify that none of the /dev files that were used for these devices have the same major or minor numbers.

■ Links exist in the file system that allow users access to the drives.

■ The configuration for the drives was modified (in the administrator interface or vm.conf) and the Media Manager device daemon, ltid, was not restarted. Verify the configuration and then start ltid.

On Windows, the problem may be that the Media and Device Management device configuration was modified but the NetBackup Device Manager service was not restarted. Verify the configuration and restart the NetBackup Device Manager service.

■ On Windows, make sure the tapes are not write protected.

■ For detailed troubleshooting information:
  ■ Create a debug log directory for bpdm (if the device is disk) or bptm (if the device is tape).
  ■ On UNIX and Linux, restart ltid in the verbose mode by running the following:

  /usr/openv/volmgr/bin/ltid -v

  Or, add a VERBOSE entry to the /usr/openv/volmgr/vm.conf file. Create the vm.conf file if necessary.

  ■ On Windows, enable verbose logging by adding VERBOSE on a line by itself in the install_path\Volmgr\vm.conf file. Then, stop and restart the NetBackup Device Manager service.

  ■ Retry the operation and check the resulting debug log files.

  ■ On Windows systems, look at the install_path\VERITAS\NetBackup\db\media\errors log for a drive that frequently produces errors.
  
  On UNIX and Linux systems, look at the /usr/openv/netbackup/db/media/errors log (which is also included in the /usr/openv/netbackup/bin/goodies/support/support script output) for a drive that frequently produces errors.

NetBackup status code: 84

Message: media write error

Explanation: The system’s device driver returned an I/O error while NetBackup wrote to removable media or a disk file.
**Recommended Action:** Do the following, as appropriate:

- **For NetBackup Snapshot Client only:**
  If the following message appears in the `/usr/openv/netbackup/bptm` log, and the values for `key, asc, and ascq` are all zero (0x0) as shown in this example message:

  ```
tape error occurred on extended copy command, key = 0x0, asc = 0x0, ascq = 0x0
  ```

  your host-bus adapter and its driver are probably not supported by NetBackup Snapshot Client. The host-bus adapters supported in the release are listed in the *NetBackup Release Notes*.

- **For additional information, check the following:**
  - NetBackup Problems report to determine the device or media that caused the error
  - System and error logs for the system (UNIX and Linux)
  - Event Viewer Application and System logs (Windows)

- If NetBackup writes backups to a disk file, verify the following: the fragment size that is configured for the disk storage unit is not greater than the maximum file size that the operating system specifies.

- On Windows, make sure the tapes are not write protected.

- If `bpbackupdb` was used to back up the NetBackup catalog to a disk path on a UNIX or Linux system, do the following:
  The image you try to write may be greater than the maximum file size that the operating system specifies. Tape files do not have this limit.

- If the media is tape, check for the following:
  - A defective or a dirty drive. Clean it or have it repaired (refer to the `tpclean` command for robotic drives).
  - The wrong media type. Verify that the media matches the drive type you use.
  - Defective media. If it is defective, use the `bpmedia` command to set the volume to the FROZEN state so it is not used for future backups.
  - Incorrect drive configuration. Verify the Media and Device Management and system configuration for the drive.
    For example, on UNIX and Linux the drive may be configured for fixed mode when it must be variable mode.
    See the *NetBackup Device Configuration Guide* for more information.
This configuration often results in the media being frozen with the message "too many data blocks written, check tape and drive block size configuration."
See “Troubleshooting frozen media” on page 62.

NetBackup status code: 85

**Message:** media read error

**Explanation:** The system device driver returned an I/O error while NetBackup reads from tape or a disk file.

**Recommended Action:** For additional information, check the following:

- NetBackup Problems report to determine the device or media that caused the error
- System and error logs for the system (UNIX and Linux)
- Event Viewer Application and System logs (Windows)
- Check for the following:
  - A defective or a dirty drive. Clean it or have it repaired (see the `tpclean` command for cleaning).
  - Incorrect drive configuration. Verify the Media and Device Management and system configuration for the drive.
  - Defective media. In this case, you may not be able to recover all the data on the media. Use the `bpmedia` command to set the volume to the FROZEN state so it is not used for future backups.
  - The wrong media type. Verify that the media matches the drive type you use.

NetBackup status code: 86

**Message:** media position error

**Explanation:** The system’s device driver returned an I/O error while NetBackup was positioning the tape media.

**Recommended Action:** For additional information, check the following:
NetBackup Problems report to determine the device or media that caused the error

System and error logs for the system (UNIX and Linux)

Event Viewer Application and System logs (Windows)

Check for the following:

- A defective or a dirty drive. Clean it or have it repaired (see the `tpclean` command for cleaning).

- Incorrect drive configuration. Verify the Media and Device Management and system configuration for the drive. For example, on UNIX and Linux, the drive may be configured for fixed mode when it must be variable mode. See the *NetBackup Device Configuration Guide* for more information.

- Defective media. In this case, some data may be lost. Use the `bpmedia` command to set the volume to the FROZEN state so it is not used for future backups. See “Troubleshooting frozen media” on page 62.

- The wrong media type. Verify that the media matches the drive type you use.

**NetBackup status code: 87**

**Message:** media close error

**Explanation:** The system’s device driver returned an I/O error while NetBackup closed a tape.

**Recommended Action:** For additional information, check the following:

- NetBackup Problems report to determine the device or media that caused the error

- System and error logs for the system (UNIX and Linux)

- Event Viewer Application and System logs (Windows)

- Check for the following:

  - A defective or a dirty drive. Clean it or have it repaired (see the `tpclean` command for cleaning).

  - Defective media. In this case, some data may be lost. Use the `bpmedia` command to set the volume to the FROZEN state so it is not used for future backups. See “Troubleshooting frozen media” on page 62.
NetBackup status code: 89

Message:  problems encountered during setup of shared memory

Explanation:  The NetBackup processes use shared memory for some operations. This status is returned when an error is encountered in the initialization of the shared memory by the operating system’s APIs.

Recommended Action:  Check for a shared memory problem. This error can occur if the system cannot allocate enough shared memory. It usually occurs with multiplexing, which increases the amount of shared memory required for the operation. An entry similar to the following may be seen in a NetBackup log or report:

```
    system cannot allocate enough shared memory
```

If you see this type of message, refer to your platform vendor documentation for instructions on how to increase shared memory on your system.

For older levels of Solaris: you may need to change one or more default System V Shared Memory settings to prevent jobs failing with "system cannot allocate enough shared memory," as follows.

- For Solaris 9, the default shminfo_shmmax value is 8 megabytes. You can place the following line in your /etc/system file to increase this setting. A value of 32 megabytes has been used in this example. Your system may require a greater value under some circumstances such as a high value for the NetBackup multiplexing parameter. According to Sun Microsystems documentation, setting this parameter to its maximum possible value has no side effects. (This parameter is not applicable to Solaris 10).

  ```
  set shmsys:shminfo_shmmax=33554432
  ```

- For Solaris 9, the default shminfo_shmmni value is 100. You can place the following line in your /etc/system file to increase this setting. The default value is usually sufficient for NetBackup. In some circumstances, such as installing a NetBackup media server on a large database server, this setting may need to be increased. A value of 220 has been used in this example. (This parameter is not applicable to Solaris 10).

  ```
  set shmsys:shminfo_shmmni=220
  ```

Note: If you modify any of these values in the /etc/system file, you must reboot the system with boot -r for the new settings to take effect.
Refer to your vendor documentation for detailed instructions on how to modify these values. Note that these shminfo parameters are not applicable to Solaris 10.

**NetBackup status code: 90**

**Message:** media manager received no data for backup image

**Explanation:** The tape manager (bptm) or disk manager (bpdm) received no data when it performed a backup, archive, or duplication. This error can occur for incremental backups where no data was backed up because no files have changed.

**Recommended Action:** Do the following, as appropriate:

- Check the All Log Entries report.
- For detailed debug information, create `bpdm` or `bptm` debug log directories on the server. If the client is Windows, also create a `bpbkar` debug log directory on the client. Retry the operation and check the resulting debug logs.
- For additional information, check the following:
  - NetBackup Problems report to determine the device or media that caused the error
  - System and error logs for the system (UNIX and Linux)
  - Event Viewer Application log (Windows)
- Verify the Media and Device Management and system configuration for the drive. For example, on UNIX and Linux, the drive may not be set for variable mode in a case where NetBackup requires that mode. Check the *NetBackup Device Configuration Guide* for drive configuration information.
- Verify that the Media and Device Management configuration for the backup device matches what is specified for the storage unit in the NetBackup policy.
- Verify that you use the correct media in the drive.
- For detailed debug information, create a `bpdm` or `bptm` debug log directory (whichever applies) on the server. If the client is Windows, also create a `bpbkar` debug log directory on the client. Retry the operation and check the resulting debug logs.
- If the error occurred during duplication or a Vault session that uses an Alternate Read Server to perform duplication, do the following: verify that the Alternate Read Server has access to the source media.
NetBackup status code: 91

Message: fatal NB media database error

Explanation: The tape manager (bptm) received an error while it read or updated its media catalog.

Recommended Action: Do the following, as appropriate:

- Check the All Log Entries report for more information.
- Check the NetBackup Media Lists report to see if the catalog is intact. If the catalog is not intact, you may want to reload it from the latest NetBackup catalog backup volume.
- Verify that the disk partition on which the catalog resides has enough space.
- If these actions do not explain the problem, check the NetBackup Problems report.
- For detailed troubleshooting information, create a bptm debug log directory on the server and retry the operation. Check the resulting debug log file.
- Contact customer support and send appropriate problem and debug log sections.

NetBackup status code: 92

Message: media manager detected image that was not in tar format

Explanation: When you performed a restore, the tape manager (bptm) or disk manager (bpdm) did not find a tar header at the offset it expected.

Recommended Action: Do the following, as appropriate:

- Perform a bpverify of the affected image to determine if it is written correctly.
- Check the NetBackup Problems report for additional information about the error.
- Verify the Media and Device Management and system configuration for the drive.
  For example, on some UNIX and Linux systems if you do not configure the drive for variable-mode block size writes, the following occurs: the backup images that write to the media produce this error when you attempt to restore the image.
  The following sequence of events occurs:

  - Backup succeeds
  - Verify succeeds
- **Restore fails**
  The `bptm` debug log shows an error similar to the following:

  00:58:54 [2304] <16> write_data: write of 32768 bytes indicated only 29696 bytes were written, errno = 0

  In this case, configure the drive for variable-mode block sizes and suspend the media that writes on that device.
  See the *NetBackup Device Configuration Guide*.
  The images that were written to those media may be restorable (platform dependent), but single file restores are almost guaranteed to fail. You can expire these media and regenerate the backups. Or you can attempt to duplicate the images on these media to another device and then expire the original copy.

- This error has occurred on re-labeled and value-added 8-mm tape drives where the drive’s micro code incorrectly processes a "forward space record" SCSI command.

- If the problem is not one of those discussed, create a debug log directory for either `bpdm` or `bptm` and retry the operation. Check the resulting debug log file.

### NetBackup status code: 93

**Message:** media manager found wrong tape in drive

**Explanation:** When you load a volume for a backup or restore, the tape manager (`bptm`) found a volume that loaded without the expected tape header. This error may mean that volumes in a robot are not in the slots that are indicated in the Media and Device Management volume configuration.

**Recommended Action:** Do the following, as appropriate:

- If the volume is in a robot and the robot supports bar codes, do the following:
  perform a Compare Contents with Volume Configuration (on Windows) or Compare robot contents with volume configuration (on UNIX and Linux). The resulting report shows the media ID that was found and validates its slot number with what is in the volume configuration. Then, either change the physical location in the robot or change the volume configuration to show the correct slot.

- If the volume was mounted on a nonrobotic drive, verify that the correct volume was mounted and assigned.

### NetBackup status code: 94

**Message:** cannot position to correct image
**Explanation:** The tape manager \( \text{bptm} \) searched for a backup image to restore but did not find the correct backup ID at the expected position on the volume. This error can indicate a drive hardware problem.

**Recommended Action:** Do the following, as appropriate:

- Try the restore on another drive if possible.
- For additional information, check the following:
  - NetBackup Problems report to determine the device or volume that caused the error
  - System and error logs for the system (UNIX and Linux)
  - Event Viewer Application and System logs (Windows)
- For detailed troubleshooting information, create a debug log directory for \( \text{bptm} \) and retry the operation. Check the resulting debug log files.

**NetBackup status code: 95**

**Message:** media id is not assigned to this host in the EMM database

**Explanation:** An operation was requested on a media ID for which NetBackup does not have a record assigned to the requesting server. An example of this is using \text{bpmedia} to suspend or freeze a media ID that does not exist or is not assigned to the requesting server.

**Recommended Action:** Run a NetBackup Media List report to determine the valid media IDs and their assigned hosts. Then, retry the command with a valid media ID and assigned host.

**NetBackup status code: 96**

**Message:** unable to allocate new media for backup, storage unit has none available

**Explanation:** The NetBackup resource broker \( \text{nbrb} \) did not allocate a new volume for backups. This error indicates that the storage unit has no more volumes available in the volume pool for this backup. Note that NetBackup does not change storage units during the backup.

**Recommended Action:** Check the NetBackup Problems report to determine the storage unit that is out of media.

- If the storage unit is a robot with empty slots, add more volumes (remember to specify the correct volume pool).
- If there are no empty slots, move some media to nonrobotic and then add new volumes.
- If you have difficulty keeping track of your available volumes, try the available_media script:
  
  On UNIX and Linux, this script is in:

  `/usr/openv/netbackup/bin/goodies/available_media`

  On Windows, the script is in:

  `install_path\NetBackup\bin\goodies\available_media.cmd`

  This script lists all volumes in the volume configuration, and augments that list with information on the volumes currently assigned to NetBackup.

- Set up a scratch volume pool as a reserve of unassigned tapes. If NetBackup needs a new tape and none are available in the current volume pool, it does the following: moves a tape from the scratch pool into the volume pool that the backup uses.

- If the storage unit and volume pool appear to have media, verify the following:
  - Volume is not FROZEN or SUSPENDED. Check for this condition by using the NetBackup Media List report. If the volume is frozen or suspended, use the `bpmedia` command to unfreeze or unsuspend it (if that is wanted).
    See “Troubleshooting frozen media” on page 62.
  - Volume has not expired or exceeded its maximum number of mounts.
  - The EMM database host name for the device is correct. If you change the EMM database host name, stop and restart the following: the Media Manager device daemon, `ltd`, (if the server is UNIX or Linux) or the NetBackup Device Manager service (if the server is a Windows system).
  - The correct host is specified for the storage unit in the NetBackup configuration. The host connection should be the server (master or media) with drives connected to it.
  - The Media and Device Management volume configuration has media in the correct volume pool. Unassigned or active media is available at the required retention level. Use the NetBackup Media List report to show the retention levels, volume pools, and status (active and so on) for all volumes. Use the NetBackup Media Summary report to check for active volumes at the correct retention levels.
The NetBackup `bptm` process is rejected when it requests media from the `vmd` process (UNIX and Linux) or the NetBackup Volume Manager service (Windows). The cause of this problem is that the process or service cannot determine the name of the host that makes the request.

This error can be due to an incorrect network configuration that involves the following:

- Multiple network interfaces
- `/etc/resolv.conf` on those UNIX or Linux systems that use it
- Running DNS with reverse addressing not configured

Create `bptm` and `vmd` debug log directories and retry the operation.

Examine the `bptm` debug log to verify that `bptm` connects to the correct system. If an error is logged, examine the `vmd` log.

On UNIX and Linux, the `vmd` log is:

```
/usr/openv/volmgr/debug/daemon/log.xxxxxx
```

On Windows, the `vmd` log is:

```
install_path\Volmgr\debug\daemon\xxxxxx.log
```

If this storage unit is new and this attempt to use it is the first, stop and restart NetBackup on the master server.

---

**Note:** The mds unified logging files (OID 143) usually show the NetBackup media selection process.

---

**NetBackup status code: 97**

**Message:** requested media id is in use, cannot process request

**Explanation:** An operation was requested on a media ID that is in use. An example of this operation is the attempt to suspend or freeze a volume while it is in use for a backup or restore.

**Recommended Action:** Retry the command when the volume is not in use. Use the Device Monitor to determine if the volume is in use.

**NetBackup status code: 98**

**Message:** error requesting media (tpreq)
**Explanation:** The tape manager (bpnm) received an error when they requested a media mount from the following: the NetBackup Device Manager service (on Windows) or the Media Manager device daemon (ltid) (on UNIX and Linux).

**Recommended Action:** Do the following, as appropriate:
- Check the NetBackup Problems report to determine the reason for the failure. The most common cause is that the NetBackup Device Manager service (on Windows) or the Media Manager device daemon (ltid) (on UNIX and Linux) is not running. Start it if necessary.
- If you duplicate backups or use Vault to duplicate backups, this error could indicate the following: the Alternate Read Server does not have access to the tape where the original backup resides.

**NetBackup status code: 99**

**Message:** NDMP backup failure

**Explanation:** The paths in your NDMP policy file list did not back up successfully.

**Recommended Action:** Check the NetBackup All Log Entries report for more information. A possible cause for this error is that none of the backup paths exist on the NDMP host.

**NetBackup status code: 100**

**Message:** system error occurred while processing user command

**Explanation:** A system call failure in bparchive, bpbackup, bplist, or bprestore.

**Recommended Action:** Do the following, as appropriate:
- Enable debug logging for bparchive, bpbackup, bplist, or bprestore (as appropriate) by creating debug log directories for them.
  On UNIX and Linux, if a nonroot user has problems, verify that the directory that was created has mode 666. Look for and correct any reported errors.
- Retry the operation and check the resulting logs.
  If the logs do not reveal the problem, use the command line version of the command and correct any problems that are reported on stderr.

**NetBackup status code: 101**

**Message:** failed opening mail pipe

**Explanation:** The process that attempts to send mail did not open the pipe to the server.
**Recommended Action:** Make sure that mail is configured on the client. For detailed troubleshooting information, create a `bpcd` debug log directory and retry the operation. Check the resulting `bpcd` debug log.

**NetBackup status code: 102**

**Message:** failed closing mail pipe

**Explanation:** The process that sends mail could not close the pipe to the server.

**Recommended Action:** Make sure that mail is configured on the client. For detailed troubleshooting information, create a `bpcd` debug log directory and retry the operation. Check the resulting `bpcd` debug log.

**NetBackup status code: 103**

**Message:** error occurred during initialization, check configuration file

**Explanation:** None

**Recommended Action:** None

**NetBackup status code: 104**

**Message:** invalid file pathname

**Explanation:** None

**Recommended Action:** None

**NetBackup status code: 105**

**Message:** file pathname exceeds the maximum length allowed

**Explanation:** The path name (built by using the current working directory) exceeds the maximum path length that the system allows.

**Recommended Action:** Shorten the current working directory path length.

**NetBackup status code: 106**

**Message:** invalid file pathname found, cannot process request

**Explanation:** One of the file paths to be backed up or archived is not valid.

**Recommended Action:** Verify that the full path names are used and that they do not exceed the maximum path length for the system. (On UNIX and Linux, they start with a slash character `/`.) Also, verify that the files exist and the permissions allow NetBackup to access them.
NetBackup status code: 108

Message: Action succeeded but auditing failed

Explanation: The primary action being audited has succeeded but the corresponding audit record has failed because it was never created.

For example, you use the `bppolicynew` command to create a policy and it returns status code 108. The policy is created successfully, but the associated audit record does not appear in the audit report that the `nbauditreport` command generates.

This error can be returned only if auditing is enabled using the `nbemmcmd` command.

Recommended Action: Do the following:

- Ensure that the `nbaudit` daemon (NetBackup Audit Manager) is running.
- **Recommended Action:** Examine the logs responsible for the primary action and the `nbaudit` logs for more details on the cause of the error. For example, check the `bpdbm` logs for policy creation.

NetBackup status code: 109

Message: invalid date specified

Explanation: This error can occur when you run a command on the command line that contains a date option. The format of a date option can vary depending on the locale of the master server.

Recommended Action: Do the following, as appropriate:

- If the error occurred on a command line, examine the standard error output from the command for an explanatory message.
- Refer to the format for the date options in the usage statement for the command. Look up the locale of the master server. Compare the date format of that locale with the date format on the usage statement for the command.
- Check the NetBackup Problems report for clues.
- If the error appears in a Java interface, enable the debug print manager in the Java startup file. Retry and compare the parameters that are logged in the Java log with the parameters listed in the command’s usage statement.
- If these actions do not reveal the problem, create a debug log directory for the process that returned this status code. Then retry the operation and check the resulting debug log.

NetBackup status code: 110

Message: Cannot find the NetBackup configuration information
**Explanation:** On Windows, NetBackup did not read the registry entries that were created during installation. On UNIX and Linux, the /usr/openv/netbackup/bp.conf file does not exist.

**Recommended Action:** On Windows, reinstall NetBackup software on the client. On UNIX and Linux, create a /usr/openv/netbackup/bp.conf file with at least the following lines:

```
SERVER = server_name
CLIENT_NAME = client_name
```

**NetBackup status code: 111**

**Message:** No entry was found in the server list

**Explanation:** On UNIX and Linux, the SERVER = server_name line is omitted from the bp.conf file. On Windows, the server list contains no entries.

**Recommended Action:** Do the following, as appropriate:

- On a UNIX and Linux client, add the following line to the top of the /usr/openv/netbackup/bp.conf file:

  ```
  SERVER = server_name
  ```

- On a Microsoft Windows or nontarget NetWare client, do the following: add the server name on the Server to use for backups and restores drop-down in the Specify NetBackup Machines and Policy Type dialog box. To display this dialog box, start the Backup, Archive, and Restore interface on the client. Then click Specify NetBackup Machines and Policy Type on the File menu.

- On a NetWare target client, add the server name to the bp.ini file.

- On a Macintosh client, add the SERVER = server_name line to the bp.conf file in the NetBackup folder in the Preferences folder.

**NetBackup status code: 112**

**Message:** no files specified in the file list

**Explanation:** A restore was requested with no files in the file list.

**Recommended Action:** Do the following, as appropriate:

- Specify at least one file to be restored.

- This status code may occur if nbjm is running and a stream discovery fails to find all stream files. Examine the nbjm unified log (originator ID 117) for more details on the cause of the error.
**NetBackup status code: 114**

**Message:** unimplemented error code

**Explanation:** This error should not occur. If nbjm received a negative error number, status 114 is issued.

**Recommended Action:** Examine the nbjm unified log (originator ID 117) for detailed information on the cause of the error.

**NetBackup status code: 116**

**Message:** VxSS authentication failed

**Explanation:** On either end of a socket connection, the parties did not mutually authenticate each other.

**Recommended Action:** Do the following, as appropriate:

- Ensure that the Symantec Product Authentication Service is installed and configured.
  For complete installation instructions, see the *NetBackup Security and Encryption Guide*.

- Check that both parties have a valid certificate. Examine the expiry date that is listed from `bpnbat -WhoAmI`. For example:

  ```
  bpnbat -WhoAmI
  Name: JDOG
  Domain: MYCOMPANY
  Issued by: /CN=broker/OU=root@machine1.mycompany.com/O=vx
  Expiry Date: Sep 19 12:51:55 2009 GMT
  Authentication method: Microsoft Windows
  Operation completed successfully.
  ```

  Shows an expiry date of September 19th, 2009. After 12:51:55 GMT this credential is no longer valid and a new credential is required.

- If you run from the NetBackup Administration console, close and reopen the console. The console automatically obtains a credential for the currently logged in identity, if possible. By default these certificates are valid for 24 hours. To set a longer default time, consult the *NetBackup Security and Encryption Guide*.

- Ensure the following: that the certificates for both sides use the same broker or are children of the same root broker and that trusts were established between them.
  See the *NetBackup Security and Encryption Guide* for more information on broker hierarchies and how to establish trust relationships between brokers.
- Ensure that connectivity between the physical systems in question is possible. If general sockets cannot connect between the machines (such as ping and telnet), issues within the network unrelated to NetBackup can cause this problem.

- Ensure that the system has sufficient swap space and the following directories are not full:
  - /home/username
  - /user/openv/netbackup/logs
  - /tmp

**NetBackup status code: 117**

**Message:** VxSS access denied

**Explanation:** The user identity that was used to attempt an operation does not have the permissions that are needed to perform the action.

**Recommended Action:** Do the following, as appropriate:

- If you use the default groups, make certain that the user attempts to perform an operation appropriate for that group. For example, a member of NBU_Operators is unable to modify policy information, which is a permission reserved for administrator roles.

- Ensure that the system has sufficient swap space and the following directories are not full:
  - /home/username
  - /user/openv/netbackup/logs
  - /tmp

- If you use your own defined groups and permissions, first determine the object with which the operation is associated. Then add the permissions relative to the action. For example, a user is required to up and down drives but currently does not have permission to do so. Verify that the user belongs to the correct authorization group.

  If necessary, verify that the group has Up and Down permissions on the Drive object within the Group Permission tab. If necessary, increase the verbosity level of NetBackup to locate what object and what permissions are required for the failing request. The pertinent lines in the debug logs look similar to the following:

  Name: JMIZZLE
In this example, the user JMIZZLE attempts to perform an operation that requires the Up permission on the Drives object. To diagnose the problem, examine the group(s) to which the user belongs to ensure that the appropriate group includes the Up permission. (Up is a member of the Operate permission set for Drives.)

**NetBackup status code: 118**

**Message:** VxSS authorization failed

**Explanation:** NetBackup was unable to complete the authorization check against the authorization service.

**Recommended Action:** Do the following, as appropriate:

- Ensure that the Symantec Product Authorization Service or daemon is running. Refer to the *NetBackup Security and Encryption Guide* for more information on authentication and authorization daemons.

- Ensure that you are in communication with the correct master server. Within the bp.conf files on the local server, verify that the entry AUTHORIZATION_SERVICES specifies the proper host name (fully qualified) of the authorization service. For example, `AUTHORIZATION_SERVICE = machine2.mycompany.com 0` specifies that the server contacts machine2 to perform authorization checks. Also ensure that this entry matches that of the master server.

- Ensure that the system has sufficient swap space and the following directories are not full:
  - `/home/username`
  - `/user/openv/netbackup/logs`
  - `/tmp`
Ensure that the server that contacts the master has a valid certificate. The machine certificate can be examined as follows:

For UNIX and Linux:

```
# bpnbat -WhoAmI -cf
/usr/openv/var/vxss/credentials/machine3.mycompany.com
```

For Windows:

```
Bpnbat WhoAmI -cf "c:\Program
Files\VERITAS\NetBackup\var\vxss\credentials\machine3.my
company.com"
```

Both of which would return:

- **Name**: machine3.mycompany.com
- **Domain**: NBU_Machines@machine2.mycompany.com
- **Issued by**: /CN=broker/OU=root@machine2.mycompany.com/O=vx
- **Expiry Date**: Sep 2 19:25:29 2004 GMT
- **Authentication method**: Symantec Private Security
- Operation completed successfully.

If the expiry date was exceeded, use `bpnbaz -LoginMachine` to obtain a new credential for the machine.

See the Netbackup Commands manual for more information on `bpnbaz`.

The server that attempts the check is not authorized to examine the authorization database. Ensure that `bpnbaz -ShowAuthorizers` re-tuned the machines identity. Ensure that the machine has a machine credential under the directory as follows:

- **Windows**: "Program Files\VERITAS\var\vxss\credentials"
- **UNIX and Linux**: `/usr/openv/var/vxss/credentials`

This credential should have the full name of the machine as in the following example: `machine1.company.com`.

Check that the maximum number of open sockets to the authorization database was not exhausted. Use `netstat` to determine the number of sockets that are opened to port 4032 on the authorization server and that refer to the following configurations:

- **Windows**: `HKLM\SOFTWARE\VERITAS\Security\Authorization\Communication\ClientMaxConnections`
- **UNIX and Linux**: `/etc/vx/vss/VRTSaz.conf` entry "ClientMaxConnections"

If the maximum number of open connections was reached, you may need to increase the number of maximum open connections. An increase in the number of open connections increases the memory footprint of the authorization
NetBackup status code: 120

Message: cannot find configuration database record for requested NB database backup

Explanation: The program that backs up the NetBackup internal catalogs did not find the attributes that indicate which media IDs to use or paths to back up. This error should not occur under normal circumstances.

Recommended Action: Do the following, as appropriate:

- Check the NetBackup Problems report for additional information about the error.
- For detailed troubleshooting information, create admin and bpdbm debug log directories and retry the operation. Check the resulting debug logs.
- Contact customer support and send the appropriate problem and debug log sections that detail the error.

NetBackup status code: 121

Message: no media is defined for the requested NB database backup

Explanation: When NetBackup attempted to back up its internal catalogs, no media IDs were defined in the catalog backup configuration.

Recommended Action: Add the media IDs to the catalog backup configuration. Verify that the media IDs are in the NetBackup volume pool.

NetBackup status code: 122

Message: specified device path does not exist

Explanation: The NetBackup internal catalogs were backed up in the following manner: by using the bpbackupdb command line and by specifying a device path (on Windows) or a raw device file (on UNIX and Linux) that does not exist.

Recommended Action: Retry the command by using a valid device file name.

NetBackup status code: 123

Message: specified disk path is not a directory

Explanation: When NetBackup attempted to back up its internal catalogs, the backup attributes were set to dump to a disk. However, the disk file path already exists and is not a directory.
**Recommended Action:** Specify a different disk path for the catalog backup or delete the file that already exists.

**NetBackup status code: 124**

**Message:** NB database backup failed, a path was not found or is inaccessible

**Explanation:** One or more of the specified paths in the catalog backup configuration were not backed up.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for additional information about the error.

  The following are some possible causes:

  - The path does not exist.
  - On a UNIX or Linux system, one of the paths contains a symbolic link.

  - After you determine which path cannot be accessed, correct the path names in the catalog backup configuration.

**NetBackup status code: 125**

**Message:** a NetBackup catalog backup is in progress

**Explanation:** Only one NetBackup catalog backup can be active at any given time. Certain operations are not allowed during an online catalog backup. (These include catalog archiving, catalog compression, and expiration of the last copy of an image.)

**Recommended Action:** Retry the operation after the catalog backup completes.

**NetBackup status code: 126**

**Message:** NB database backup header is too large, too many paths specified

**Explanation:** Too many paths were specified in the NetBackup catalog backup configuration to fit in a fixed-size media header. This error should not occur under normal circumstances.

**Recommended Action:** Delete some of the paths from the catalog backup configuration.

**NetBackup status code: 127**

**Message:** specified media or path does not contain a valid NB database backup header
**Explanation:** The `bprecover` command was issued and the media ID specified does not have valid catalog backup data.

**Recommended Action:** Validate that the correct media ID is used.

**NetBackup status code: 128**

**Message:** NB database recovery failed, a process has encountered an exceptional condition

**Explanation:** In the catalogs that were specified for recovery, one or more cannot be restored. For more detail, refer to the error message that precedes this status code in the output from the `bprecover` command.

**Recommended Action:** Do the following, as appropriate:

- Fix the problem that was reported in the error message in the `bprecover` output.
- Refer to one of the following topics to identify which NetBackup services to shut down before a NetBackup database recovery attempt:
  - See “Catalog recovery from an online backup” on page 589.
  - The NetBackup services should be shut down except for the NetBackup Client Service, which must be running for the database recovery to succeed.
- Check the NetBackup Problems report for additional information about the error.

The following are some possible causes:

- A disk may be full.
- The NetBackup catalog tape may be corrupt.

**NetBackup status code: 129**

**Message:** Disk storage unit is full

**Explanation:** As NetBackup writes to the file system for the disk storage unit, runs out of space. Until more file system space is available, images of similar size or larger may fail with this error when written to this disk storage unit.

In a scheduled backup job that writes to a storage unit group (which contains this disk storage unit), the following occurs: the NetBackup scheduler requests the storage unit with the greatest available capacity when the job is retried.

For the retry, when the scheduler requests the storage unit with the greatest available capacity, note the following:

- A tape storage unit in the storage unit group has preference over any disk storage units since tape storage units usually have more capacity.
If the storage unit with the most unused capacity is busy, NetBackup skips it. NetBackup then selects an available storage unit with the next largest, unused capacity.

If the storage unit with the greatest unused capacity is the one that lacked capacity when the job first failed, the scheduler tries it again. That storage unit may have more unused capacity now than it did when the job failed.

**Recommended Action:** Do the following, as appropriate:

- Either free sufficient space or add more space to the file system for this storage unit.
- Lower the high capacity mark for this disk storage unit. Configure the policies to access it through a storage unit group that provides alternative storage to use when this storage unit fills up. Ideally, if an image exceeds the file system’s high capacity mark, it also completes successfully. This image leaves the storage unit in a "full" state (over the high capacity mark). The storage unit then is not assigned to other jobs until its capacity falls under its high capacity mark.
- If the Staging attribute is set on the disk storage unit that did not have enough capacity, it may be unable to create free space. It cannot create space because the backups that are staged to the disk are not relocated (eligible to be deleted from the staging storage unit). Ensure that staging’s relocation (duplication) jobs successfully copy enough images to provide sufficient free space for new backups.

**NetBackup status code: 130**

**Message:** system error occurred

**Explanation:** An error occurred that prevents the product from operating in a consistent fashion. This error is usually related to a system call.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report for additional information about the error.
- Check the system log for reported problems.
- For detailed troubleshooting information, create `bpdm`, `bptm`, and `bprd` debug log directories on the master server. Increase the unified logging level by using the `vxlogcfg` command.
  
  See “Configuring and using unified logging” on page 93.
- Retry the operation and check the resulting debug logs.
NetBackup status code: 131

Message: client is not validated to use the server

Explanation: The client name, as determined from the connection to the server, did not match any client name in the NetBackup configuration. No altnames configuration for this client exists on the master server. A client and server with multiple network connections can encounter this problem in the following situation: the name by which the client is configured is not the one by which its routing tables direct connections to the server.

Recommended Action: Do the following, as appropriate:

- Examine the NetBackup Problems report.
- Create a debug log directory for bprd and retry the operation. Check the resulting debug log to determine the connection and the client names.
  Depending on the request type (restore, backup, and so on), you may need or want to do the following:
  - Change the client’s configured name.
  - Modify the routing tables on the client.
  - On the master server, set up an altnames directory and file for this client
    See the NetBackup Administrator’s Guide, Volume I.
    or
  - On a UNIX or Linux master server, create a soft link in the NetBackup image catalog.
  - See “Verifying host name and service entries” on page 48.

NetBackup status code: 132

Message: user is not validated to use the server from this client

Explanation: None

Recommended Action: None

NetBackup status code: 133

Message: invalid request

Explanation: One of two explanations exist.

- A request was made that is not recognized. This usually results from different versions of NetBackup software being used together.
If a client receives this error in response to a list or restore request, then the `DISALLOW_CLIENT_LIST_RESTORE` or `DISALLOW_CLIENT_RESTORE` option exists in the `bp.conf` file on the following: a UNIX or Linux NetBackup server or in the registry on a Windows NetBackup server. These options deny list and restore requests from all NetBackup clients.

**Recommended Action:** Do the following, as appropriate:

- If you suspect that the software versions are the problem, verify that all NetBackup software is at the same version level.
  - On UNIX and Linux NetBackup servers and clients, check the `/usr/openv/netbackup/bin/version` file.
  - On Windows NetBackup servers, check the `install_path\netbackup\version.txt` file or the About NetBackup item on the Help menu.
  - On Microsoft Windows clients, check the About NetBackup item on the Help menu.
  - On NetWare target clients, check the Version entry in the `bp.ini` file.
  - On Macintosh clients, check the version file in the bin folder in the NetBackup folder in the Preferences folder.

- If the server denies list and restore requests, remove the `DISALLOW_CLIENT_LIST_RESTORE` and `DISALLOW_CLIENT_RESTORE` options from the `bp.conf` file on the following: a UNIX or Linux NetBackup server or from the registry on a Windows NetBackup server. Then, stop and restart the NetBackup request daemon (UNIX and Linux) or NetBackup Request Manager service (Windows).

- For detailed troubleshooting information, create `bpdbm`, `bprd`, and `admin debug` log directories. Retry the operation and check the resulting debug logs.

---

**NetBackup status code: 134**

**Message:** unable to process request because the server resources are busy

**Explanation:** Status code 134 is an informational message that indicates that all drives in the storage unit are currently in use. If all drives are in use, NetBackup automatically tries another storage unit. If one is not available, NetBackup re-queues the job with a status of 134 and retries it later.

**Recommended Action:** None.

The 134 code is an informational message only and is not considered an error. It can occur for a number of reasons in normal operation. The 134 status code can occur more frequently in an SSO environment. No action is necessary.
A status 134 is not logged in the error logs. A 134 status causes a new try to appear in the Activity Monitor. It does not increase the retry count associated with the allowed number of retries.

**NetBackup status code: 135**

**Message:** client is not validated to perform the requested operation

**Explanation:** An alternate client restore was tried that did not come from the root user (on UNIX and Linux) or the administrator (on Windows).

**Recommended Action:** Retry the operation as a root user (on UNIX and Linux) or as an administrator (on Windows) on the master server. Also see status code 131.

**NetBackup status code: 136**

**Message:** tir info was pruned from the image file

**Explanation:** The TIR information was pruned from one or more of the component (differential or cumulative) backup images being synthesized.

This situation arises when the following occurs:

- The most recent backup image for the client is a synthetic full or cumulative backup
- The TIR information from one or more of the component images before the synthetic full (or cumulative) backup is pruned

The TIR information is automatically restored to the image catalog if you do the following: expire the synthetic backup (full or cumulative) image and try to rerun the synthetic backup job for the client. However, the synthetic backup job fails with this error if the TIR restore fails due to bad, missing, or vaulted media or a bad drive.

**Recommended Action:** Reimport the TIR information into the catalog of each component image (from which the TIR information was pruned). Then rerun the synthetic backup job. The TIR information can be imported into the image catalog by initiating a true image restore of any file from that component image. The restore process also restores the TIR information in the image catalog.

**NetBackup status code: 140**

**Message:** user id was not superuser

**Explanation:** A user or process that did not have root privileges (on UNIX and Linux) or administrator privileges (on Windows) started the process.
**Recommended Action:** If appropriate, give the user or the process administrator privileges (on Windows) or root privileges (on UNIX and Linux) and retry the operation.

**NetBackup status code: 141**

**Message:** file path specified is not absolute

**Explanation:** The file specification must be an absolute path.

**Recommended Action:** Correct the file specification and retry the command.

**NetBackup status code: 142**

**Message:** file does not exist

**Explanation:** To back up a VxFS file system with Snapshot Client, the VxFS file system on the client must be patched with correct, dynamically linked libraries. If the correct VxFS libraries are not installed, the backup fails with status 142.

The following appears in the log:

- For most snapshot backups, the following message appears in the 
  /usr/openv/netbackup/logs/bpfis log on the client:

  09:36:48.299 [527] <32> fs_dev_rt_check: FTL - snapshot method: 
  nbu_snap abort - required VxFS dynamic linked libraries for 
  NetBackup are not installed. Please visit the Symantec support 
  web site, and refer to Technote number 262225 for further 
  information.

- For the backups that run from a FlashBackup policy, the following appears in 
  the /usr/openv/netbackup/logs/bpbkar log on the client:

  abort - required VxFS dynamic linked libraries for NetBackup are 
  not installed. Please visit the Symantec support web site, and 
  refer to Technote number 262225 for further information. 
  status = 142: file does not exist
  10:09:56.573 [1146] <4> bpbkar Exit: INF - EXIT STATUS 142: file 
  does not exist

**Recommended Action:** Install the VxFS dynamic libraries on the NetBackup client as described in Technote 262225 and try the backup again.
NetBackup status code: 143
Message: invalid command protocol
Explanation: A poorly formed request was made to the NetBackup request daemon (UNIX and Linux) or to the Request Manager service (Windows). This error can be due to the following: mismatched versions of the product, corrupted network communication, or to a non-NetBackup process sending data across the port for the daemon or service.
Recommended Action: Examine the NetBackup error logs to determine the system that was the source of the data. On that system, determine the process that initiated the request. If it was a NetBackup process, verify that the process or command is compatible with the version of software on the server.

NetBackup status code: 144
Message: invalid command usage
Explanation: This status code is due to a NetBackup process being started with improper options or an incompatibility in the product.
Recommended Action: Either correct the command or verify that all NetBackup binaries are at the same version level.

NetBackup status code: 145
Message: daemon is already running
Explanation: Another copy of the process is running.
Recommended Action: Terminate the current copy of the process and then restart the process.

NetBackup status code: 146
Message: cannot get a bound socket
Explanation: The service or daemon did not bind to its socket. A system call fails when the daemon (UNIX and Linux) or service (Windows) attempts to bind to its configured port number. This error is usually caused when another process acquired the port before the daemon or service started.
Recommended Action: Do the following, as appropriate:
- Examine the NetBackup Problems and All Log Entries reports.
- Create bprd and bpdbm debug log directories and retry the operation. Check the resulting logs to see the system error message that resulted from the attempt.
If another process has the port, use other system commands to determine the process. Based on this research, either change the port number in your services file or map or terminate the process that acquired the port.

On UNIX and Linux, another possible cause for this error is the use of the kill command to terminate bprd or bpdbm. If you have to stop bprd, use the Terminate Request Daemon option on the Special Actions menu in bpadm. To stop bpdbm, use the `/usr/openv/netbackup/bin/bpdbm -terminate` command. Use of the kill command to stop these processes can leave them unable to bind to their assigned ports the next time they are started.

To identify a bprd or a bpdbm problem, look for lines similar to the following in the debug log for the respective process:

```
<16> getsockbound: bind() failed, Address already in use (114)
<32> listen_loop: cannot get bound socket. errno = 114
<4> terminate: termination begun...error code = 146
```

Similar entries can appear in the reports.

- If the problem persists longer than ten minutes, it may be necessary to restart the server.

**NetBackup status code: 147**

**Message:** required or specified copy was not found

**Explanation:** The requested copy number of a backup or an archive image cannot be found.

**Recommended Action:** Correct the request to specify a copy number that does exist.

**NetBackup status code: 148**

**Message:** daemon fork failed

**Explanation:** A NetBackup service did not create a child process due to an error that was received from the system. This error is probably an intermittent error that is based on the availability of resources on the system.

**Recommended Action:** Do the following, as appropriate:

- Restart the service at a later time and investigate the system problems that limit the number of processes.

- On Windows systems, check the Event Viewer Application and System logs.
NetBackup status code: 149
Message: master server request failed
Explanation: None
Recommended Action: None

NetBackup status code: 150
Message: termination requested by administrator
Explanation: The process terminates (or has terminated) as a direct result of a request from an authorized user or process.
Recommended Action: None.

NetBackup status code: 151
Message: Backup Exec operation failed
Explanation: The Global Data Manager console reported that a Backup Exec job (backup, archive, or restore) did not complete normally.
Recommended Action: Consult the Backup Exec job history on the Backup Exec server for details.

NetBackup status code: 152
Message: required value not set
Explanation: An incomplete request was made to the bpdbm process (on UNIX and Linux), or the NetBackup Database Manager service (on Windows). This error usually occurs because different versions of software are used together.
Recommended Action: Do the following, as appropriate:
- Verify that all software is at the same version level.
- For detailed troubleshooting information, create bpdbm and admin debug log directories and retry the operation. Check the resulting debug logs.

NetBackup status code: 153
Message: server is not the master server
Explanation: This status code is reserved for future use.
Recommended Action: None.
NetBackup status code: 154
Message: storage unit characteristics mismatched to request
Explanation: A backup was tried and the storage unit selected for use had the characteristics that were not compatible with the backup type.
Recommended Action: Verify that the characteristics of the selected storage unit are appropriate for the attempted backup.

- For a NetBackup Snapshot Client, the policy storage unit was set to Any_available and the off-host backup method was set to Third-Party Copy Device or NetBackup Media Server. Do not choose Any_available. A particular storage unit (such as nut-4mm-robot-t14-0) must be specified when Third-Party Copy Device or NetBackup Media Server is specified as the off-host backup method.

- For an NDMP policy type, verify the following: a storage unit of type NDMP is defined and the NDMP host value matches the host name of the client. For example, if the NDMP policy specifies toaster as the client, the configuration for the storage unit must specify toaster as the NDMP host.

- For a policy type other than NDMP, verify that the policy specifies a Media Manager or Disk type storage unit.

NetBackup status code: 155
Message: disk is full
Explanation: The write to the catalog file failed because the disk that contains the catalog database is full.
Recommended Action: Free up space on the disks where NetBackup catalogs reside and retry the operation.

NetBackup status code: 156
Message: snapshot error encountered
Explanation: The following are possible causes of this status code:

- An Enterprise Vault Agent related error. The following errors can result in a status code 156:
  - VSS_E_BAD_STATE snapshot error
  - VSS_E_INSUFFICIENT_STORAGE snapshot error

- A snapshot-backup related error regarding Windows Open File Backup or Snapshot Client.
Recommended Action: Do the following, as appropriate:

- **For the Enterprise Vault Agent:**
  See the Troubleshooting section of the *NetBackup for Enterprise Vault Agent Administrator’s Guide*.

- **For a Windows Open File Backup Snapshot Provider that uses VSS:**
  See the Troubleshooting section of one of the following guides:
  - *NetBackup for VMware Administrator’s Guide*
  - *NetBackup for Hyper-V Administrator’s Guide*
  - *NetBackup Snapshot Client Administrator’s Guide*

The VSS cache files may be too small for the number of files being backed up using VSS.

If `bpbkar debug` logs are turned on, a message similar to the following appears in the `bpbkar debug` log for the backup.

8:51:14.569 AM: [1924.2304] <4> tar_base::vTartMsgW: INF - tar message received from dos_backup::tfs_readdata
8:51:14.569 AM: [1924.2304] <2> tar_base::vTartMsgW: ERR - Snapshot Error while reading test.file
8:51:14.569 AM: [1924.2304] <4> tar_base::vTartMsgW: INF - tar message received from tar_backup::nextfile_state_switch
8:51:14.569 AM: [1924.2304] <2> tar_base::vTartMsgW: FTL - Backup operation aborted!
8:51:14.569 AM: [1924.2304] <2> tar_base::vTartMsgW: INF - Client completed sending data for backup

To increase the VSS cache size by using the Shadow Copy configuration in Windows 2003, do the following in the order listed:

- In Windows, right-click **My Computer** and select **Manage**.
- In the console tree, right-click **Shared Folders**, select **All Tasks**, and select **Configure Shadow Copies**.
- Select the volume where you want to make changes, and then select **Settings**.
In the Settings dialog box, change the **Maximum Size** setting to either of the following: No Limit or a size large enough to suit the requirements of your installation and your usage of VSS.

**For backups using Snapshot Client and the NAS_Snapshot method, with or without SnapVault:**

- If the backup fails with status code 156, consult the bpfis legacy log, in `/usr/openv/netbackup/logs` (UNIX and Linux) or `install_path\NetBackup\logs` (Windows). If the bpfis directory does not already exist, you must create it and rerun the job.
- If necessary, increase the logging level and retry the job.
- See “About using logs and reports” on page 79.

- On Windows clients, when restoring files from a backup that is made with the NAS_Snapshot method, log into the "NetBackup Client Service" as the Administrator account, not as the local system account. Otherwise, the backup fails with status 156.
- In Windows Services, double-click the NetBackup Client Service.
- Then check the Log On tab: if the service is not logged in as Administrator, stop the service.
- Change the login to the Administrator account and restart the service.
- Retry the restore.

**For other NetBackup Snapshot Client issues:**

- The file system that is specified as a snapshot source is not mounted. In this case, you may see the following in the `/usr/openv/netbackup/logs/bpfis` log:

```
17:12:51 bpfis: FTL - snapshot creation failed, status 156
17:12:51 bpfis: INF - EXIT STATUS 156: snapshot error encountered
```

and the following in the `/usr/openv/netbackup/logs/bpfis` log:

```
17:12:51 onlfi_vfms_logf: INF - cannot snap_on, err: 5
17:12:51 delete_mount_point: INF - Deleted mount point /tmp/__jody_test:20958
17:12:51 onlfi_freeze: FTL - VfMS error 11; see following messages:
17:12:51 onlfi_freeze: FTL - Fatal method error
```
17:12:51 onlfi_freeze: FTL - VfMS method error 5; see following message:
17:12:51 onlfi_freeze: FTL - nbu_snap_freeze: Cannot turn on snapshot; snapshot source=/opt, cache=/dev/rdsk/c1t3d1s0, snap error=5
17:12:51 onlfi_thaw: WRN - / is not frozen

Make sure that the file system that is specified for the snapshot source has been mounted.

- **The file system that is specified as the snapshot source does not correspond to the file system that contains the actual files (as opposed to symbolic links to the files).** The mounted file system for the snapshot source must contain the actual files, not symbolic links. If items in the file list, such as `/oracle`, is a symbolic link to `/export/home/oracle`, the snapshot source must specify `/export` or `/export/home`, not `/oracle`.

- **vxvm** is selected as the snapshot method but the snapshot source is not configured over a Veritas Volume Manager (VxVM) volume. In this case, you may see the following in the `/usr/openv/netbackup/logs/bpfis` log:

```
17:12:51 bpfis: FTL - snapshot creation failed, status 156
17:12:51 bpfis: INF - EXIT STATUS 156: snapshot error encountered
```

and something like the following in the `/usr/openv/netbackup/logs/bpfis` log:

```
17:12:51 onlfi_vfms_logf: INF - vxvm_freeze: Snapshot source /cockpit1 on device /dev/dsk/c1t0d0s6 is not on a VxVM volume
17:12:51 delete_mount_point: INF - Deleted mount point /tmp/_cockpit1_coc_group1:3518
17:12:51 onlfi_freeze: FTL - VfMS error 11; see following messages:
17:12:51 onlfi_freeze: FTL - Fatal method error
17:12:51 onlfi_freeze: FTL - VfMS method error 9; see following message:
17:12:51 onlfi_freeze: FTL - vxvm_freeze: Snapshot source /cockpit1 on device /dev/dsk/c1t0d0s6 is not on a VxVM volume
17:12:51 onlfi_thaw: INF - fim=vxvm
17:12:51 onlfi_thaw: WRN - /cockpit1 is not frozen
```

Make sure that the snapshot source is configured over a Veritas Volume Manager (VxVM) volume.
vxvm was selected as the snapshot method, but a Veritas Volume Manager snapshot mirror of the snapshot source volume had not been created before running the backup, or another backup is currently running that uses the snapshot mirror. In either case, you may see the following in the /usr/openv/netbackup/logs/bpfis log:

17:12:51 onlfi_freeze: FTL - VfMS error 11; see following messages:
17:12:51 onlfi_freeze: FTL - Fatal method error
17:12:51 onlfi_freeze: FTL - VfMS method error 3; see following message:
17:12:51 onlfi_freeze: FTL - find_ready_snapshot: Cannot find available snapshot mirror

Refer to the NetBackup Snapshot Client Administrator’s Guide for information on how to create a snapshot mirror on the client before you run the backup.

vxvm was selected as the snapshot method, and a Veritas Volume Manager snapshot mirror of the snapshot source volume has been created. However, two different backup jobs (A and B) try to back up the same volume (for example, vol01), but job A starts before job B. After an available snapshot mirror is found, a brief pause occurs before the snapshot is formed. Job B that runs slightly behind job A may try to create a snapshot of the snapshot mirror immediately before job A creates the snapshot and gets the lock on it.

In this case, you may see the following in the /usr/openv/netbackup/logs/bpfis log:

17:12:51 onlfi_freeze: FTL - VfMS error 11; see following messages:
17:12:51 onlfi_freeze: FTL - Fatal method error
17:12:51 onlfi_freeze: FTL - VfMS method error 3; see following message:
17:12:51 onlfi_freeze: FTL - vxvm_freeze: Command failed with status=11: /usr/sbin/vxassist -g rootdg snapshot vol01 VfMSCAAu7a4Uw </dev/null>/var/tmp/VfMSAAAs7a4Uw 2>/var/tmp/VfMSBAAt7a4Uw

The job that was unable to get a lock (job B in the preceding example) fails, and must be run again.
When using `nbu_snap` as a snapshot method, you may have stale snapshots if status code 156 occurs with the following messages in the 
`/usr/openv/netbackup/logs/bpfis` log. (Stale snapshots are those that `nbu_snap` did not automatically delete.)

```
17:12:51 onlfi_freeze: FTL - VfMS error 11; see following messages:
17:12:51 onlfi_freeze: FTL - Fatal method error
17:12:51 onlfi_freeze: FTL - VfMS method error 5; see following message:
17:12:51 onlfi_freeze: FTL - nbu_snap_freeze: Cannot turn on snapshot; snapshot source=/oracle/ufs_r, cache=/dev/rdsk/c4t1d11s4, snap error=11
```

- Look for stale snapshots by running the `snaplist` command when there are no active backups running. If the `snaplist` command shows cache entries, there are stale snapshots. Nothing is displayed if there are no stale snapshots.
  
  **Example snaplist output:**

  ```
  id ident size cached minblk err time
  43 6515 8390970 0 0 0 11/16/00 13:31:36
  device = /dev/rdsk/c1t6d0s0
  cache = /dev/rdsk/c1t6d0s7
  ```

- Use the `snapoff` command to remove the stale snapshot, as follows:

  ```
  /usr/openv/netbackup/bin/driver/snapoff id
  ```

  where `id` is the ID from the `snaplist` output (such as 43 in the preceding example).

- If a backup using the `VxFS_Checkpoint` snapshot method failed, the NetBackup `bpbkar` process should automatically remove the clone. Sometimes, however, `bpbkar` is unable to remove the clone. In this case, you may see messages such as the following in the `bpfis` log:

  ```
  15:21:45.716 [4236] <4> create_mount_point: INF - Created mount point /tmp/_vtrax_test:4236
  ```
15:21:45.869 [4236] <2> onlfi_vfms_logf: INF - vxfs clone handle: 9600344
15:21:45.870 [4236] <2> onlfi_vfms_logf: INF - VxFS_Checkpoint_freeze: Cannot create checkpoint; status=17
15:21:45.872 [4236] <4> delete_mount_point: INF - Deleted mount point /tmp/_vtrax_test:4236
15:21:45.873 [4236] <32> onlfi_freeze: FTL - VfMS error 11; see following messages:
15:21:45.873 [4236] <32> onlfi_freeze: FTL - Fatal method error was reported
15:21:45.873 [4236] <32> onlfi_freeze: FTL - VfMS method error 17; see following message:
15:21:45.874 [4236] <32> onlfi_freeze: FTL - VxFS_Checkpoint_freeze: Cannot create checkpoint; status=17

Remove the clone as follows.

**Note:** If the checkpoint is not removed, you cannot use **VxFS_Checkpoint** to back up any data in the file system where the checkpoint is mounted.

- List the name of the checkpoint by entering the following VxFS command:

  ```
  /usr/lib/fs/vxfs/fsckptadm list /file_system
  ```

  where `file_system` is the name of the file system where the checkpoint is mounted. A sample output follows. In this example, `/vtrax_test` is the file system and `fi_ckpt` is the name of the checkpoint.

  ```
  /vtrax_test
  fi_ckpt:
  ctime = Mon Nov 12 10:08:13 2001
  mtime = Mon Nov 12 10:08:13 2001
  flags = largefiles
  ```

- Remove the checkpoint by entering the following:

  ```
  /usr/lib/fs/vxfs/fsckptadm remove checkpoint /file_system
  ```

- If the checkpoint cannot be removed, unmount the checkpoint and retry the first step in this procedure.
If a snapshot backup fails using TimeFinder, ShadowImage, or BusinessCopy method, there may be a VxVM clone left over from a previous backup. You may see messages similar to the following in the /usr/openv/netbackup/logs/bpfis log:

```
19:13:07.686 [14981] <2> onlfi_vfms_logf: INF - do_cmd: Command failed with status=20: /usr/openv/netbackup/bin/bpdgclone -g wil_test -n vol01 -f /var/tmp/HDSTFCAAs7aOqD </dev/null >/var/tmp/VfMSAAAg7aOqD 2>/var/tmp/VfMSBAAr7aOqD
19:13:07.687 [14981] <2> onlfi_vfms_logf: INF - --- Dumping file /var/tmp/VfMSAAAg7aOqD (stdout):
19:13:07.687 [14981] <2> onlfi_vfms_logf: INF - --- End of file /var/tmp/VfMSAAAg7aOqD
19:13:07.687 [14981] <2> onlfi_vfms_logf: INF - clone group and volume already exists
```

NetBackup automatically creates VxVM clones for TimeFinder, ShadowImage, or BusinessCopy backups of data that is configured over volumes. After the backup has completed, NetBackup removes the VxVM clone. In this case, a system crash or restart may have prevented the removal. Remove the clone as follows.

(Do the following on the client or alternate client, depending on the type of backup.)

- When no backups are running, use the following VxVM command to list any clones: `vxdg list`
  The clone name is of the form `clone_disk_group_clone`.

- To remove the clone, enter the following:

  ```
  /usr/openv/netbackup/bin/bpdgclone -g disk_group -n volume -c
  ```

  For example:

  ```
  /usr/openv/netbackup/bin/bpdgclone -g wil_test -n vol01 -c
  ```

  where `wil_test` is the name of the disk group and `vol01` is the name of the VxVM volume.

  For more information on how to remove a VxVM clone, refer to the NetBackup Snapshot Client Administrator’s Guide. For `vxdg`, refer to the Veritas Volume Manager Administrator’s Guide.
Before running the backup again, resynchronize the primary disk with the secondary disk. For assistance, refer to the NetBackup Snapshot Client Administrator’s Guide.

If a snapshot backup fails using the FlashSnap or VVR snapshot method, a VxVM snapshot may be left over from a previous backup. You may see messages similar to the following in the /usr/openv/netbackup/logs/bpfis log:

```bash
14:41:15.345 [22493] <32> onlfi_freeze: FTL - VfMS error 11; see following messages:
14:41:15.345 [22493] <32> onlfi_freeze: FTL - Fatal method error was reported
14:41:15.345 [22493] <32> onlfi_freeze: FTL - VfMS method error 8; see following message:
14:41:15.345 [22493] <32> onlfi_freeze: FTL - vxvm__find_ready_snapshot: Cannot find available snapshot mirror
```

NetBackup automatically creates VxVM snapshots for backups of data that is configured over volumes. After the backup completes, NetBackup removes the VxVM snapshot. In this case, a system crash or restart may have prevented the removal. Remove the snapshot as follows.

For FlashSnap:
(Do the following on the client or alternate client, depending on the type of backup.)

Find the VxVM disk group:

```bash
vxdg list
```

The format of the disk group name is as follows:

```bash
primaryhost_diskgroup_split
```

If `vxdg list` does not show the disk group, the group might have been deported. You can discover all the disk groups, that includes deported ones, by entering:

```bash
vxdisk -o alldgs list
```

The disk groups that are listed in parentheses are not imported on the local system.

Deport the VxVM disk group:
Enter the following on the primary (original) client:

- **Import and join the VxVM disk group:**
  
  ```
  vxdg import primaryhost_diskgroup_split
  vxrecover -g primaryhost_diskgroup_split -m
  vxdg join primaryhost_diskgroup_split diskgroup
  ```

- **Start the volume and snap back the snapshot volume:**
  
  ```
  vxvol -g primaryhost_diskgroup_split start
  SNAP_diskgroup_volume
  vxassist snapback SNAP_diskgroup_volume
  ```

For VVR, on the alternate client:

- **Enter the following to display unsynchronized mirror disks:**
  
  ```
  vxprint -g diskgroup
  ```

- **Enter the following to resynchronize the mirror disks:**
  
  ```
  vxassist -g diskgroup -v volume snapback
  ```

When you use a snapshot method such as VxFS_Checkpoint to back up a Veritas File System (VxFS), the backup fails if the VxFS license has expired. Messages such as the following appear in the `/usr/openv/netbackup/logs/bpfis log`:

```
11:37:42.279 [24194] <2> onlfi_vfms_logf: INF - VxFS_Checkpoint_freeze: Cannot open checkpoint; status=100
11:37:42.283 [24194] <4> delete_mount_point: INF - Deleted mount point /tmp/_vrts_frzn_img__test1_24194
11:37:42.283 [24194] <32> onlfi_freeze_fim_fs: FTL - VfMS error
11; see following messages:
11:37:42.283 [24194] <32> onlfi_freeze_fim_fs: FTL - Fatal method error was reported
11:37:42.284 [24194] <32> onlfi_freeze_fim_fs: FTL - VfMS method error 100; see following message:
11:37:42.284 [24194] <32> onlfi_freeze_fim_fs: FTL - VxFS_Checkpoint_freeze: Cannot open checkpoint; status=100
```
Obtain a new VxFS license and retry the backup.

- If the backup is enabled for instant recovery with either the vxvm or VVR snapshot method, your VxVM mirrors may not be properly configured. In this case, you may see the following in the /usr/openv/netbackup/logs/bppfi log on the client (when verbose mode is set high).

```

13:43:39.512 [16375] <2> onlfi_vfms_logf: INF - 0 active plexes for /rootdg/pfi_concat: 0 are PFI 0 non-PFI
```

Configure the VxVM mirrors as described in the Instant Recovery chapter of the *NetBackup Snapshot Client Administrator’s Guide*.

- When you use the VxFS_Checkpoint snapshot method, the backup fails if the client’s file system does not support mountable checkpoints using the Storage Checkpoint feature. Messages such as the following appear in the /usr/openv/netbackup/logs/bpfis log:

```
14:54:27.530 [23563] <32> onlfi_freeze_fim_fs: FTL - VfMS error 11; see following messages:
14:54:27.530 [23563] <32> onlfi_freeze_fim_fs: FTL - Fatal method error was reported
14:54:27.530 [23563] <32> onlfi_freeze_fim_fs: FTL - vfm_freeze: method: VxFS_Checkpoint, type: FIM, function:
VxFS_Checkpoint_freeze 14:54:27.531 [23563] <32> onlfi_freeze_fim_fs: FTL - VfMS method error 2; see following message:
```
Cannot open checkpoint on /mnt_vxvm/2G_concat: fsckpt_get_api_version returns 1; mountable checkpoints not supported with this version

Do one of the following:

- Upgrade the client file system to a version that supports mountable VxFS Storage Checkpoints
- Configure the policy with a snapshot method that supports the client’s current file system.

**NetBackup status code: 157**

**Message:** suspend requested by administrator

**Explanation:** Status code 157 is an informational message, which indicates that the administrator suspended the job from the Activity Monitor. The job is in the suspended state in the Activity Monitor. It can be resumed from the last checkpoint by the administrator.

**Recommended Action:** The administrator can resume the job from the last checkpoint from the Activity Monitor.

**NetBackup status code: 158**

**Message:** failed accessing daemon lock file

**Explanation:** The process cannot lock its lock file because an error was received from a system call. This lock file synchronizes process activities (for example, it prevents more than one daemon from running at a time).

**Recommended Action:** Do the following, as appropriate:

- Examine the NetBackup error log to determine why the system call failed. Then correct the problem. It may be a permission problem.

- If the error log does not show the error, create a debug log directory for bprd or bpdbm (depending on which process encountered the error). Increase the unified logging level if nbpem, nbjm, or nbrb encountered the error. Use the vxlogcfg command as explained in the following topic:
  
  See “Configuring and using unified logging” on page 93. Retry the operation and check the resulting debug log.

**NetBackup status code: 159**

**Message:** licensed use has been exceeded
**Explanation:** A configuration limit was exceeded.

For example, a job fails with this error code if a policy is set up that specifies the following:

- A storage unit that is on a SAN media server
- A client that is not the SAN media server itself

SAN media servers can only back up themselves.

This status code is used when the creation of a storage unit on a SAN media server fails because "On demand only" is not selected. "On demand only" is required for storage units on a SAN media server.

**Recommended Action:** To determine the cause of the error, examine the NetBackup All Log Entries report for the command that was ran. See also the Activity Monitor details for informative messages.

If the job fails on a SAN media server storage unit, ensure that only the local client is specified in the policy. If remote clients are specified in the policy, do one of the following: remove them and place them in a policy that specifies a different storage unit or change the storage unit for that policy.

If you want to back up remote clients by using the SAN media server, you can purchase a regular NetBackup media server license.

**NetBackup status code: 160**

**Message:** authentication failed

**Explanation:** NetBackup encounters a problem when two systems try to authenticate one another.

**Recommended Action:** Do the following, as appropriate:

- Ensure that the authentication libraries exist:
  - On Windows:
    ```
    install_path\NetBackup\lib\libvopie.dll
    install_path\NetBackup\lib\libvnoauth.dll
    ```
  - On UNIX and Linux (except HP-UX):
    ```
    /usr/openv/lib/libvopie.so
    /usr/openv/lib/libvnoauth.so
    ```
  - On UNIX and Linux (HP-UX only):
    ```
    /usr/openv/lib/libvopie.sl
    /usr/openv/lib/libvnoauth.sl
    ```
On Macintosh:

:System Folder:Extensions:libvopie.dll
:System Folder:Extensions:libvnoauth.dll

- Check the methods_allow.txt files on the systems that have problems to ensure that authentication is enabled. The files are in the following locations:
  - Windows: \install_path\NetBackup\var\auth
  - UNIX and Linux: /usr/openv/var/auth
  - Macintosh: :System Folder:Preferences:NetBackup::

One system may report authentication failure (status code 160) while the other system reports that a network connection timed out (status code 41). In this case, authentication may be enabled in the methods_allow.txt file on the first system but not on the second system.

- On the systems with the authentication problem, remove the remote host that is not authenticated from the methods_allow.txt file.
  For example, if host A and host B have the problem, remove host A from the file on host B and vice versa.
  Retry the operation. If the problem still exists, it indicates that connection problems are not related to authentication. If connections are now successful, proceed to the next step.

- Run bpauthsync -vopie on the master server to synchronize the key files again on the systems.
  On Windows:

  \install_path\NetBackup\bin\admincmd\bpauthsync -vopie
  -servers -clients

  On UNIX and Linux:

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

- Add back the names that were removed and retry the operation.

- Create debug log directories for the processes that are involved in authentication between NetBackup systems. These include:
  - On the server, create debug log directories for bprd, bpdbm, bpcd.
  - On the client, create debug log directories for bpbackup, bprestore, bpbkar (Windows only).

  Retry the operation and check the logs.
NetBackup status code: 161

**Message:** Evaluation software has expired.

**Explanation:** The time that was allowed for the NetBackup evaluation software ended.

See www.symantec.com for ordering information.

**Recommended Action:** Obtain a licensed copy of NetBackup.

NetBackup status code: 162

**Message:** incorrect server platform for license

**Explanation:** The platform identifier in the license key does not match the platform type on which the key was installed.

**Recommended Action:** Ensure that you use a license key that is intended for the platform on which you plan to install.

NetBackup status code: 163

**Message:** media block size changed prior resume

**Explanation:** Status code 163 is an informational message. It indicates that the media block size was changed before a backup job from the last checkpoint resumed. Since the media block size must be consistent, the job was restarted from the beginning.

**Recommended Action:** Check the Activity Monitor job details for the job ID of the restarted job.

NetBackup status code: 164

**Message:** unable to mount media because it is in a DOWN, or otherwise not available

**Explanation:** A restore was tried and the volume required for the restore was in a DOWN drive in a robot. Or, the slot is empty that should contain the volume.

**Recommended Action:** Do the following, as appropriate:

- If volume is in a DOWN drive, remove it and place it in its designated slot. Then, retry the restore.

- If the volume is in the wrong slot, use a robot inventory option to reconcile the contents of the robot with the volume configuration.
NetBackup status code: 165

**Message:** NB image database contains no image fragments for requested backup id/copy number

**Explanation:** A restore was tried and NetBackup has no record of the fragments that are associated with the backup ID that has the files.

**Recommended Action:** Check the NetBackup Problems report for additional information about the error. For detailed troubleshooting information, create a debug log directory for either `bpdm` or `bptm` (whichever applies) and retry the operation. Check the resulting debug log.

NetBackup status code: 166

**Message:** backups are not allowed to span media

**Explanation:** An end of media (EOM) was encountered while the backup image was written. The backup was terminated because the NetBackup `DISABLE_BACKUPS_SPANNING_MEDIA` option was present in `bp.conf` (on UNIX and Linux) or in the registry (on Windows). The backup is retried automatically with a different volume if the backup tries attribute allows it in the NetBackup global attribute configuration.

**Recommended Action:** None.

NetBackup status code: 167

**Message:** cannot find requested volume pool in EMM database

**Explanation:** A backup to a nonrobotic drive was tried and the tape manager (`bptm`) cannot find or add the specified volume pool.

**Recommended Action:** Verify the Media and Device Management volume configuration. Check the NetBackup Problems report for more information about the error. For detailed troubleshooting information, create a `bptm` debug log directory and retry the operation. Check the resulting debug log.

NetBackup status code: 168

**Message:** cannot overwrite media, data on it is protected

**Explanation:** A catalog backup was tried to a volume that cannot be overwritten because it contains data that by default NetBackup does not overwrite. (This data includes items such as tar, cpio, and ANSI.)

**Recommended Action:** Replace the volume with a new one or set the NetBackup `ALLOW_MEDIA_OVERWRITE` option to the appropriate value.
NetBackup status code: 169

**Message:** media id is either expired or will exceed maximum mounts

**Explanation:** A backup or a catalog backup was tried and the volume selected for use has reached its maximum number of mounts. The maximum number is specified in the Media and Device Management volume configuration. For a regular backup, the volume is automatically set to the SUSPENDED state and not used for further backups. For a NetBackup catalog backup, the operation terminates abnormally.

**Recommended Action:** If the volume was suspended, wait until it expires and then replace it. For NetBackup catalog backups, replace the media.

NetBackup status code: 170

**Message:** third party copy backup failure

**Explanation:** Usually indicates a problem with the 3pc. file or the mover.conf file. (For detailed causes, see recommended actions.)

For more information on these files, refer to the *NetBackup Snapshot Client Configuration online document*.

For help accessing this document, see "Snapshot Client Assistance" in the *NetBackup Snapshot Client Administrator’s Guide*.

**Recommended Action:** Do the following, as appropriate:

- If a non third-party copy device is listed in 3pc. file, correct it or remove the non third-party copy device entry.
- If an incorrect lun is specified in the 3pc. file or the device does not exist, correct the 3pc. file as appropriate.
- If an appropriate mover.conf file (with or without file name extension) cannot be found, the /usr/openv/netbackup/logs/bptm log may show the following:

```
09:51:04 [22281] <2> setup_mover_tpc: no mover.conf.vertex_std_tpc or mover.conf file exists, cannot perform TPC backup
09:51:04 [22281] <16> bptm: unable to find or communicate with Third-Party-Copy mover for policy vertex_std_tpc
```

Make sure that an appropriate mover.conf file exists in /usr/openv/netbackup on the media server. This file can be any of the following:

- mover.conf.policy_name file, where policy_name exactly matches the name of the policy.
mover.conf.storage_unit_name, where storage_unit_name exactly matches the name of the storage in the Backup Policy Management Policy attributes dialog box (such as nut-4mm-robot-tl4-0).

mover.conf file (no extension) for the configurations that have only one third-party copy device.

Note that NetBackup looks for an appropriate mover.conf file in the order.

If the SCSI pass-through path of the third-party copy device, as entered in the mover.conf file, does not exist, the bptm log may show the following:

09:50:12 [22159] <16> setup_mover_tpc: open of passthru path /dev/sg/cXtXlX failed, No such file or directory
09:50:12 [22159] <16> bptm: unable to find or communicate with Third-Party-Copy mover for policy vertex_std_tpc

Correct the SCSI pass-through path of the third-party copy device that is entered in the mover.conf file.

If the third-party copy device returned an error, you may see either of the following messages in /usr/openv/netbackup/logs/bptm log:

cannot process extended copy error due to truncated sense data, may be HBA problem
disk error occurred on extended copy command, key = 0x0, asc = 0x0, ascq = 0x0

(where key, asc, and ascq are all zero)

Your host-bus adapter (HBA) and its driver may need to be updated, or NetBackup Snapshot Client may not support them. The supported host-bus adapters are listed.

See the NetBackup Release Notes.

NetBackup status code: 171

Message: media id must be 6 or less characters

Explanation: operation, such as using bpmedia to suspend or freeze a media ID, was tried and the media ID specified was longer than six alpha-numeric characters

Recommended Action: Retry the command with a valid media ID.

NetBackup status code: 172

Message: cannot read media header, may not be NetBackup media or is corrupted
Explanation: When you loaded a volume for a backup or restore, the tape manager (bptm), did not find the expected tape header. This error can mean that a robotic device volume is not in the slot number that is in the Media and Device Management volume configuration. It also can mean that a read error (I/O error) occurred.

Recommended Action: Do the following, as appropriate:

■ If the volume is in a robot that supports bar codes, verify the robot contents by using a robot inventory option.

■ If the volume was mounted on a nonrobotic drive, verify that the correct volume was mounted and assigned.

■ Check the NetBackup Problems report. If it shows a fatal read error, try the operation again with another drive, if possible.

■ If your configuration has multiple servers or HBAs with access to your tape services, make sure the SCSI Reserve or Release is configured correctly. (Most likely, the tape services configuration is an SSO configuration.)

For more information, refer to the *NetBackup Shared Storage Guide*.

NetBackup status code: 173

Message: cannot read backup header, media may be corrupted

Explanation: When the tape manager (bptm) searches for a backup image to restore, the following occurs: it cannot find the correct backup ID at the position on the media where NetBackup expected it. This status code can indicate a drive hardware problem.

Recommended Action: Do the following, as appropriate:

■ Check the NetBackup Problems report for clues as to what caused the error.

■ Try the restore on another drive if possible.

■ For detailed troubleshooting information, create a debug log directory for bptm and retry the operation. Check the resulting debug log.

NetBackup status code: 174

Message: media manager - system error occurred

Explanation: An abnormal condition caused a tape manager (bptm) or disk manager (bpdm) failure.

Recommended Action: Do the following, as appropriate:
Check the NetBackup Problems report to see if it shows the cause of the problem. If you see a Problems report message similar to the following, save all logs and call &Company Name; customer support:

"attempted to write 32767 bytes, not a multiple of 512"

On UNIX and Linux, if this error occurs during a restore, the tape drive may be incorrectly configured. It may be configured to write in fixed length mode when it should write in variable length mode. Verify your drive's configuration by comparing it to what is recommended in the NetBackup Device Configuration Guide.

If your configuration incorrectly specifies fixed length mode, change it to variable length mode and suspend the media that were written on that device. The images that were written to those media may be restorable (platform dependent), but single file restores are likely to fail.

If the problem occurs with a particular client only, verify that the client binaries are correct, especially for bpcd.

If you can read or write any other images on this media, check the following reports for clues:

- Images on Media report
- Media Contents report

Verify the following:

- The media, by using the NetBackup image verify option.
- That you used the correct media type for the device.

Check the system or the console log for errors (on UNIX and Linux) or the Event Viewer Application log (on Windows).

For detailed debug information, create a debug log directory for either bptm or bpdm (whichever applies) and retry the operation. Check the resulting debug log.

On UNIX and Linux, if the bptm debug log shows an error similar to the following, the tape drive is configured to write in fixed length mode rather than variable length mode:

```
00:58:54 [2304] <16> write_data: write of 32768 bytes indicated only 29696 bytes were written, errno = 0
```

The image being written encountered the end-of-media.

If the backup was configured for an OpenStorage disk storage unit, the OpenStorage vendor's plug-in may not be installed on all media servers in the
storage unit’s media server list. Either install the vendor plug-in on all of the media servers or remove from the list the servers that do not have the plug-in installed.

**NetBackup status code: 175**

**Message:** not all requested files were restored

**Explanation:** When the `bptm` or the `bpdm` process restores files from an image, it detected a fatal error condition and terminated the restore before it completed. Under normal circumstances, this error should not occur.

**Recommended Action:** Do the following, as appropriate:

- Check the NetBackup Problems report and the status log or the progress log on the client for additional information about the error
- For detailed troubleshooting information, create a debug log directory for either `bptm` or `bpdm` (whichever applies) and retry the operation. Check the resulting debug log.

**NetBackup status code: 176**

**Message:** cannot perform specified media import operation

**Explanation:** The tape manager (`bptm`) detected an error condition when it tried to import a specific backup image.

Possible reasons for this error are as follows:

- Media ID is already active in the NetBackup media catalog on this server
- Media ID is not in the volume configuration
- Fatal tape manager (`bptm`) error occurred
- Total image was not obtained from Phase 1 of import
- The barcode and media ID do not match in the volume database. One possible reason for a mismatch is when using tapes previously written by a different barcode, labels are placed into an ACSLS library using a new barcode label. Another possible reason is when the administrator attempts to change the media ID field (using `vmchange`) to match the RVSN. When the inventory is updated, the barcode and media ID are synchronized.

**Recommended Action:** Check the NetBackup Problems report to find the exact cause of the failure and try the following:

- If the media ID is already active, duplicate all images on the original media ID to another volume. Then, manually expire the original media and redo the import.
If the media ID is not present in the volume configuration, add it.

If you received a fatal bptm error, verify that the following are active: the NetBackup Volume Manager (vmd) on UNIX and Linux or the NetBackup Volume Manager on Windows.

If the entire image is not present, perform import phase 1 on the media IDs that have the remainder of the image.

If the barcode and media ID are a mismatch, use a barcode label that matches the recorded media ID. Tapes can then be mounted in a drive with AVRD running so that the recorded media ID is displayed. Then, a barcode with that label needs to be placed on the tape.

NetBackup status code: 177

Message: could not deassign media due to Media Manager error

Explanation: The tape manager (bptm) cannot successfully unassign a media ID.

Recommended Action: Do the following, as appropriate:

- Check the NetBackup Problems report for the cause of the problem.
- Verify that the NetBackup Volume Manager (vmd) is active on UNIX and Linux or the NetBackup Volume Manager service is active on Windows.
- For detailed troubleshooting information, create a debug log directory for bptm and retry the operation. Check the resulting debug log.

NetBackup status code: 178

Message: media id is not in NetBackup volume pool

Explanation: NetBackup tried a backup of its catalogs and the media ID that was specified for the catalog backup was not in the NetBackup volume pool. Volumes for catalog backups must be in the NetBackup volume pool.

Recommended Action: Check the Media and Device Management volume configuration to verify that the media IDs are present and in the NetBackup volume pool.

NetBackup status code: 179

Message: density is incorrect for the media id

Explanation: An operation such as "list contents" was tried on an invalid media ID, such as a cleaning tape. Another possibility: a media ID in the NetBackup catalog backup configuration does not match the media type that was entered in the volume configuration.
**Recommended Action:** Check the volume configuration and the NetBackup catalog backup configuration and correct any problems found.

**NetBackup status code: 180**

**Message:** tar was successful

**Explanation:** tar returned a successful exit status.

**Recommended Action:** None.

**NetBackup status code: 181**

**Message:** tar received an invalid argument

**Explanation:** One of the parameters that was passed to tar was not valid.

**Recommended Action:** Do the following, as appropriate:

- On a UNIX or Linux client:
  - Ensure that the tar command in /usr/openv/netbackup/bin is the one provided by NetBackup. If you are in doubt, reinstall it.
  - Check /usr/openv/netbackup/bin/version on the client to verify that the client is running the correct level software. If the software is not at the correct level, update the software per the directions in the NetBackup release notes.

- On a Windows client, create a tar debug log directory, retry the operation, and check the log.

- On a Macintosh client, check the version file that is in the bin folder in the NetBackup folder in the Preferences folder. If the software is not at the correct level, install the correct software.
  
  See the *NetBackup Installation Guide for UNIX*.

**NetBackup status code: 182**

**Message:** tar received an invalid file name

**Explanation:** tar cannot write to the file that is specified with the -f parameter.

**Recommended Action:** Do the following, as appropriate:

- Create a bpcd debug log directory on the client (on a Macintosh, NetBackup creates the log automatically).

- On a Windows client, create a tar debug log directory.

- Increase the logging level on the client:
On a UNIX or Linux client, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.

On PC clients, increase the debug or log level. See “How to set logging levels on PC clients” on page 120.

Rerun the operation, check the resulting debug logs for the parameters that were passed to `tar` and call customer support.

**NetBackup status code: 183**

**Message:** `tar` received an invalid archive

**Explanation:** The data that was passed to `tar` was corrupt.

**Recommended Action:** Do the following, as appropriate:

- If the problem is with a UNIX or Linux client, create a `/usr/openv/netbackup/logs/tar` debug log directory on the client and rerun the operation.
- Check the `tar` debug log file for any error messages that explain the problem.
- Restart the client to see if it clears the problem.
- When you finish with your investigation of the problem, delete the `/usr/openv/netbackup/logs/tar` directory on the client.

- If the problem is with a Microsoft Windows, NetWare, or Macintosh client, do the following in the order presented:
  - Create a `bpcd` debug log directory on the client (on a Macintosh NetBackup creates the log automatically).
  - On a Windows client, create a `tar` debug log directory.
  - Increase the debug or log level. See “How to set logging levels on PC clients” on page 120.
  - Rerun the operation and check the resulting debug logs.
  - Restart the client to see if it clears the problem.

**NetBackup status code: 184**

**Message:** `tar` had an unexpected error

**Explanation:** A system error that occurred in `tar`.

**Recommended Action:** Do the following, as appropriate:
If the problem is with a UNIX or Linux client, create a 
/usr/openv/netbackup/logs/tar debug log directory on the client and rerun the operation.

- Check the tar debug log file for any error messages that explain the problem.
- Restart the client to see if it clears the problem.
- When you finish your investigation of the problem, delete the 
/usr/openv/netbackup/logs/tar directory on the client.

If the problem is with a Microsoft Windows, NetWare, or Macintosh client:

- Create a bpcd debug log directory on the client (on a Macintosh NetBackup creates the log automatically).
- Increase the debug or log level. 
  See “How to set logging levels on PC clients” on page 120.
- On a Windows client, create a tar debug log directory.
- Retry the operation and check the resulting debug logs.
- Restart the client to see if it clears the problem.

NetBackup status code: 185

Message:  tar did not find all the files to be restored

Explanation:  The tar file list contained files that were not in the image.

Recommended Action: Do the following, as appropriate:

- If the problem is with a UNIX or Linux client:
  - Enable bpcd debug logging by creating the 
    /usr/openv/netbackup/logs/bpcd directory on the client.
  - Rerun the operation, check the resulting bpcd log file for the parameters that were passed to tar, and call customer support.

- If the problem is with a Microsoft Windows, NetWare, or Macintosh client:
  - Create a bpcd debug log directory on the client (on a Macintosh NetBackup creates the log automatically).
  - Increase the debug or log level. 
    See “How to set logging levels on PC clients” on page 120.
  - On a Windows client, create a tar debug log directory.
  - Retry the operation.
Check the resulting debug logs for the parameters that were passed to \texttt{tar} and call customer support.

**NetBackup status code: 186**

**Message:** tar received no data  
**Explanation:** NetBackup did not send data to \texttt{tar}.  
**Recommended Action:** Do the following, as appropriate:

- Retry the operation and check the status or the progress log on the client for any error messages that reveal the problem.
- Verify that the tape is available and readable.
- Verify that the drive is in an UP state. Use the Device Monitor.
- For detailed troubleshooting information:
  - Create a \texttt{bp\_tm} debug log on the server.
  - On a Windows client, create a \texttt{tar} debug log.
  - Retry the operation and check the resulting debug logs.

**NetBackup status code: 189**

**Message:** the server is not allowed to write to the client’s filesystems  
**Explanation:** The client does not allow writes from the server.  
**Recommended Action:** Perform the following to perform restores or install software from the server.

- On a UNIX or Linux client, delete \texttt{DISALLOW\_SERVER\_FILE\_WRITES} from the \texttt{/usr/openv/netbackup/bp.conf} file.
- On a Microsoft Windows or NetWare nontarget client, select \texttt{Allow server-directed restores} on the General tab in the NetBackup Client Properties dialog box. To display this dialog box, start the Backup, Archive, and Restore interface on the client and select **NetBackup Client Properties** from the File menu.
- On a Macintosh client, delete \texttt{DISALLOW\_SERVER\_FILE\_WRITES} from the \texttt{bp.conf} file in the NetBackup folder in the Preferences folder.
- On a NetWare target client, set \texttt{ALLOW\_SERVER\_WRITE} to yes in the \texttt{bp.ini} file.

**NetBackup status code: 190**

**Message:** found no images or media matching the selection criteria
Explanation: A verify, duplicate, or import was tried and no images that matched the search criteria were found in the NetBackup catalog.

Recommended Action: Change the search criteria and retry.

NetBackup status code: 191

Message: no images were successfully processed

Explanation: A verify, duplicate, or import was tried and failed for all selected images.

Recommended Action: Do the following, as appropriate:

- Check the NetBackup Problems report for the cause of the error. To obtain detailed troubleshooting information, create an admin debug log directory and retry the operation. Check the resulting debug log.

- If the error was encountered during duplication of backups, check the duplication progress log to help determine the root cause of the problem.

- If a Vault job encountered the error responsible for the duplication, check the duplicate.log files in your sidxxx directories to determine the root cause:

  UNIX and Linux:
  /usr/openv/netbackup/vault/sessions/vault_name/sidxxx

  Windows:
  install_path\NetBackup\vault\sessions\vault_name\sidxxx

  (where xxx is the session ID)

NetBackup status code: 192

Message: VxSS authentication is required but not available

Explanation: On one side of a NetBackup network connection, the system requires VxSS authentication. On the other side of the connection, the other system is not configured to use VxSS. VxSS authentication is used with the NetBackup Access Control feature (NBAC). The connection was terminated because VxSS authentication cannot be completed.

Recommended Action: Make sure both systems are configured to use NetBackup Access Control VxSS authentication with each other. Or, make sure both systems are not configured to use VxSS with each other. The first thing to check is the Use VxSS Host properties value on each system. If one is configured for REQUIRED, the other must be configured for REQUIRED or AUTOMATIC. If one is configured for PROHIBITED, the other must be configured for PROHIBITED or AUTOMATIC.
See the NetBackup Administrator’s Guide, Volume I, for the following information: how to set the Access Control related host properties, and how to configure a system to use Access Control.

**NetBackup status code: 193**

**Message:** VxSS authentication is requested but not allowed

**Explanation:** On one side of a NetBackup network connection, the system requires VxSS authentication. The system on the other side of the connection is not configured to use VxSS. VxSS authentication is used with the NetBackup Access Control feature (NBAC). The connection has been terminated because VxSS authentication cannot be completed.

**Recommended Action:** Make sure both systems are configured to use NetBackup Access Control VxSS authentication with each other. Or, make sure both systems are not configured to use VxSS with each other. The first thing to check is the Use VxSS Host properties value on each system. If one is configured for REQUIRED, the other must be configured for REQUIRED or AUTOMATIC. If one is configured for PROHIBITED, the other must be configured for PROHIBITED or AUTOMATIC.

See the NetBackup Administrator’s Guide, Volume I, for the following information: how to set the Access Control related host properties how to configure a system to use Access Control.

**NetBackup status code: 194**

**Message:** the maximum number of jobs per client is set to 0

**Explanation:** The NetBackup Maximum jobs per client global attribute is currently set to 0. Set the value to 0 to disable backups and archives.

**Recommended Action:** To enable backups and archives, change the Maximum jobs per client value to the wanted nonzero setting. This attribute is on the Global NetBackup Attributes tab in the Master Server Properties dialog box.

See “Using the Host Properties window” on page 60.

**NetBackup status code: 195**

**Message:** client backup was not attempted

**Explanation:** A backup job was in the NetBackup scheduler but was not tried.

**Recommended Action:** Do the following, as appropriate:

- Retry the backup either immediately with a manual backup or allow the normal scheduler retries.
■ For additional information, check the All Log Entries report. For detailed troubleshooting information, increase the logging level for the diagnostic and debug logs for nbpem, nbjm, and nbrb.

Use the `vxlogcfg` command as explained in the following topic:

See “Configuring and using unified logging” on page 93.

After the next backup try, check the logs.

■ The following are some actions to perform:

■ Verify that the vmd and the l tid daemons (UNIX and Linux) or the NetBackup Volume Manager and NetBackup Device Manager services (Windows) are running.

■ Look for a problem in an earlier backup that made the media or the storage unit unavailable.

**NetBackup status code: 196**

**Message:** client backup was not attempted because backup window closed

**Explanation:** A backup or an archive operation that the backup scheduler queued was not tried because the backup window was no longer open.

**Recommended Action:** Do the following, as appropriate:

■ If possible, change the schedule to extend the backup window for this combination of policy and schedule so it does not occur again.

■ If the backup must be run, use the Manual Backup command on the Policy menu in the Backup Policy Management window to perform the backup. Manual backups ignore the backup window.

**NetBackup status code: 197**

**Message:** the specified schedule does not exist in the specified policy

**Explanation:** A user backup or archive request specified the exact policy and schedule to use when a backup is performed. The policy exists but does not contain the schedule.

■ On Microsoft Windows and NetWare nontarget clients, you can specify a policy or schedule on the Backups tab in the NetBackup Client Properties dialog box. To display this dialog box, start the Backup, Archive, and Restore interface on the client and select NetBackup Client Properties on the File menu.

■ On UNIX, Linux, and Macintosh clients, you can specify a policy or schedule by using the `bp.conf` options, `BPBACKUP_POLICY` or `BPBACKUP_SCHED`.
On NetWare target clients, you can specify a policy or schedule in the `bp.ini` file.

**Recommended Action:** Do the following, as appropriate:

- Check the client progress log (if available) to determine the policy and schedule that were specified.
- Check the configuration on the master server to determine if the schedule is valid for the policy. If the schedule is not valid, either add the schedule to the policy configuration or specify a valid schedule on the client.

**NetBackup status code: 198**

**Message:** no active policies contain schedules of the requested type for this client

**Explanation:** A user backup or archive was requested, and this client is not in a policy that has a user backup or archive schedule.

**Recommended Action:** Determine if the client is in any policy that has a schedule of the appropriate type (either user backup or archive).

- If the client is in such a policy, check the general policy attributes to verify that the policy is set to active.
- If the client is not in such a policy, do either of the following:
  - Add a schedule of the appropriate type to an existing policy that has this client
  - Create a new policy that has this client and a schedule of the appropriate type

**NetBackup status code: 199**

**Message:** operation not allowed during this time period

**Explanation:** A user backup or archive was requested and this client is not in a policy that has the following: a user backup or archive schedule with an open backup window. This error implies that an appropriate policy and schedule combination exists for this client.

**Recommended Action:** Determine the policies to which this client belongs that also have a schedule of the appropriate type (either user backup or archive).

- If possible, retry the operation when the backup window is open.
- If the backup window is not open during appropriate time periods, adjust a backup window for a schedule in one of the policies.
NetBackup status code: 200

**Message:** scheduler found no backups due to run

**Explanation:** When the NetBackup scheduler process (`nbpem`) checked the policy and the schedule configuration, it did not find any clients to back up.

This error may be due to the following:

- No backup time windows are open (applies only to full and to incremental schedules).
- Policies are set to inactive.
- The clients were recently backed up and are not due for another backup (based on Frequency setting for the schedules).
- Policies do not have any clients.

**Recommended Action:** Usually, this message can be considered informational and does not indicate a problem. However, if you suspect a problem, do the following:

- Examine the NetBackup All Log Entries report for any messages in addition to the one that indicates the scheduler found nothing to do.
- Examine the policy configuration for all policies or the specific policy in question to determine if any of the reasons in the Explanation section apply.
- To obtain detailed troubleshooting information, increase the unified logging level for the diagnostic and debug logs. Use the `vxlogcfg` command as explained in the following procedure:
  - See “Configuring and using unified logging” on page 93.
  - Retry the operation and check the resulting logs.

NetBackup status code: 201

**Message:** handshaking failed with server backup restore manager

**Explanation:** A process on the master server encountered an error when it communicated with the media host (can be either the master or a media server). This error means that the master and the media server processes were able to initiate communication, but were not able to complete them. This problem can occur during a backup, restore, or media list in a single or a multiple server configuration.

**Recommended Action:** Do the following, as appropriate:

- Determine the activity that encountered the handshake failure by examining the NetBackup All Log Entries report for the appropriate time period. If there are media servers, determine if:
The handshake failure was encountered between the master and a media server.

or

Only the master server was involved.

If necessary, create the following debug log directories and increase the logging level:

- `bpcd` on the NetBackup media host (can be either the master or a media server).

- If the error was encountered during a backup operation, increase the logging level for the diagnostic and debug logs for nbpem, nbjm, and nbbrb. Use the `vxlogcfg` command as explained in the following procedure:
  See “Configuring and using unified logging” on page 93.

- If the error was encountered during a restore operation, `bprd` on the master server.

- If the error was encountered during a media list operation, `admin` in the NetBackup `logs/admin` directory on the master server.

- Status code 201 may occur if nbjm fails after connecting to bpbrm or bpmount but before the policy file list is sent. Examine the nbjm unified log (originator ID 117) or the bpbrm or the bpmount legacy logs for more detail on the cause of the error.

- Retry the operation and examine the resulting debug logs for information on why the error occurred.

**NetBackup status code: 202**

**Message:** timed out connecting to server backup restore manager

**Explanation:** A master server process that tried to initiate communications with the media host timed out (can be either the master or a media server). This problem can occur during a backup or restore in either a single or a multiple server configuration.

**Recommended Action:** Determine which activity encountered the connection timeout failure by examining the All Log Entries report for the appropriate time period. If there are media servers, determine if the timeout occurred between the master and a media server or if only the master was involved.

- Verify that the schedule specifies the correct storage unit.

- Run the `ping` command from one host to another by using the following combinations:
From the master server, ping the master and all media servers by using the host names that are found in the storage unit configuration.

From each of the media servers, ping the master server by using the host name that is specified in the NetBackup server list. On a UNIX or Linux server, the master is the first SERVER entry in the bp.conf file. On a Windows server, the master is designated on the Servers tab in the Master Server Properties dialog box.

To access this dialog box, see the following:
See “Using the Host Properties window” on page 60.

Verify that the master server can communicate with bpcd on the host that has the storage unit.

Perform the following procedures:
See “Testing media server and clients” on page 37.
See “Resolving network communication problems” on page 40.

If necessary, create debug log directories for the following processes and retry the operation. Then, check the resulting debug logs on the master server:

If the error occurred during a backup operation, increase the logging level for the diagnostic and debug logs for nbpem, nbjm, and nbrb.
Use the vxlogcfg command as explained in the following procedure:
See “Configuring and using unified logging” on page 93.
Also, check the bpcd legacy debug logs.

If the error occurs during a restore operation, check the bprd debug logs.

NetBackup status code: 203

Message: server backup restore manager’s network is unreachable

Explanation: A process on the master server cannot connect to a particular host on the network when it tries to initiate communication with the media host. This problem can occur during a backup or restore in either a single or a multiple server configuration.

Recommended Action: Determine which activity encountered this failure by examining the All Log Entries report for the appropriate time frame. If there is more than one NetBackup server (one or more media servers), determine the following: if the failure was between the master and a media server or if only the master server was involved. Run the ping command from one host to another by using the following combinations:

From the master server, ping the master and all media servers by using the host names in the storage unit configuration.
From each of the media servers, ping the master server host by using the host name that is specified in the NetBackup server list. On a UNIX or Linux server, the master is the first SERVER entry in the bp.conf file. On a Windows server, the master is designated on the Servers tab in the Master Server Properties dialog.

To access this dialog box, see the following topic:
See “Using the Host Properties window” on page 60.

Perform the following procedures:
See “Testing media server and clients” on page 37.
See “Resolving network communication problems” on page 40.

If necessary, create debug log directories for bprd and retry the operation. Then, check the resulting debug logs on the master server. If the error occurred during a restore, check the bprd debug logs.

NetBackup status code: 204

Message: connection refused by server backup restore manager

Explanation: The media host refused a connection on the port number for bpcd. This error can be encountered during a backup or restore.

Recommended Action: Run the ping command from one host to another by using the following combinations:

- From the master server, ping the master and all media servers by using the host names in the storage unit configuration.

- From each of the media servers, ping the master server by using the name that was specified in the NetBackup server list. On a UNIX or Linux server, the master is the first SERVER entry in the bp.conf file. On a Windows server, the master is designated on the Servers tab in the Master Server Properties dialog box. The following topic shows how to access this dialog box:
See “Using the Host Properties window” on page 60.

- On UNIX and Linux servers, verify that the bpcd entries in /etc/services or NIS on all the servers are identical. Verify that the media host listens on the correct port for connections to bpcd. To verify, run one of the following commands (depending on platform and operating system):

  netstat -a | grep bpcd

  netstat -a | grep 13782 (or the value that was specified during the install)
  rpcinfo -p | grep 13782 (or the value that was specified during the install)
On UNIX and Linux servers, it may be necessary to change the service number for the following: `bpcd` in `/etc/services` and the NIS services map and send `SIGHUP` signals to the `inetd` processes on the clients.

```
/bin/ps -ef | grep inetd
kill -HUP the_inetd_pid
```

or

```
/bin/ps -aux | grep inetd
kill -HUP the_inetd_pid
```

**Note:** On a Hewlett-Packard UNIX platform, use `inetd -c` to send a `SIGHUP` to `inetd`.

- On Windows servers, do the following:
  - Verify that the `bpcd` entries are correct in the following:
    
    `%SystemRoot%\system32\drivers\etc\services`
  - Verify that the following numbers match the settings in the `services` file: **NetBackup Client Service Port** number and **NetBackup Request Service Port** number on the **Network** tab in the NetBackup Client Properties dialog box. To display this dialog box, start the Backup, Archive, and Restore interface and select **NetBackup Client Properties** on the **File** menu. The values on the Network tab are written to the `services` file when the NetBackup Client service starts.
  - Stop and restart the NetBackup services.
  - Perform the following procedures:
    See “Testing media server and clients” on page 37.
    See “Resolving network communication problems” on page 40.
  - If necessary, create debug log directories for `bprd` and retry the operation. Then, check the resulting debug logs on the master server:
    - If the error occurred during a backup operation, check the `nbpem`, `nbjm`, and `nbrb` logs by using the `vxlogview` command.
    - If the error occurred during a restore operation, check the `bprd` debug logs.

Also, see the following topic:

See “Resolving network communication problems” on page 40.
NetBackup status code: 205

Message: cannot connect to server backup restore manager

Explanation: A process on the master server cannot connect to a process on a host on the network. This error occurs when the process tries to initiate communication with the server that has the storage unit. This problem can occur during a backup or restore in either a single or a multiple server configuration.

Recommended Action: Run the ping command from one host to another by using the following combinations:

- From the master server, ping the master and all media servers by using the host names in the storage unit configuration.

- From each of the media servers, ping the master server by using the name that is specified in the NetBackup server list. On a UNIX or Linux server, this master is the first SERVER entry in the bp.conf file. On a Windows server, the master is designated on the Servers tab in the Master Server Properties dialog box. To access this dialog box, see the following topic: See “Using the Host Properties window” on page 60.

- On a UNIX or Linux server, verify that the bpcd entry in /etc/services or NIS on all the servers are identical. Verify that the media host listens on the correct port for connections to bpcd. To verify, run one of the following commands (depending on platform and operating system):

  ```
  netstat -a | grep bpcd
  netstat -a | grep 13782 (or the value that is specified during the install)
  rpcinfo -p | grep 13782 (or the value that is specified during the install)
  ```

- On Windows servers, do the following:
  - Verify that the bpcd entries are correct in the services file:

    ```
    %SystemRoot%\system32\drivers\etc\services
    ```

  - Verify that the following numbers match the settings in the services file: NetBackup Client Service Port number and NetBackup Request Service Port number on the Network tab in the NetBackup Client Properties dialog box. To display this dialog box, start the Backup, Archive, and Restore interface and select NetBackup Client Properties on the File menu. The values on the Network tab are written to the services file when the NetBackup Client service starts.

  - Stop and restart the NetBackup services.

  - Perform the following procedures:
See “Testing media server and clients” on page 37.
See “Resolving network communication problems” on page 40.

- Create a bpcd debug log directory on the server that has the storage unit and retry the operation. Then, check for additional information in the debug log.

Also, see the following topic:
See “Resolving network communication problems” on page 40.

NetBackup status code: 206

**Message:** access to server backup restore manager denied

**Explanation:** The master server tries to start a process on another server (or itself) but does not appear in the NetBackup server list on that server. On a UNIX or Linux server, the master is the first SERVER entry in the bp.conf file. On a Windows server, the master is designated on the Servers tab in the Master Server Properties dialog box. To access this dialog box, see the following topic:
See “Using the Host Properties window” on page 60.

**Recommended Action:** Do the following, as appropriate:

- Verify that the master server appears as a server in its own server list as well as being listed on all media servers.
  If you change the server list on a master server, stop and restart the NetBackup database manager and request the following: daemons (UNIX and Linux) or the NetBackup Database Manager and NetBackup Request Manager services (Windows).
- If necessary, create debug log directories for bprd and retry the operation. Then, check the resulting debug logs on the master server:
  - If the error occurred during a backup operation, check the nbpm, nbjm, and nbrb logs by using the vxlogview command.
  - If the error occurred during a restore operation, check the bprd debug logs.

NetBackup status code: 207

**Message:** error obtaining date of last backup for client

**Explanation:** When nbpm tries to obtain the date of the last backup for a particular client, policy, and schedule combination, an error occurs.

**Recommended Action:** Do the following, as appropriate:

- Verify that the NetBackup database manager (bpdbm) process (on UNIX and Linux) or the NetBackup Database Manager service (on Windows) is running.
Examine the All Log Entries report for the appropriate time frame to gather more information about the failure.

For detailed troubleshooting information, create a \texttt{bpdbm} log directory on the master server. Increase the logging level for the diagnostic and debug logs for \texttt{nbpem}.

Use the \texttt{vxlogcfg} command as explained in the following topic:
See “Configuring and using unified logging” on page 93.
Retry the operation, then check the resulting logs.

**NetBackup status code: 209**

**Message:** error creating or getting message queue

**Explanation:** When a NetBackup process tries to create an internal message queue construct for inter-process communication, an error occurs. This error indicates a problem on the master server. On UNIX and Linux systems, this error may be due to a lack of system resources for System V inter-process communication.

**Recommended Action:** Create debug log directories on the master server and retry the operation. Then, determine the type of system failure by examining the logs. Start with the \texttt{bprd} debug log.

On UNIX and Linux servers, also gather the output of the \texttt{ipcs -a} command to see what system resources are currently in use.

**NetBackup status code: 210**

**Message:** error receiving information on message queue

**Explanation:** When a NetBackup process tries to receive a message from a NetBackup daemon using bprd on an internal message queue construct, an error occurs. This error indicates a problem on the master server. On UNIX and Linux systems, this error may be due to a lack of system resources for System V inter-process communication.

**Recommended Action:** Create debug log directories on the master server and retry the operation. Then, determine the type of system failure by examining the logs. Start with the \texttt{bprd} debug log.

On UNIX and Linux servers, also gather the output of the \texttt{ipcs -a} command to see what system resources are currently in use.

**NetBackup status code: 212**

**Message:** error sending information on message queue
**Explanation:** When a NetBackup process tries to attach to an already existing internal message queue construct for inter-process communication, an error occurs. This error indicates a problem on the master server. On UNIX and Linux systems, this error may be due to a lack of system resources for System V inter-process communication.

**Recommended Action:** Create debug log directories on the master server and retry the operation. Then, determine the type of system failure by examining the logs. Start with the `bprd` debug log.

On UNIX and Linux servers, also, gather the output of the `ipcs -a` command to see what system resources are currently in use.

### NetBackup status code: 213

**Message:** No storage units available for use

**Explanation:** The NetBackup resource broker (`nbrb`) did not find any storage units available for use. Either all storage units are unavailable or all storage units are configured for **On demand only**. In addition, the policy and schedule does not require a specific storage unit.

**Recommended Action:** Do the following, as appropriate:

- Examine the Backup Status and All Log Entries report for the appropriate time period to determine the policy or schedule that received the error.
- Verify that the media server has not been deactivated for the storage unit or units that are unavailable.
- Verify that the storage unit’s drives are not down.
- Verify the following attribute settings for all storage units:
  - For disk storage units, the **Maximum concurrent jobs** is not set to 0
  - For Media Manager storage units, the **Maximum concurrent write drives** is not set to 0
- Verify that the robot number and host name in the storage unit configuration matches the Media and Device Management device configuration.
- Determine if all storage units are set to **On demand only** for a combined policy and schedule that does not require a specific storage unit. In this case, either specify a storage unit for the policy and the schedule combination or turn off **On demand only** for a storage unit.
- If the storage unit is on a UNIX or Linux NetBackup media server, it may indicate a problem with `bpcd`. Check `/etc/inetd.conf` on the media server to verify that the `bpcd` entry is correct.
If the storage unit is on a Windows NetBackup media server, verify that the NetBackup Client service was started on the Windows NetBackup media server.

- For detailed troubleshooting information, increase the logging levels of `nbrb` and `mds` on the master server.
  
  Use the `vxlogcfg` command as explained in the following topic:
  
  See “Configuring and using unified logging” on page 93.
  
  Retry the operation and check the resulting debug logs.

**NetBackup status code: 215**

**Message:** failed reading global config database information

**Explanation:** During the periodic checking of the NetBackup configuration, `nbproxy` was unable to read the global configuration parameters.

**Recommended Action:** Do the following, as appropriate:

- On UNIX and Linux master servers, verify that the NetBackup database manager (`bpdbm`) process is running. On a Windows master server, verify that the NetBackup Database Manager service is running.

- Try to view the global configuration settings by using the NetBackup administration interface (on UNIX and Linux systems), or by using Host Properties (on Windows systems).

- For detailed troubleshooting information, create debug log directories for `nbproxy` and `bpdbm` on the master server and retry the operation. Check the resulting debug logs for these processes. Also check the `nbpem` logs by using the `vxlogview` command.

**NetBackup status code: 216**

**Message:** failed reading retention database information

**Explanation:** During its periodic checking of the NetBackup configuration, `nbpem` did not read the list of retention levels and values.

**Recommended Action:** Do the following, as appropriate:

- On a UNIX or Linux master server, verify that the NetBackup database manager (`bpdbm`) process is running. On a Windows master server, verify that the NetBackup Database Manager service is running.

- For detailed troubleshooting information, create a debug log directory for `bpdbm` on the master server.

  Increase the logging level for `nbpem` by using the `vxlogcfg` command as described in the following topic:
See “Configuring and using unified logging” on page 93. Retry the operation and check the resulting logs.

NetBackup status code: 217

**Message:** failed reading storage unit database information

**Explanation:** During its periodic checking of the NetBackup configuration, nbpem did not read the storage unit configuration.

**Recommended Action:** Do the following, as appropriate:

- On a UNIX or Linux server, verify that the NetBackup database manager (`bpdbm`) process is running. On a Windows server, verify that the NetBackup Database Manager service is running.
- Try to view the storage unit configuration by using the NetBackup administration interface.
- For detailed troubleshooting information, create debug logs for `nbproxy` and `bpdbm` on the master server and retry the operation. Check the resulting debug logs. Also check the `nbpem` logs by using the `vxlogview` command. Ensure that the correct master server is specified for the connection.

NetBackup status code: 218

**Message:** failed reading policy database information

**Explanation:** During the periodic checking of the NetBackup configuration, nbpem did not read the backup policy configuration.

**Recommended Action:** Do the following, as appropriate:

- On a UNIX or Linux server, verify that the NetBackup Database Manager (`bpdbm`) process is running. On a Windows server, verify that the NetBackup Database Manager service is running.
- Try to view the policy configuration by using the NetBackup administration interface.
- For detailed troubleshooting information, create debug log directories for `nbproxy` and `bpdbm` on the master server and retry the operation. Check the resulting debug logs. Also check the `nbpem` logs by using the `vxlogview` command. Ensure that the correct master server is specified for the connection.

NetBackup status code: 219

**Message:** the required storage unit is unavailable
**Explanation:** The policy or schedule for the backup requires a specific storage unit, which is currently unavailable. This error also occurs for other tries to use the storage unit within the current backup session.

**Recommended Action:** Look in the Job Details window for the failed job.

- Verify that the schedule specifies the correct storage unit and the storage unit exists.

- Verify that the following devices are running: the Media Manager device daemon (ltd) (UNIX or Linux server) or the NetBackup Device Manager service (Windows server). Use `bppsrc` on UNIX and Linux and the Activity Monitor on Windows or the Services application in the Windows Control Panel.

- Verify the following attribute settings:
  - For a disk storage unit, **Maximum concurrent jobs** is not set to 0.
  - For a Media Manager storage unit, the **Maximum concurrent drives** attribute is not set to 0.

- If the storage unit is a tape, verify that at least one of the drives is in the UP state. Use the Device Monitor.

- Verify that the robot number and host in the storage unit configuration match what is specified in the Media and Device Management device configuration.

- Verify that the master server can communicate with the `bpcd` process on the server that has the storage unit.

- Verify that `bpcd` listens on the port for connections.
  - On a UNIX or Linux server where the storage unit is connected, if you run `netstat -a | grep bpcd`, it should return something similar to the following:
    ```
    *.bpcd   *.*        0    0    0    0 LISTEN
    ```
  - On a Windows NetBackup server where the storage unit is connected, run `netstat -a` to print several lines of output. If `bpcd` listens, one of those lines is similar to the following:
    ```
    TCP      myhost:bpcd   0.0.0.0:0    LISTENING
    ```

- Check the nbrb and the mds logs by using the `vxlogview` command.

- If the cause of the problem is not obvious, perform some of the steps in the following procedure:
  - See “Resolving network communication problems” on page 40.
NetBackup status code: 220

Message: database system error

Explanation: The bpdbm process (UNIX and Linux), or the NetBackup Database Manager service (Windows) did not create a directory path for its configuration catalogs. This error is due to a system call failure, which is usually due to a permission problem or an "out of space" condition.

Recommended Action: Create a debug log directory for bpdbm. Increase the logging level for the diagnostic and debug logs for nbemm.

Use the vxlogcfg command as explained in the following topic:

See “Configuring and using unified logging” on page 93.

Retry the operation and check the resulting logs for information.

NetBackup status code: 221

Message: continue

Explanation: This status code is used to coordinate communication between various NetBackup processes and normally does not occur. If the logs show that it is associated with a subsequent error, it usually indicates a communication problem. In this case, concentrate your troubleshooting efforts on the subsequent error.

Recommended Action: Determine the cause of the status code that follows this one.

NetBackup status code: 222

Message: done

Explanation: This status code is used to coordinate communication between various NetBackup processes and is normally not seen. If the error logs show that it is associated with a subsequent error, it usually indicates a communication problem. In this case, concentrate your troubleshooting efforts on the subsequent error.

Recommended Action: Determine the cause of the status code that follows this one.

NetBackup status code: 223

Message: an invalid entry was encountered

Explanation: A request to the bpdbm process (on UNIX and Linux) or the NetBackup Database Manager service (on Windows) had invalid information or some
information that conflicted. This error is usually a result of the use of software from different versions. Another cause can be incorrect parameters on a command.

**Recommended Action:** Verify that all NetBackup software is at the same version level and the command parameters are specified correctly. If neither of these is the problem, obtain detailed troubleshooting information by creating a `bpdbm` debug log directory. Then retry the operation. Check the resulting debug log.

**NetBackup status code: 224**

**Message:** there was a conflicting specification

**Explanation:** A request to the `bpdbm` process (on UNIX and Linux) or the NetBackup Database Manager service (on Windows) had some information that conflicted. This error is usually a result of the use of software from different version levels together.

**Recommended Action:** Verify that all NetBackup software is at the same version level. If that is not the problem, obtain detailed troubleshooting information by creating `bpdbm` and `admin` debug log directories. Then retry the operation. Check the resulting debug logs.

**NetBackup status code: 225**

**Message:** text exceeded allowed length

**Explanation:** Text in a request exceeds a buffer size. The request was made to the `bpdbm` process (on UNIX and Linux) or the NetBackup Database Manager service (on Windows). This error is usually a result of the use of software from different version levels.

**Recommended Action:** Verify that all NetBackup software is at the same version level. If that is not the problem, create debug log directories for `bpdbm` and `admin`. Then, retry the operation and examine the resulting debug logs.

**NetBackup status code: 226**

**Message:** the entity already exists

**Explanation:** The configuration already has an entity with the same name or definition. For example: this status appears if you add a new policy when an existing policy has the same name or definition such as attributes or clients.

**Recommended Action:** Correct your request and re-execute the command.

**NetBackup status code: 227**

**Message:** no entity was found
Explanation: The item requested was not in the catalog. For example, the entity can be a file or it can be policy information.

Recommended Action: A common cause for this problem is a query that has no matching images. Specify different parameters or options for the operation and try it again.

NetBackup status code: 228
Message: unable to process request

Explanation: An inconsistency exists in the catalog or a request was made that would be improper to satisfy.

Recommended Action: Do the following, as appropriate:

- If this status involves a media server, verify that its server list specifies the correct master server. On a UNIX or Linux server, the master server is the first SERVER entry in the bp.conf file. On a Windows server, the master is designated on the Servers tab in the Master Server Properties dialog box. To access this dialog box, see the following topic: See “Using the Host Properties window” on page 60.

- For detailed troubleshooting information, create a bpdbm debug log directory and retry the operation. Then, check the resulting debug log.

NetBackup status code: 229
Message: events out of sequence - image inconsistency

Explanation: A request was made that would cause the image catalog to become inconsistent if satisfied

Recommended Action: Obtain detailed troubleshooting information by creating a debug log directory for bpdbm. Then, retry the operation, save the resulting debug log, and call customer support.

NetBackup status code: 230
Message: the specified policy does not exist in the configuration database

Explanation: The specified policy name does not exist.

Recommended Action: Correct your parameters or options and retry the operation.

NetBackup status code: 231
Message: schedule windows overlap
**Explanation:** The specified start and the duration times for one day of the schedule overlap with another day of the schedule.

**Recommended Action:** Correct the schedule to eliminate the overlapping backup windows.

**NetBackup status code: 232**

**Message:** a protocol error has occurred

**Explanation:** This error is an intermediate status code that usually precedes another status code. It indicates the following: either the bpdbm process (on UNIX and Linux) or the NetBackup Database Manager service (on Windows) or the process that communicates with it has received unexpected information.

**Recommended Action:** Create a debug log directory for bpdbm. Then, retry the operation, save the debug log, and call customer support.

**NetBackup status code: 233**

**Message:** premature elf encountered

**Explanation:** This status code is an intermediate one that usually precedes another status code and is associated with a problem in network communication.

**Recommended Action:** During a restore, this status codes means that tar (on the client) received a stream of data that was not what it expected. If the restore is a new configuration, verify that the tape drive is configured for variable mode. See the *NetBackup Device Configuration Guide*.

If the communication failure is not due to an interrupt on a client system, save all error information and call customer support.

**NetBackup status code: 234**

**Message:** communication interrupted

**Explanation:** This status code is an intermediate one that usually precedes another status code and is associated with a problem in network communication. Either a server or a client process received an interrupt signal.

**Recommended Action:** Save all error information and call customer support.

**NetBackup status code: 235**

**Message:** inadequate buffer space

**Explanation:** This code usually indicates a mismatch between server and client software versions.
**Recommended Action:** Do the following, as appropriate:

- Verify that all NetBackup software is at the same version level. Update earlier versions of NetBackup software.
  - On UNIX and Linux, NetBackup servers and clients, check the `/usr/openv/netbackup/bin/version` file.
  - On Windows NetBackup servers, check the `install_path\NetBackup\version.txt` file or the **About NetBackup** item on the **Help** menu.
  - On Microsoft Windows clients, check the **About NetBackup** item on the **Help** menu.
  - On NetWare target clients, check the Version entry in the `bp.ini` file.
  - If the client software is earlier than 3.0, verify that the client is in a Standard type policy.
  - On Macintosh clients, check the version file in the `bin` folder in the **NetBackup** folder in the **Preferences** folder.

- If the problem persists, save all error information and call customer support.

**NetBackup status code: 236**

**Message:** the specified client does not exist in an active policy within the configuration database

**Explanation:** A client name was not specified or the specified client does not exist.

**Recommended Action:** Activate the required policy, correct the client name, or add the client to a policy that meets your needs. After you make the correction, retry the operation.

**NetBackup status code: 237**

**Message:** the specified schedule does not exist in an active policy in the configuration database

**Explanation:** The specified schedule does not exist in the NetBackup configuration.

**Recommended Action:** Activate the required policy, correct the schedule name, or create a schedule in a policy that meets your needs. After you make the correction, retry the operation.
NetBackup status code: 238
Message: the database contains conflicting or erroneous entries
Explanation: The catalog has an inconsistent or a corrupted entry.
Recommended Action: Obtain detailed troubleshooting information for bpdbm (on UNIX and Linux) or the NetBackup Database Manager service (on Windows) by creating a debug log directory for it. Then, retry the operation, save resulting debug log, and call customer support.

NetBackup status code: 239
Message: the specified client does not exist in the specified policy
Explanation: The specified client is not a member of the specified policy.
Recommended Action: Correct the client name specification, specify a different policy, or add the required client name to the policy. After you make the correction, retry the operation.

NetBackup status code: 240
Message: no schedules of the correct type exist in this policy
Explanation: The appropriate schedule was not found in the specified policy. For example, a user backup specified a policy name but no user backup schedule exists in that policy.
Recommended Action: Specify a different policy or create a schedule of the needed type in the policy. After you make the correction, retry the operation.

NetBackup status code: 241
Message: the specified schedule is the wrong type for this request
Explanation: The specified schedule for an immediate manual backup is not for a full nor an incremental backup. It must be one of these.
Recommended Action: Specify only full or incremental schedules for manual backups. If one does not exist in the policy, create one.

NetBackup status code: 242
Message: operation would cause an illegal duplication
Explanation: If the request is processed, it causes a duplicate entry (for example, in the catalog or the configuration database). A duplicate catalog entry is usually due to a mistake in the specification of media IDs for NetBackup catalog backups.
**Recommended Action:** Check the error reports to determine the specific duplication that would occur. Correct the settings for the operation and retry it.

**NetBackup status code: 243**

**Message:** the client is not in the configuration

**Explanation:** The specified client name was not in the catalog.

**Recommended Action:** Either correct the client name or add the client to the wanted policy.

**NetBackup status code: 245**

**Message:** the specified policy is not of the correct client type

**Explanation:** A user backup specified a policy that is not the type that is required for the client.

**Recommended Action:** Retry the operation by specifying a policy that is the correct type for the client. If such a policy does not exist, create one.

**NetBackup status code: 246**

**Message:** no active policies in the configuration database are of the correct client type

**Explanation:** A user backup request was not satisfied because no active policies were the type that were required for the client.

**Recommended Action:** Create or activate an appropriate policy so the user backup request can be satisfied.

**NetBackup status code: 247**

**Message:** the specified policy is not active

**Explanation:** Backups for the specified policy are disabled because the policy is inactive.

**Recommended Action:** Activate the policy and retry the operation.

**NetBackup status code: 248**

**Message:** there are no active policies in the configuration database

**Explanation:** No active policy was found that would satisfy the request.

**Recommended Action:** Activate the appropriate policy and retry the operation.
NetBackup status code: 249
Message: the file list is incomplete

Explanation: While the server waited for the client to finish sending the file list, it timed out or a sequencing problem occurred.

Recommended Action: First, obtain additional information by creating debug logs. Then try to recreate the error. The debug logs to create are as follows:

- On the server, bptm, bpbrm, and bpdbm.
- On UNIX, Linux, and Windows clients, bpbkar.
- On other clients, bpcd.

To increase the amount of information that is included in the logs, see the following:

See “Debug logs on PC clients” on page 116.

NetBackup status code: 250
Message: the image was not created with TIR information

Explanation: This error is internal and should not appear to customers.

Recommended Action: Obtain detailed troubleshooting information by creating debug logs for bptm or bpdbm on the server. Then, retry the operation and check the resulting debug logs.

NetBackup status code: 251
Message: the tir information is zero length

Explanation: For a true-image backup, the client sent no file information to the master server. NetBackup discovered this condition when it tried to write the TIR information to media.

Recommended Action: Check the policy file list and the exclude and include lists on the client to verify that the client has eligible files for backup. For example, this status code can appear if the exclude list on the client excludes all files.

To obtain detailed troubleshooting information, create debug logs for bptm or bpdbm on the server. Then, retry the operation and check the resulting debug logs.

NetBackup status code: 252
Message: An extended error status has been encountered, check detailed status
Explanation: If a process was unable to report the extended error status as the final job status, the job exits with status 252. (The extended error status has a number greater than 255.)

Recommended Action: To determine the actual error, examine the job details display.

NetBackup status code: 253

Message: the catalog image .f file has been archived

Explanation: The catalog image .f file was archived.

Recommended Action: Refer to catalog archiving help information to restore archived catalog image .f files.

NetBackup status code: 254

Message: server name not found in the NetBackup configuration

Explanation: This error should not occur through normal use of NetBackup.

Recommended Action: Save all error information and call customer support.

NetBackup status code: 256

Message: logic error encountered

Explanation: An internal Vault error occurred.

Recommended Action: Contact customer support and send appropriate logs.

NetBackup status code: 257

Message: failed to get job data

Explanation: This error can indicate either of the following:

- Vault failed to get job data because of a broken connection with the job manager (nbjm).
- Vault received empty job data. This error occurs if a user-specified job ID on the vltrun -haltdups command is out of range. (That is, the job ID is not among the job IDs created by job manager.)

Recommended Action: Contact customer support and send the appropriate logs.

NetBackup status code: 258

Message: Vault duplication was aborted by administrator request
**Explanation:** The administrator initiated an abort request on the active vault duplication job.

**Recommended Action:** Ensure that the abort request was intentional.

**NetBackup status code: 259**

**Message:** vault configuration file not found

**Explanation:** This error should not occur.

**Recommended Action:** Contact customer support and send appropriate logs.

**NetBackup status code: 260**

**Message:** failed to send signal

**Explanation:** vltrun failed to send a signal to the Vault duplication job.

**Recommended Action:** Contact customer support and send the appropriate logs.

**NetBackup status code: 261**

**Message:** vault internal error 261

**Explanation:** This error code should not occur.

**Recommended Action:** Contact customer support and send appropriate logs.

**NetBackup status code: 262**

**Message:** vault internal error 262

**Explanation:** This error code should not occur.

**Recommended Action:** Contact customer support and send appropriate logs.

**NetBackup status code: 263**

**Message:** session id assignment failed

**Explanation:** The unique identifier to be assigned to the Vault session is corrupt.

**Recommended Action:** Verify that the session ID that is stored in the `session.last` file is valid.

UNIX and Linux:

```
/usr/openv/netbackup/vault/sessions/vault_name/session.last
```

Windows:
Make sure that the file system is not full and that no one has inadvertently edited the `session.last` file. To correct the problem, store the highest session ID that was assigned to a session for this Vault in the `session.last` file. If the problem persists, contact customer support and send the appropriate logs.

**NetBackup status code: 265**
**Message:** session id file is empty or corrupt
**Explanation:** The session ID that is stored in the following file is corrupt.

UNIX and Linux:
/usr/openv/netbackup/vault/sessions/vault_name/session.last
Windows:
`install_path\NetBackup\vault\sessions\vault_name\session.last`

**Recommended Action:** Ensure that the session ID that is stored in the `session.last` file is not corrupt. Make sure that the file system is not full and that no one has inadvertently edited the file. To correct the problem, store the highest session ID that was assigned to a session for this Vault in the `session.last` file. If the problem persists, contact customer support and send the appropriate logs.

**NetBackup status code: 266**
**Message:** cannot find robot, vault, or profile in the vault configuration
**Explanation:** NetBackup cannot find the specified `profile_name` or triplet `robot_name/vault_name/profile_name` on the Vault command (vltrun, vltreject, vltoffsitemedia) or in `vltopmenu` in the Vault configuration.

**Recommended Action:** Rerun the command with the correct `profile_name` or triplet `robot_name/vault_name/profile_name`.

**NetBackup status code: 267**
**Message:** cannot find the local host name
**Explanation:** A Vault job obtains the local host name through an OS call. This error occurs when the Vault job is unable to get the local host name.
**Recommended Action:** Issue a hostname command at the OS command prompt. See the hostname (or gethostbyname) man page for an explanation of the conditions that would cause it to fail.

Refer to the *OS System Administrator’s Guide* for more information.

**NetBackup status code: 268**

**Message:** the vault session directory is either missing or inaccessible

**Explanation:** This error occurs when a Vault job cannot access the following:

- UNIX and Linux: `/usr/openv/netbackup/vault/sessions`
- Windows: `install_path\NetBackup\vault\sessions`

This directory is created when Vault is installed.

**Recommended Action:** Make sure you are running on the master server where Vault is installed and configured. Also ensure that no one accidentally removed the sessions directory or changed permission on the directory path so it is inaccessible to the Vault job.

**NetBackup status code: 269**

**Message:** no vault session id was found

**Explanation:** This error is encountered when `vltopmenu` cannot find a sidxxx *session id* directory for the specified profile. Either no Vault jobs were run for this profile or the corresponding sidxxx *session id* directory (or directories) were removed from the following directory:

- UNIX and Linux: `/usr/openv/netbackup/vault/sessions/vault_name`
- Windows: `install_path\NetBackup\vault\sessions\vault_name`

**Recommended Action:** Either specify a different profile for the Vault jobs that were run or exit `vltopmenu` and run a Vault job for the specific profile. Then rerun `vltopmenu` and select the profile.

**NetBackup status code: 270**

**Message:** unable to obtain process id, getpid failed

**Explanation:** This error occurs when a Vault process is unable to obtain its process ID by means of the `getpid()` OS system call.
Recommended Action: Look at the system log for any unusual system problems. Wait a while and then try running the process again when system resources are freed up.

NetBackup status code: 271
Message: vault XML version mismatch
Explanation: The Vault upgrade process failed.
Recommended Action: Enable logging, start nbvault, and then examine the nbvault logs to determine the cause of the failure. If the upgrade process fails again, contact your customer support representative.

The following are the locations of the nbvault logs:

UNIX and Linux: /usr/openv/netbackup/logs/nbvault/
Windows: install_path\NetBackup\logs\nbvault

NetBackup status code: 272
Message: execution of a vault notify script failed
Explanation: This error occurs when the Vault process is unable to run a Vault notify script due to permissions problems or coding problems in the script. It also occurs if the script returns an error.
Recommended Action: Ensure that the notify script is executable and runs without errors. You must debug the script by running it manually to eliminate coding errors.

NetBackup status code: 273
Message: invalid job id
Explanation: This error can occur in either of the following situations:
- The specified job is not an active Vault job
- The specified active Vault job is not at the duplication step
Recommended Action: Specify the job ID of the active Vault job that is currently at the duplication step or operation.

NetBackup status code: 274
Message: no profile was specified
Explanation: This error should not occur.
Recommended Action: Contact customer support and send the appropriate logs.
NetBackup status code: 275
Message: a session is already running for this vault
Explanation: This error occurs when you start a session for a vault and another session is already running for this vault. Only one session is allowed for a vault at any given time.
Recommended Action: Start the Vault session after the previous session has completed.

NetBackup status code: 276
Message: invalid session id
Explanation: This error should not occur.
Recommended Action: Contact customer support and send the appropriate logs.

NetBackup status code: 277
Message: unable to print reports
Explanation: This error should not occur.
Recommended Action: Contact customer support and send the appropriate logs.

NetBackup status code: 278
Message: unable to collect pre eject information from the API
Explanation: This error occurs when robotic information cannot be retrieved before ejection.
Recommended Action: Ensure that all Media and Device Management daemons are running or the robot is live and up.

NetBackup status code: 279
Message: eject process is complete
Explanation: This error occurs when the eject process is completed successfully.
Recommended Action: None.

NetBackup status code: 280
Message: there are no volumes to eject
Explanation: This error occurs when media to be ejected are not in the library.
**Recommended Action**: Ensure that the media to be ejected are not removed from the library manually.

### NetBackup status code: 281

**Message**: vault core error

**Explanation**: An internal Vault error occurred.

**Recommended Action**: Contact customer support and send the appropriate logs.

### NetBackup status code: 282

**Message**: cannot connect to nbvault server

**Explanation**: The vault job cannot connect to the NetBackup Vault Manager service (nbvault on UNIX and Linux, nbvault.exe on Windows).

Possible causes are the following:

- The &CompanyName; Private Branch Exchange service (VRTSpbx) or NetBackup Request Manager (bprd) is down.
- The NetBackup Vault Manager service is down, possibly because of the following: the Vault is not licensed, the vault.xml configuration file is corrupt, or the vault.xml configuration file upgrade failed during an upgrade installation.

**Recommended Action**: To determine the reason for failure, examine the logs for the service or services that are down and the operating system logs (EventLog on Windows). Restart the service or services that are down after resolving the problem.

The following are the locations of the nbvault logs:

- UNIX and Linux: `/usr/openv/netbackup/logs/nbvault/`
- Windows: `install_path\NetBackup\logs\nbvault`

### NetBackup status code: 283

**Message**: error(s) occurred during vault report generation

**Explanation**: Vault encountered errors during the report generation phase.

**Recommended Action**: Check logs for details of the failure.

### NetBackup status code: 284

**Message**: error(s) occurred during vault report distribution
**Explanation:** Vault encountered errors during the report distribution phase. Potential reasons include the following:

- Reports were not emailed (possibly because of malformed email addresses in the `vault.xml` file).
- On Windows, the third-party mail client (such as blat) is not configured properly.
- The reports destination directory is not present or it does not have appropriate permissions.
- The printer is not set up correctly or the printer command in `vault.xml` is incorrect.

**Recommended Action:** Check logs for details of the failure.

**NetBackup status code: 285**

**Message:** unable to locate vault directory

**Explanation:** A Vault job or a command for a missing or a corrupt directory of the session in question returns this error.

**Recommended Action:** The Vault directory is created when the Vault package is installed on the master server. Ensure that the Vault job or command is started as root on the master server. Ensure that the Vault directory was not removed inadvertently or made inaccessible to the root user.

**NetBackup status code: 286**

**Message:** vault internal error

**Explanation:** This error should never occur.

**Recommended Action:** Contact customer support and send the appropriate logs.

**NetBackup status code: 287**

**Message:** vault eject failed

**Explanation:** This error occurs when Vault fails to eject any of the media that was identified for eject during a Vault Session. Potential reasons: Media and Device Management services are down, the robot is down, or no empty slots are available in the media access port (MAP).

**Recommended Action:** Ensure that the Media and Device Management services are running, the robot is up, and empty slots are available in the media access port (MAP).
NetBackup status code: 288

Message: vault eject partially succeeded

Explanation: This error occurs when not all of the media that was identified for eject during a Vault session can be ejected. Potential reasons include the following:

- Some of the media is in use by NetBackup
- Some of the media are in a drive
- Not enough empty slots are available in the media access port (MAP)

Recommended Action: Ensure that the media are not loaded in a drive and in use by other processes. Ensure that empty slots are available in the media access port (MAP).

NetBackup status code: 289

Message: cannot consolidate reports of sessions from container and slot-based vaults

Explanation: This error occurs when you consolidate reports and at least one session uses slots and another uses containers.

Recommended Action: Change the report consolidation so that only reports for one type of vault operation are consolidated, either slots or containers.

NetBackup status code: 290

Message: one or more errors detected during eject processing

Explanation: This error occurs when more than one error is encountered during an eject procedure by vltopmenu. Any "eject" errors that range from 291 to 300 may have occurred in any of the sessions being ejected.

Recommended Action: For detailed information, review the Vault debug log in the following directory:

```
UNIX and Linux: /usr/openv/netbackup/logs/vault
Windows: install_path\NetBackup\logs\vault
```

Also review the summary.log in each of the sidxxx directories that had problems:

```
UNIX and Linux:
/usr/openv/netbackup/vault/sessions/vault_name/sidxxx
Windows:
install_path\NetBackup\vault\sessions\vault_name\sidxxx
```
After the problem is identified and corrected, the media that were not ejected may need to be ejected manually by means of `vlteject` or `vltopmenu`.

This error often indicates that the media were left in the off-site Vault volume group but physically reside in the robot or the robotic MAP.

To solve this problem, do one of the following:

- Manually remove any media that are in the off-site Vault volume group but are still in the robotic library.
- Inventory the robotic library. An inventory puts any media that were in the off-site Vault volume group back into the robotic volume group. Then rerun the Vault sessions that failed.

**NetBackup status code: 291**

**Message:** number of media has exceeded capacity of MAP; must perform manual eject using `vltopmenu` or `vlteject`

**Explanation:** This error occurs in the following situation: a Vault job is run for a profile that selected automatic eject mode and the number of media to be ejected exceeds the MAP capacity.

**Recommended Action:** Use `vltopmenu` to manually eject the media for the selected profile and session ID. The `vltopmenu` option lets you eject the selected media, a MAP-full (or less) at a time.

**NetBackup status code: 292**

**Message:** eject process failed to start

**Explanation:** This error occurs when the following cannot start the eject process: the Vault job, the `vlteject` command, or the use of the `vltopmenu`.

**Recommended Action:** For detailed information about the problem, review the Vault debug log in the following directory:

UNIX and Linux: `/usr/openv/netbackup/logs/vault`

Windows: `install_path\NetBackup\logs\vault`

Also review the `summary.log` in each of the `sidxxx` directories that had problems:

UNIX and Linux:

`/usr/openv/netbackup/vault/sessions/vault_name/sidxxx`

Windows:

`install_path\NetBackup\vault\sessions\vault_name\sidxxx`
Use the robtest utility to ensure that you can communicate with the Vault robotic library. After the problem is resolved, rerun the Vault session, vlteject command, or vltopmenu command.

**NetBackup status code: 293**

**Message:** eject process has been aborted

**Explanation:** This error occurs when the eject process is canceled. This error can be encountered during a Vault job or with the `vlteject` or the `vltopmenu` eject command.

This error can occur because of one of the following conditions:

- Could not open a pipe to `vmchange -verify_eject` call.
- Unexpected output from `vmchange -verify_eject` call.
- No MAP elements exist to eject media into.
- The robotic library had problems putting media into the MAP.
- The user pressed Return in interactive mode and did not first remove the media from the MAP. In this case, the media that were in the MAP are put back into their original slots in the robotic library.

**Recommended Action:** For detailed information about why the process was canceled, review the Vault debug log in the following directory:

UNIX and Linux: `/usr/openv/netbackup/logs/vault`

Windows: `install_path\NetBackup\logs\vault`

Also review the `summary.log` in each of the `sidxxx` directories that had problems:

UNIX and Linux:

```
/usr/openv/netbackup/vault/sessions/vault_name/sidxxx
```

Windows:

```
install_path\NetBackup\vault\sessions\vault_name\sidxxx
```

(Where `xxx` is the session ID)

This error often indicates that the media were left in the off-site Vault volume group but physically reside in the robot or the robotic MAP.

To solve this problem, do one of the following:

- Manually remove any media that are in the off-site Vault volume group but are still in the robotic library.
Inventory the robotic library. An inventory puts any media that were in the off-site Vault volume group back into the robotic volume group. Then, rerun the Vault sessions that failed.

**NetBackup status code: 294**

**Message:** vault catalog backup failed

**Explanation:** During a Vault job, the catalog backup step failed.

**Recommended Action:** Review the Vault debug log in the following directory for detailed information about why the process failed:

UNIX and Linux: /usr/openv/netbackup/logs/vault
Windows: install_path\NetBackup\logs\vault

To find the actual problem that caused the catalog backup (bpbackupdb) to fail, review the summary.log in each of the sidxxx directories that had problems:

UNIX and Linux:
/usr/openv/netbackup/vault/sessions/vault_name/sidxxx
Windows:
install_path\NetBackup\vault\sessions\vault_name\sidxxx

(where xxx is the session ID)

Correct the problem and rerun the Vault job.

**NetBackup status code: 295**

**Message:** eject process could not obtain information about the robot

**Explanation:** This error occurs when the eject process cannot collect information about the robotic library and its associated MAPs and volumes.

**Recommended Action:** For detailed information about why the process fails, review the Vault debug log in the following directory:

UNIX and Linux: /usr/openv/netbackup/logs/vault
Windows: install_path\NetBackup\logs\vault

Also review the summary.log in each of the sidxxx directories that had problems:

UNIX and Linux:
/usr/openv/netbackup/vault/sessions/vault_name/sidxxx
Windows:
install_path\NetBackup\vault\sessions\vault_name\sidxxx

(where xxx is the session ID)
Correct the error and rerun the Vault session, `vlteject` command, or `vltopmenu` eject command.

**NetBackup status code: 296**

**Message:** process called but nothing to do

**Explanation:** This error occurs in the following situations:
- `vlteject` is called with `-eject` but the system has no tapes to eject
- `vlteject` is called with `-eject` and the eject is already done
- `vlteject` is called with `-report` and the reports are already done
- `vlteject` is called with `-eject` and `-report`, and both the eject and the reports are done

**Recommended Action:** This error is an informative one and does not require any action.

**NetBackup status code: 297**

**Message:** all volumes are not available to eject

**Explanation:** This error occurs when an try is made to eject a non-existent or bad media ID during the eject phase of the following: a Vault session, a `vlteject` command, or a `vltopmenu` command.

Possible reasons for this error are as follows:
- The bad media ID was added by means of the `vlt_ejectlist_notify` script.
- The bad media ID is already in the MAP or not in the robotic library.
- The bad media ID is in a robotic drive.
- The bad media ID is in transit in the robotic library.

**Recommended Action:** Remove or correct the defective media ID from the `vlt_ejectlist_notify` script and rerun the Vault session. If the bad media ID is in the MAP or a drive or in transit, something is misconfigured.

**NetBackup status code: 298**

**Message:** the library is not ready to eject volumes

**Explanation:** This error occurs if the robotic library is not in a state to support ejecting media.

Possible reasons for this error include the following:
Currently, the library ejects media
- The library waits to eject media
- Currently, the library injects media
- The library waits to inject media

**Recommended Action:** Wait until the robotic library can support the eject action and rerun the Vault session, `vlteject` command, or `vltopmenu` command.

**NetBackup status code: 299**

**Message:** there is no available MAP for ejecting

**Explanation:** The robotic library you vault from does not have a MAP available for use and so media cannot be ejected.

**Recommended Action:** Wait until the robotic library’s MAP is available for use and rerun the Vault session, `vlteject` command, or `vltopmenu` command.

**NetBackup status code: 300**

**Message:** vmchange eject verify not responding

**Explanation:** During the eject process, the `vmchange` command is called with a "-verify_eject" call until all of the volumes for the request are in the MAP. This command call failed. Or it did not return the proper information to the Vault eject process.

**Recommended Action:** Do the following, as appropriate:

- Review the Vault debug log in the following directory for detailed information about why the process failed:

  UNIX and Linux: `/usr/openv/netbackup/logs/vault`  
  Windows: `install_path\NetBackup\logs\vault`

- Also review the `summary.log` in each of the `sidxxx` directories that had problems:

  UNIX and Linux:
  `/usr/openv/netbackup/vault/sessions/vault_name/sidxxx`

  Windows:
  `install_path\NetBackup\vault\sessions\vault_name\sidxxx`

  (where `xxx` is the session ID)
This error often indicates that the media were left in the off-site Vault volume group but physically reside in the robot or the robotic MAP. To solve this problem, do one of the following:

- Manually remove any media that are in the off-site Vault volume group but are still in the robot.
- Inventory the robot. An inventory puts any media that were in the off-site Vault volume group back into the robotic volume group. Then, rerun the Vault sessions that failed.

**NetBackup status code: 301**

**Message:** vmchange api_eject command failed

**Explanation:** During the eject process, the vmchange command is called with an "-api_eject" call to begin the process to eject media. This command call failed.

**Recommended Action:** Review the Vault debug log in the following directory for detailed information about why the process failed:

UNIX and Linux: /usr/openv/netbackup/logs/vault  
Windows: install_path\NetBackup\logs\vault

Also review the summary.log in each of the sidxxx directories that had problems:

UNIX and Linux:  
/usr/openv/netbackup/vault/sessions/vault_name/sidxxx  
Windows:  
install_path\NetBackup\vault\sessions\vault_name\sidxxx

(where xxx is the session ID)

When the problem is resolved, rerun the Vault session, vlteject command, or vltopmenu command.

**NetBackup status code: 302**

**Message:** error encountered trying backup of catalog (multiple tape catalog backup)

**Explanation:** This error occurs when the NetBackup command that was used for stage one of the two-stage catalog backup fails.

**Recommended Action:** For the actual error that caused the failure, review the Vault debug log in the following directory:

UNIX and Linux: /usr/openv/netbackup/logs/vault  
Windows: install_path\NetBackup\logs\vault
Review the `summary.log` in each of the `sidxxx` directories that had problems:

UNIX and Linux:
/usr/openv/netbackup/vault/sessions/vault_name/sidxxx
Windows:
`install_path\NetBackup\vault\sessions\vault_name\sidxxx`

(where `xxx` is the session ID)

In addition, review the admin debug log in the following directory:

UNIX and Linux: `/usr/openv/netbackup/logs/admin`
Windows: `install_path\NetBackup\logs\admin`

Correct the error and rerun the Vault session.

**NetBackup status code: 303**

**Message:** error encountered executing Media Manager command

**Explanation:** This error occurs when a Media and Device Management command fails during a Vault job.

**Recommended Action:** For the actual error that caused the command to fail, review the Vault debug log in the following directory:

UNIX and Linux: `/usr/openv/netbackup/logs/vault`
Windows: `install_path\NetBackup\logs\vault`

Also review the `summary.log` in each of the `sidxxx` directories that had problems:

UNIX and Linux:
/usr/openv/netbackup/vault/sessions/vault_name/sidxxx
Windows:
`install_path\NetBackup\vault\sessions\vault_name\sidxxx`

(where `xxx` is the session ID)

Try running the command (with the same arguments as in the log file) to see the actual error. Ensure that the Media and Device Management daemons are running. Also ensure that the robot is functional and you can communicate with it (for example, inventory the robot through the GUI).

**NetBackup status code: 304**

**Message:** specified profile not found

**Explanation:** This error occurs when the profile name that is specified on the Vault command is not defined in the Vault configuration.
**Recommended Action:** Rerun the Vault command with a profile name that is defined in the Vault configuration.

**NetBackup status code: 305**

**Message:** multiple profiles exist

**Explanation:** This error may occur when duplicate profile names are defined in multiple Vault configurations and only the profile name is specified on the Vault command.

**Recommended Action:** Rerun the Vault command with the triplet `robot_name/vault_name/profile_name`. The triplet uniquely identifies the profile in your Vault configuration.

**NetBackup status code: 306**

**Message:** vault duplication partially succeeded

**Explanation:** This error occurs when all selected images are not duplicated successfully.

**Recommended Action:** Check the Vault and `induplicate` logs for cause of the failure.

**NetBackup status code: 307**

**Message:** eject process has already been run for the requested Vault session

**Explanation:** This error occurs when `vlteject` is run to eject media for a session ID for which media has already been ejected.

**Recommended Action:** Rerun `vlteject` for another session ID for which media has not been ejected.

**NetBackup status code: 308**

**Message:** no images duplicated

**Explanation:** This error occurs when Vault failed to duplicate any images.

**Recommended Action:** For more information, review the Vault debug log in the following directory:

- UNIX and Linux: `/usr/openv/netbackup/logs/vault`
- Windows: `install_path\NetBackup\logs\vault`

Also review the `summary.log` in each of the `sidxxx` directories that had problems:
UNIX and Linux:
/usr/openv/netbackup/vault/sessions/<vault_name/>sidxxx
Windows:
install_path\NetBackup\vault\sessions\vault_name\sidxxx

(where vault_name is the name of the vault, and xxx is the session ID)

Look for the log entry that gives the total number of images processed. A common cause of failure is a lack of resources, such as no more media available in the specified pools for duplication. Correct the problem and rerun the Vault job. Note that the NetBackup scheduler retries a Vault job that terminates with this error. Review the admin debug log for induplicate entries and the bptm debug log.

**NetBackup status code: 309**

**Message:** report requested without eject being run

**Explanation:** This error occurs when a report is run that requires media to have been ejected first.

**Recommended Action:** Perform one of these actions:

- Rerun vlteject or vltopmenu to eject the media for the session before you generate the reports.
- Reconfigure the profile to allow the eject step to be performed when the next Vault session for this profile runs.
- Disable the report generation in the profile for the reports that require media to be ejected.

**NetBackup status code: 310**

**Message:** Updating of Media Manager database failed

**Explanation:** This error occurs when Vault physically ejects tapes but fails to update the EMM database to reflect the eject operation. A typical reason for this failure is that EMM detected a mismatch between the media type and its volume group.

**Recommended Action:** To find the root cause of the error, review the Vault debug logs in the following directory:

UNIX and Linux: /usr/openv/netbackup/logs/vault
Windows: install_path\NetBackup\logs\vault

To fix the issue may involve making configuration changes.
NetBackup status code: 311

Message: Iron Mountain Report is already created for this session

Explanation: This error occurs when an Iron Mountain report has already been generated for the session.

Recommended Action: None. This report cannot be generated again.

NetBackup status code: 312

Message: invalid container database entry

Explanation: NetBackup Vault has found an invalid entry while reading the container database. Each container entry in the container database must follow the expected format. The container database exists in file cntrDB, which is located at ${install_path}/netbackup/vault/sessions/cntrDB.

Recommended Action: To get the line number of an invalid record in the container database, read the log file under the directory netbackup/logs/vault. Be aware that a Vault log may not exist unless the directory netbackup/logs/vault existed before the error occurred. Open the container database file cntrDB and correct that invalid entry. Note that this error occurs every time Vault reads this entry in cntrDB until either this invalid entry is deleted or it is corrected.

NetBackup status code: 313

Message: container does not exist in container database

Explanation: The specified container does not have an entry in the container database. The container database exists in file cntrDB, which is located at ${install_path}/netbackup/vault/sessions/cntrDB.

Recommended Action: Verify that you put some media into this container by using the vltcontainers command. Verify that you did not delete it by using the vltcontainers -delete command.

NetBackup status code: 314

Message: container database truncate operation failed

Explanation: An error occurs while truncating the container database. This error may occur during the modification or deletion of an entry from the container database. The container database exists in file cntrDB, which is located at ${install_path}/netbackup/vault/sessions/cntrDB.
**Recommended Action:** See the log file under the directory `netbackup/logs/vault` for more details. Be aware that a log file is not created unless the `netbackup/logs/vault` directory has already been created.

**NetBackup status code: 315**

**Message:** failed appending to container database

**Explanation:** This error can occur while appending a container record to the container database. This error may occur with the addition, modification, or deletion of an entry from the container database. The container database exists in file `cntrDB`, which is located at `install_path/netbackup/vault/sessions/cntrDB`.

**Recommended Action:** Read the relevant log file under the directory `install_path/netbackup/logs/vault` for more details. Be aware that if this directory does not already exist, a log file is not created.

**NetBackup status code: 316**

**Message:** container_id is not unique in container database

**Explanation:** NetBackup Vault has found a previously-existing entry for this container ID in the container database while adding it to the container database. Each container record in the container database must have a unique container ID. Note that the container database exists in file `cntrDB`, which is located at `install_path/netbackup/vault/sessions/cntrDB`.

**Recommended Action:** Verify that you have specified the correct container ID.

**NetBackup status code: 317**

**Message:** container database close operation failed

**Explanation:** This error occurs while closing the container database. This error may occur during the reading, addition, modification, or deletion of an entry from the container database. Note that the container database exists in file `cntrDB`, which is located at `install_path/netbackup/vault/sessions/cntrDB`.

**Recommended Action:** Read the relevant log file under the directory `netbackup/logs/vault` for more details. Be aware that if this directory does not already exist, a log file is not created.

**NetBackup status code: 318**

**Message:** container database lock operation failed
**Explanation:** This error occurs while locking the container database. This error may occur during the addition, modification, or deletion of an entry from the container database. Note that the container database exists in file cntrDB, which is located at `install_path/netbackup/vault/sessions/cntrDB`.

**Recommended Action:** Read the relevant log file under the directory `netbackup/logs/vault` for more details. Be aware that if this directory does not already exist, a log file is not created.

If some other Vault operation uses the container database and locks it, wait until that operation completes and the container database is unlocked.

**NetBackup status code: 319**

**Message:** container database open operation failed

**Explanation:** This error occurs while opening the container database. This error may occur during the reading, addition, modification, or deletion of an entry from the container database. Note that the container database exists in file cntrDB, which is located at `install_path/netbackup/vault/sessions/cntrDB`.

**Recommended Action:** Read the relevant log file under the directory `netbackup/logs/vault` for more details. Be aware that if this directory does not already exist, a log file is not created.

**NetBackup status code: 320**

**Message:** the specified container is not empty

**Explanation:** This error occurs if you try to delete a container from the container database, but the container still holds media. You can only delete empty containers.

**Recommended Action:** Verify that you have specified the correct container ID.

If you still want to delete this container from the container database, first empty it by doing either of the following:

- Inject all the media it contains into a robot
- Clear the Vault container ID fields for these media from the EMM database by using `vmchange -vltcid` with a value of `-`.

Try to delete the container again.

**NetBackup status code: 321**

**Message:** container cannot hold any media from the specified robot

**Explanation:** This error occurs while trying to place media from an unexpected EMM database host into a container. All the media that are placed in a container...
should belong to the same EMM database host. For example, you have media from a robot that belongs to one EMM database host. Then you try to put this media into a container that already holds media from the robots that belong to a different EMM database host.

**Recommended Action:** Verify that you specified the correct container ID and media IDs. Read the relevant log file under the directory `install_path/netbackup/logs/vault` for more details. Be aware that if this directory does not already exist, a log file is not created.

**NetBackup status code: 322**

**Message:** cannot find vault in vault configuration file

**Explanation:** NetBackup Vault cannot find an entry for the specified Vault name into the Vault configuration file. Note that the Vault configuration file is located at `install_path/netbackup/db/vault/vault.xml`.

**Recommended Action:** Verify that you specified the correct Vault name. Read the relevant log file under the directory `netbackup/logs/vault` for more details. Be aware that if this directory does not already exist, a log file is not created.

**NetBackup status code: 323**

**Message:** cannot find robot in vault configuration file

**Explanation:** NetBackup Vault cannot find an entry for the specified robot number in the Vault configuration file. Note that the Vault configuration file is located at `install_path/netbackup/db/vault/vault.xml`.

**Recommended Action:** Verify that you specified the correct robot number. Read the relevant log file under the directory `netbackup/logs/vault` for more details. Be aware that if this directory does not already exist, a log file is not created.

**NetBackup status code: 324**

**Message:** invalid data found in retention map file for duplication

**Explanation:** This error occurs when the retention mapping file (either generic or for a specific vault) contains invalid data. If the file contains too much or too little data or the user defines invalid retention levels in the file, this error occurs.

The retention mapping file is used as follows: in a Vault session when a Vault profile duplication is configured with the Use mappings retention level configured for one of the copies for duplication. The product installs a mapping file template named `retention_mappings` in `install_path/netbackup/db/vault`.
To specify a mappings file for any single vault, copy the retention_mappings template to another file and append the name of the vault. For example, netbackup/db/vault/retention_mappings.V1

**Recommended Action:** Check the entries in the retention_mappings file.

**NetBackup status code: 325**

**Message:** unable to find policy/schedule for image using retention mapping

**Explanation:** This error occurs with duplication of the backup policy or the schedule of an image by Vault. The Use mappings option on the Duplication tab of the Profile dialog box is selected, but the policy or the schedule no longer exists.

**Recommended Action:** Verify whether or not the backup policy or the schedule that created the image still exists. If either one or both do not exist, the image is not duplicated through the Vault profile.

**NetBackup status code: 326**

**Message:** specified file contains no valid entry

**Explanation:** The specified file contains no valid entries for media IDs or the alphanumeric equivalent of bar codes. As per the expected format, each line should contain only one string that represents either a media ID or the bar code numeric equivalent.

**Recommended Action:** Verify that each entry in the specified file does not exceed the string size limit: six characters for media IDs and 16 characters for the numeric equivalent of bar codes. Correct the invalid entries in the specified file and try the same operation again. Read the relevant log file under the directory install_path/netbackup/logs/vault for more details. Be aware that if this directory does not already exist, a log file is not created.

**NetBackup status code: 327**

**Message:** no media ejected for the specified vault session

**Explanation:** This error occurs while moving media ejected by the specified Vault session to a container. Either the specified Vault session has not ejected any media, or you specified an incorrect Vault name or session ID.

**Recommended Action:** Verify that you have specified the correct combination of Vault name and session ID. Verify that the specified Vault session has ejected at least one piece of media. Read the relevant log file under the directory netbackup/logs/vault for more details. Be aware that if this directory does not already exist, a log file is not created.
NetBackup status code: 328
Message: invalid container id

Explanation: This error occurs while adding a container record to the container database. The container ID is found invalid. Note that the container database exists in file cntrDB, which is located at install_path/netbackup/vault/sessions/cntrDB.

Recommended Action: Verify that the container ID does not contain any space characters, and that the string size is a maximum of 29 characters long.

NetBackup status code: 329
Message: invalid recall status

Explanation: This error occurs while adding a container record to the container database. The container recall status is found invalid. Note that the container database exists in file cntrDB, which is located at install_path/netbackup/vault/sessions/cntrDB.

Recommended Action: Verify that the recall status is either 1 or 0.

NetBackup status code: 330
Message: invalid database host

Explanation: This error occurs while adding a container record to the container database. The EMM database host name is found invalid. Note that the container database exists in file cntrDB, which is located at install_path/netbackup/vault/sessions/cntrDB.

Recommended Action: Verify that the EMM database host name does not contain any space characters, and that the string size is a maximum of 256 characters long.

NetBackup status code: 331
Message: invalid container description

Explanation: This error occurs while adding a container record to the container database. The container description is found invalid. Note that the container database exists in file cntrDB, which is located at install_path/netbackup/vault/sessions/cntrDB.

Recommended Action: Verify that the string size of the container description is a maximum of 25 characters long.
NetBackup status code: 332
Message: error getting information from EMM database
Explanation: This error can occur while the backup process communicates with the EMM database to retrieve some information.
Recommended Action: Do the following, as appropriate:
- On UNIX and Linux, verify that the NetBackup Volume Manager (vmd) is running. On Windows, verify that the NetBackup Volume Manager service is running.
- See the process-specific error log directory for more details.
  UNIX and Linux: /usr/openv/netbackup/logs/process_name
  Windows: install_path\NetBackup\logs\process_name
For example, if you get this error while running a Vault command (such as vltcontainers or vltopmenu), look at the following logs to learn why:
  /usr/openv/netbackup/logs/vault

Note: The log file cannot be created unless the appropriate log directory such as /usr/openv/netbackup/logs/vault is already created.

NetBackup status code: 333
Message: error getting information from media manager command line
Explanation: This error occurs when Vault cannot retrieve robot information such as map information, volume information, library status, and so on. It is an internal error.
Recommended Action: Contact customer support and send appropriate logs.

NetBackup status code: 334
Message: unable to receive response from robot; robot not ready
Explanation: This error occurs when a problem exists with the robot.
Recommended Action: Ensure that all Media and Device Management daemons are running or the robot is live and up.

NetBackup status code: 335
Message: failure occurred while suspending media for eject
**Explaination:** This error occurs when Vault cannot suspend the media. It is an internal error.

**Recommended Action:** Contact customer support and send appropriate logs.

**NetBackup status code:** 336

**Message:** failure occurred while updating session information

**Explanation:** Vault cannot update the session files. It is an internal error.

**Recommended Action:** Contact customer support and send appropriate logs.

**NetBackup status code:** 337

**Message:** failure occurred while updating the eject.mstr file

**Explanation:** Vault cannot update the eject list file. It is an internal error.

**Recommended Action:** Contact customer support and send appropriate logs.

**NetBackup status code:** 338

**Message:** vault eject timed out

**Explanation:** This error occurs when a problem exists with the robot.

**Recommended Action:** Do the following, as appropriate:

- Remove the media from the MAP if it is already full.
- Make sure that the MAP is closed properly.

**NetBackup status code:** 339

**Message:** vault configuration file format error

**Explanation:** The Vault configuration file is malformed. Unless the file has been manually modified, this error is internal. Note that the Vault configuration file is located at `install_path/netbackup/db/vault/vault.xml`.

**Recommended Action:** Contact customer support and send appropriate logs.

**NetBackup status code:** 340

**Message:** vault configuration tag not found

**Explanation:** An optional attribute may not appear in the Vault configuration file. This internal error generally does not cause problems in Vault's operation. Note that the Vault configuration file is located at `install_path/netbackup/db/vault/vault.xml`. 
**Recommended Action:** If Vault's operation is affected, contact customer support and send appropriate logs.

**NetBackup status code: 341**
**Message:** vault configuration serialization failed

**Explanation:** Vault failed to write out the Vault configuration file. It is an internal error. Note that the Vault configuration file is located at `install_path/netbackup/db/vault/vault.xml`.

**Recommended Action:** Contact customer support and send appropriate logs.

**NetBackup status code: 342**
**Message:** cannot modify - stale view

**Explanation:** This error can occur if an administration interface (NetBackup Administration Console or Vault Administration menu user interface) tries to modify the following:

- A robot or vault or profile in between the read
- Operations of the same robot or vault
- Profile by another instance of an administration interface

**Recommended Action:** Check the latest attributes of the robot or vault or profile. To check, refresh the view in the NetBackup Administration Console or retrieve the attributes in the Vault Administration menu user interface again. Then retry the operation.

**NetBackup status code: 343**
**Message:** robot already exists

**Explanation:** This error can occur during addition of a robot while a robot with the same name already exists.

**Recommended Action:** Refresh the view in the NetBackup Administration Console or retrieve the attributes in the Vault Administration menu user interface again to see the robot.

**NetBackup status code: 344**
**Message:** vault already exists

**Explanation:** This error can occur during addition of a vault if a vault with the same name already exists in the same robot.
Recommended Action: Choose a different name for the vault.

NetBackup status code: 345
Message: profile already exists
Explanation: This error can occur during addition of a profile if a profile with the same name already exists within the same vault.
Recommended Action: Choose a different name for the profile.

NetBackup status code: 346
Message: duplicate MAP
Explanation: A duplicate MAP was added in the Vault configuration file. It is an internal error.
Recommended Action: Contact customer support and send appropriate logs.

NetBackup status code: 347
Message: vault configuration cache not initialized
Explanation: This error should never occur.
Recommended Action: Contact customer support and send appropriate logs.

NetBackup status code: 348
Message: specified report does not exist
Explanation: An invalid Vault report was requested for generation. It is an internal error.
Recommended Action: Contact customer support and send appropriate logs.

NetBackup status code: 349
Message: incorrect catalog backup policy
Explanation: This error can occur when a Vault session tries to run a catalog backup. The specified policy for the catalog backup in the Vault profile is either blank or is not of type NBU-Catalog.
Recommended Action: Verify that you specified a catalog backup policy for the catalog backup in the Vault profile and that the policy is of type NBU-Catalog.
NetBackup status code: 350

Message: incorrect vault catalog backup schedule

Explanation: This error can occur when a Vault session tries to run a catalog backup. The specified Vault catalog backup schedule for catalog backup in the Vault profile is either blank or is not of type Vault Catalog Backup.

Recommended Action: Verify that you specified a Vault Catalog Backup schedule for the catalog backup in the Vault profile. Also verify that the schedule is of type Vault Catalog Backup.

NetBackup status code: 351

Message: all configured vault steps failed

Explanation: This error occurs when multiple Vault steps are configured for a session and all of them fail.

Recommended Action: For duplication and catalog backup steps, use the Activity Monitor to check the status of the respective jobs that Vault started. For Eject step status, check the Detailed Status tab of the Job Details dialog box for the Vault job.

NetBackup status code: 400

Message: Server Group Type is Invalid

Explanation: The creation of a server group fails because the server group type is invalid.

Recommended Action: Do the following, as appropriate:

- Select a valid server group type: MediaSharing, &CompanyName; OpsCenter, or AltServerRestore.
- For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for nbemm (originator ID 111), which uses unified logging.

NetBackup status code: 401

Message: Server Group Already Exists

Explanation: The attempt to create a server group failed. The server group already exists.

Recommended Action: Do the following, as appropriate:

- Verify that the specified server group name is not in use.
Create the server group by specifying a name that is not currently in use.

For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for nbemm (originator ID 111), which uses unified logging.

**NetBackup status code: 402**

**Message:** Server Group Already Exists with a different type

**Explanation:** The attempt to create a server group failed. The server group name is already in use by a server group with a different group type.

**Recommended Action:** Do the following, as appropriate:

- Verify that the specified server group name is not in use.
- Try to create the server group by specifying a name that is not currently in use.
- For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for nbemm (originator ID 111), which uses unified logging.

**NetBackup status code: 403**

**Message:** Server Group Active State is not valid

**Explanation:** The attempt to create a server group failed. The server group state was invalid.

**Recommended Action:** Do the following, as appropriate:

- Valid server group states are: ACTIVE and INACTIVE
- For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for nbemm (originator ID 111), which uses unified logging.

**NetBackup status code: 404**

**Message:** Server Group does not exist

**Explanation:** An operation was tried by using a server group that does not exist.

**Recommended Action:** Do the following, as appropriate:

- Verify that the specified media is correct.
- Verify the media ownership.
- Verify that the server group exists.
- Verify that the server where the operation is performed is a member of the owning server group. If not, try the operation from a server that is a member of the server group.
- For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for nbemm (originator IDs 111 and 143), which uses unified logging.

**NetBackup status code: 405**

**Message:** Member’s server type not compatible with Server Group

**Explanation:** The attempt to add or update a server group failed. A member’s server type was not valid for the specified server group type.

**Recommended Action:** Do the following, as appropriate:

- The Media Sharing server group can contain the following types of servers: Master, Media, NDMP, and cluster.
- For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for nbemm (originator IDs 111 and 143), which uses unified logging.

**NetBackup status code: 406**

**Message:** The computer specified is not a member of the server group specified

**Explanation:** A server that is not a member of the server group that owns the media performed an operation on a media.

**Recommended Action:** Do the following, as appropriate:

- Verify that the specified media is correct.
- Verify the media ownership
- Verify that the server where the operation is performed is a member of the owning server group. If not, try the operation from a server that is a member of the server group.
- For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for nbemm (originator IDs 111 and 143), which use unified logging.
NetBackup status code: 407

Message:  Member’s NetBackup version not compatible with Server Group

Explanation:  The attempt to add or update a server group failed. One of the server group member’s NetBackup version is not valid for the specified server group type.

Recommended Action:  Do the following, as appropriate:

■  Ensure that each member server has NetBackup 6.5 or later.

■  For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for nbemm (originator IDs 111 and 143), which uses unified logging.

NetBackup status code: 408

Message:  Server Group is in use

Explanation:  The attempt to delete a server group that failed because the server group owns one or more media.

Recommended Action:  Do the following, as appropriate:

■  Ensure that the server group is not the owner of any media by running `bpmedialist -owner group_name` from the master server.

■  For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for nbemm (originator IDs 111 and 143), which uses unified logging.

NetBackup status code: 409

Message:  Member already exists in server group

Explanation:  The attempt to add or update a server group failed because one of the server group members is the same as the one being added.

Recommended Action:  Do the following, as appropriate:

■  Ensure that the server group member that you add does not already exist in the group.

■  For detailed troubleshooting information, create the admin debug log directory and retry the operation. Check the resulting debug logs. Additional debug information can be found in the log for nbemm (originator IDs 111 and 143), which uses unified logging.
NetBackup status code: 501

Message: You are not authorized to use this application.

Explanation: The user is not authorized to use one of the NetBackup Java Administration utilities on the host that is specified in the login dialog box.

Recommended Action: Check the auth.conf file on the host that is specified in the NetBackup-Java login dialog box for the proper authorization. If the auth.conf file does not exist, it must be created with the proper entry for this user name. More details on the auth.conf file are available.


NetBackup status code: 502

Message: No authorization entry exists in the auth.conf file for user name username. None of the NB-Java applications are available to you.

Explanation: The user name is not authorized to use any NetBackup-Java applications on the host that is specified in the logon dialog box.

Recommended Action: Check the auth.conf file on the computer (host name) specified in the NetBackup-Java logon dialog box for the proper authorization. If the file does not exist, create it with the proper entry for this user name. More details on the auth.conf file are available.


NetBackup status code: 503

Message: Invalid username.

Explanation: For UNIX and Linux host logon, the NetBackup Java application server on the host where the logon is requested does not recognize the user name.

For Windows host logon, the NetBackup-Java authentication service on the host where the logon is requested does not have sufficient privileges to grant the request.

Recommended Action: Do the following, as appropriate:

- For UNIX and Linux hosts: the user name must be a valid user name in the passwd file on the host that is specified in the logon dialog box.

- For Windows hosts: refer to the LogonUser function in the section titled Client/Server Access Control Functions of the Windows Platform Software Developer's Kit to determine the required privileges.
**NetBackup status code: 504**

**Message:** Incorrect password.

**Explanation:** For logon to a UNIX or Linux host, the user name is recognized on the host where the logon is requested, but the supplied password is incorrect.

For logon to a Windows host, the attempt to log in the user failed. The failure can be due to an unrecognized user in the specified domain.

**Recommended Action:** Do the following, as appropriate:

- Enter the correct password.
- On Windows hosts: The exact error can be found in the `bpjava-msvc` log file.

For more details, refer to the LogonUser function in the section Client/Server Access Control Functions of the *Windows Platform Software Developer’s Kit*.

---

**NetBackup status code: 505**

**Message:** Can not connect to the NB-Java authentication service on *host* on the configured port - *(port_number)*. Check the log file for more details.

**Explanation:** The initial connection from the NetBackup-Java interface to its authentication service on *(host)* was on the configured_port_number that was mentioned in the error message. Either the port is in use by another application or the NetBackup-Java interface and its application server are not configured with the same port. The default port is 13722. The NetBackup Administration Console log file should contain more detail about this error.

**Recommended Action:** Do the following, as appropriate:

- On UNIX and Linux, compare the `bpjava-msvc` entry in the `/etc/services` file with the `BPJAVA_PORT` entry in the `/usr/openv/java/nbj.conf` file.
- On Windows, compare the `bpjava-msvc` entry in the `%systemroot%\system32\drivers\etc\services` file with the `install_path\java\setconf.bat` file (Windows). The entries must match.
- Ensure that no other application uses the port that is configured for the NetBackup-Java interface.

---

**NetBackup status code: 506**

**Message:** Cannot connect to the NB-Java user service on *host* on port *(port_number)*. If successfully logged in before, retry your last operation. Check the log file for more details.

**Explanation:** After the NetBackup-Java authentication service validates the user name, a NetBackup-Java user service is used for all other service requests from
the NetBackup-Java interface. Communication was tried between the NetBackup-Java interface and the user service on host (host) on the port number that was specified in the error message. More information about various port configuration options is available.


The NetBackup Administration Console log file should contain more detail about this error.

- On UNIX and Linux: the port configuration options are specified in the /usr/openv/netbackup/bp.conf file or through Administration Console Host Properties.
- On Windows: from the NetBackup Administration Console, select Host Properties. Select Properties on the Actions menu. The Port Ranges tab contains the port options.

**Recommended Action:** Do the following, as appropriate:

- Restart the NetBackup-Java interface and log in again.
- If the problem persists, enable detailed debug logging.
- Restart the NetBackup-Java interface and examine the logs.

**NetBackup status code: 507**

**Message:** Socket connection to the NB-Java user service has been broken. Retry your last operation. Check the log file for more details.

**Explanation:** The connection was broken to the NetBackup Java application server that is running on the NetBackup host (where you are logged in). The NetBackup Administration Console log file should contain more detail about this error.

**Recommended Action:** Do the following, as appropriate:

- Retry the last operation.
- If the problem persists, restart the NetBackup-Java interface and try again.
- If the problem still persists, enable detailed debug logging.
  See “Enabling detailed debug logging” on page 125.
- Restart the NetBackup-Java interface and examine the logs.

**Note:** You may have network or system problems unrelated to NetBackup.
NetBackup status code: 508

Message: Can not write file.

Explanation: This cause of this error is one of the following:

- The NetBackup-Java user service tries to write to a file that does not have write permissions. The solution is to enable write privileges.
- The NetBackup-Java user service tries to write to a temporary file whose unique name cannot be constructed. This condition is unlikely, but can result from an exhaustion of system resources (from the filling of the name space).

Recommended Action: Retrieve the specific details from the user service log files.
Enable detailed debug logging as explained in the following topic:
See “Enabling detailed debug logging” on page 125.

NetBackup status code: 509

Message: Can not execute program.

Explanation: The NetBackup-Java authentication or user service reported an error that relates to the creation (or demise) of a child job process. The NetBackup-Java service programs create separate jobs to accomplish specific tasks, as follows. The NetBackup-Java authentication service creates the NetBackup-Java user service. When it is created and connected to, the NetBackup-Java user service creates all other child processes on behalf of requests from the NetBackup-Java interface.

The cause of status code 509 can be found in the appropriate log file, either for bpjava-msvc, bpjava-susvc, or bpjava-usvc.
The cause can be categorized as one of the following:

- A job (started by either the NetBackup-Java authentication service or user service) no longer exists and did not report its result status.
- The NetBackup-Java service cannot monitor a job (started by either the NetBackup-Java authentication service or user service). The reason it cannot monitor is probably due to a lack of system resources (insufficient memory).
- The maximum number of non-transient activity monitor jobs (>100) have already been started.

Recommended Action: Do the following, as appropriate:

- If the problem persists, restart the NetBackup-Java interface and try again.
If the problem still persists, enable detailed debug logging as explained in the following topic:
See “Enabling detailed debug logging” on page 125.

Restart the NetBackup-Java interface and examine the logs.

The error is probably the result of a system resource issue. When detailed debug logging is enabled, you can retrieve the details from the bpjava-msvc, bpjava-susvc, or bpjava-usvc log files.

**NetBackup status code: 510**

**Message:** File already exists: *file_name*

**Explanation:** The NetBackup-Java user service try to create a file that already exists.

**Recommended Action:** Remove the file, which can be identified in the user service log files.

See “Troubleshooting the Administration Console for UNIX” on page 123.

**NetBackup status code: 511**

**Message:** NB-Java application server interface error.

**Explanation:** In some instances, this message concludes with "Check the log file for more details."

This generic error for all non-socket IO/connection-broken related errors (status code 507) can occur when data is processed from the NetBackup-Java authentication or user services. The Java exception provides some additional detail about the error.

This error usually results from system or network problems.

**Recommended Action:** Do the following, as appropriate:

■ If the problem persists, restart the NetBackup-Java interface and try again.

■ If the problem still persists, enable detailed debug logging as explained in the following topic:
  See “Enabling detailed debug logging” on page 125.

■ Restart the NetBackup-Java interface and examine the logs.

The error is probably the result of a system resource issue. When detailed debug logging is enabled, the details can be retrieved from the bpjava-msvc, bpjava-susvc, or bpjava-usvc log files.
**NetBackup status code: 512**

**Message:** Internal error - a bad status packet was returned by NB-Java application server that did not contain an exit status code.

**Explanation:** The NetBackup-Java authentication or user service returned a data packet that indicated an error, but no status code or error message was contained within it.

**Recommended Action:** Do the following, as appropriate:

- If the problem persists, restart the NetBackup-Java interface and try again.
- If the problem still persists, enable detailed debug logging as explained in the following topic:
  See “Enabling detailed debug logging” on page 125.
- Restart the NetBackup-Java interface and examine the logs.

The error is probably the result of a system resource issue. When detailed debug logging is enabled, the details can be retrieved from the `bpjava-msvc`, `bpjava-susvc`, or `bpjava-usvc` log files.

**NetBackup status code: 513**

**Message:** `bpjava-msvc`: the client is not compatible with this server version (`server_version`).

**Explanation:** The NetBackup-Java application server (on the remote host you log in to) is not the same version as the NetBackup-Java interface on your local host. The two are therefore incompatible.

**Recommended Action:** Do the following, as appropriate:

- Log in to a different NetBackup remote host.
- Upgrade the NetBackup software on either of the following: the computer that is specified in the logon dialog box or the local host where you started the NetBackup Java interface.

**NetBackup status code: 514**

**Message:** NB-Java: `bpjava-msvc` is not compatible with this application version (`application_version`). You may try logon to a different NetBackup host or exit the application. The remote NetBackup host has to be configured with the same version of NetBackup as the host you started the application on.

**Explanation:** In some instances, this message concludes with "Check the log file for more details."
The NetBackup-Java application server (on the remote host you log in to) is not the same version as the NetBackup-Java interface on your local host. The two are therefore incompatible.

**Recommended Action:** Do the following, as appropriate:

- Log in to a different NetBackup remote host.
- Upgrade the NetBackup software on either of the following: the specified computer in the logon dialog box or the local host where you started the NetBackup Java interface.

**NetBackup status code: 516**

**Message:** Could not recognize or initialize the requested locale - *(locale_NB-Java_was_started_in)*.

**Explanation:** This status concerns the UNIX or Linux locale configuration (or Windows regional settings) defined on the host that was specified in the NB-Java logon dialog box. At logon, the locale configuration is passed to the NB-Java authentication service. Status 516 is generated if the locale is not recognized or if the locale of the user service cannot be initialized.

The rules in the following files determine how a valid locale is recognized: 
`/usr/openv/msg/.conf` on UNIX and Linux and `install_path\msg\lc.conf` on Windows. When the locale is validated, initialization of the locale in the user service’s environment is tried (by means of `setlocale`).

**Recommended Action:** On the specified host in the NB-Java logon dialog box, check the configuration file to ensure that a mapping is available for the indicated locale.

For information on locale configuration and mapping, refer to the *NetBackup Administrator's Guide, Volume II*.

If there is a mapping, try to set the mapped locale on the host that was specified in the NB-Java logon dialog box. This system may not be configured properly.

**NetBackup status code: 517**

**Message:** Can not connect to the NB-Java user service via VNETD on *host* on port *configured_port_number*. If successfully logged in beforehand, retry your last operation. Check the log file for more details.

**Explanation:** After the NB-Java authentication service validates the user name on the logon dialog box for access, all Administration console service requests use an NB-Java user service. Communication between the Administration console and user service is tried to host (host) on the specified port number in the error message by using VNETD. (The NB-Java configuration option
NBJAVA_CONNECT_OPTION is set to 1.) The NetBackup Administration Console log file should contain more detail about this error.

**Recommended Action:** Do the following, as appropriate:

- On UNIX and Linux: Compare the VNETD entry in the `/etc/services` file with the VNETD_PORT entry in `/usr/openv/java/nbj.conf`.
  - On Windows: Compare the VNETD entry with the VNETD_PORT entry in the `install_path\java\setconf.bat` file.
  - These entries must match.
- Ensure that no other application uses the port that is configured for VNETD.

**NetBackup status code: 518**

**Message:** No ports available in range (port_number) through (port_number) per the NBJAVA_CLIENT_PORT_WINDOW configuration option.

**Explanation:** All the ports in the specified range are in use. Too many users (concurrent) of the NetBackup-Java interface or too few configured ports can cause this error.

**Recommended Action:** Do the following, as appropriate:

- Restart the NetBackup-Java interface and try again.
- If the problem persists, increase the range of ports by changing the NBJAVA_CLIENT_PORT_WINDOW option in the `/usr/openv/java/nbj.conf` file (UNIX and Linux) or the `install_path\java\setconf.bat` file (Windows).

**NetBackup status code: 519**

**Message:** Invalid NBJAVA_CLIENT_PORT_WINDOW configuration option value: (option_value).

**Explanation:** The value for the NB-Java configuration option NBJAVA_CLIENT_PORT_WINDOW is invalid.

**Recommended Action:** Correct the value in file `/usr/openv/java/nbj.conf` (UNIX and Linux) or `install_path\java\setconf.bat` file (Windows).

**NetBackup status code: 520**

**Message:** Invalid value for NB-Java configuration option (option_name): (option_value).

**Explanation:** The specified NetBackup-Java configuration option has an invalid value.
Recommended Action: Correct the value in file `/usr/openv/java/nbj.conf` (UNIX and Linux) or `install_path\java\setconf.bat` file (Windows).

NetBackup status code: 521
Message: NB-Java Configuration file (`file_name`) does not exist.
Explanation: The configuration file for the NetBackup-Java interface was not found.
Recommended Action: Make sure that the configuration file the NetBackup-Java interface exists and is properly formatted.

NetBackup status code: 522
Message: NB-Java Configuration file (`file_name`) is not readable due to the following error: (`message`).
Explanation: The specified NetBackup-Java configuration file exists but is not readable.
Recommended Action: Correct the file as specified in the message.

NetBackup status code: 523
Message: NB-Java application server protocol error.
Explanation: In some instances, this message concludes with "Check the log file for more details."
The NetBackup-Java interface received an incorrectly formatted protocol sequence from its application server.
Recommended Action: Do the following, as appropriate:
- If the problem persists, restart the NetBackup-Java interface and try again.
- If the problem still persists, enable detailed debug logging as explained in the following topic:
  See “Enabling detailed debug logging” on page 125.
- Restart the NetBackup-Java interface and examine the logs.

Note: The error is probably the result of a system resource issue. When detailed debug logging ID is enabled, the details can be retrieved from the `bpjava-msvc`, `bpjava-susvc`, or `bpjava-usvc` log files.
NetBackup status code: 525

Message: Cannot connect to the NB-Java authentication service via VNETD on (host) on port (vnetd_configured_port_number). Check the log file for more details.

Explanation: The NB-Java authentication service authenticates the user name that is provided in the logon dialog box. Communication between the NetBackup Administration Console and the authentication service is tried to host host on the configured VNETD port number that error message specifies. The NetBackup Administration Console log file should contain more detail about this error.

Recommended Action: Do the following, as appropriate:

- On UNIX and Linux: Compare the VNETD entry in the /etc/services file with the VNETD_PORT entry in /usr/openv/java/nbj.conf
  On Windows: Compare the VNETD entry with the VNETD_PORT entry in the install_path\java\setconf.bat file.
  These entries must match.
- Ensure that no other application uses the port that is configured for VNETD.

NetBackup status code: 526

Message: bpjava authentication service connection failed

Explanation: Cannot connect to the bpjava authentication service via NetBackup PBX at port 1556 (default).

Recommended Action: Do the following, as appropriate:

- Check that the PBX service or daemon has been started on the server and that NetBackup services are running.
- If the target server is running a release of NetBackup earlier than 7.0.1, the Java GUI attempts a further connection via the VNETD port 13724. No action is required.
- Check if the Java GUI properties (java/nbj.conf) have been set up to connect to a PBX port other than 1556.

NetBackup status code: 527

Message: bpjava user service connection if connection to pbx on port 1556 fails

Explanation: Unable to connect to the bpjava user service using NetBackup PBX at port 1556 (default).

Recommended Action: Do the following, as appropriate:

- Check that the PBX service or daemon has been started on the server and that NetBackup services are running.
- If the target server is running a release of NetBackup earlier than 7.0.1, the Java GUI attempts a further connection via the VNETD port 13724. No action is required.

- Check if the Java GUI properties (java/nbj.conf) have been modified to attempt a PBX port other than 1556.

**NetBackup status code: 600**

**Message:** an exception condition occurred

**Explanation:** The synthetic backup job encountered an exception condition.

**Recommended Action:** Contact customer support and send appropriate debug logs.

A complete list of required logs and configuration information is available.

See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 601**

**Message:** unable to open listen socket

**Explanation:** The bpsynth process cannot open a socket to listen for incoming connections from the bptm or the bpdm processes that were started for the following: for reading backup images or for writing the synthetic image on the media servers.

**Recommended Action:** Check the OS error that was reported in the error message, which bpsynth logged in the NetBackup error log. This error helps to diagnose the problem. Ensure that the bpsynth binary matches the installed NetBackup version. Retry the synthetic backup job. If the problem persists, contact customer support and provide the appropriate logs.

A complete list of required logs and configuration information is available.

See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 602**

**Message:** cannot set non blocking mode on the listen socket

**Explanation:** The bpsynth process is unable to set the non-blocking socket option on the listen socket.

**Recommended Action:** Check the OS error that was reported in the error message, which was logged in the NetBackup error log. The error helps to diagnose the problem. Ensure that the bpsynth binary matches the installed NetBackup version. If the condition persists, contact customer support and send appropriate logs.
A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 603**

**Message:** cannot register handler for accepting new connections  
**Explanation:** The `bpsynth` process cannot register the listen socket with the ACE reactor.  
**Recommended Action:** Ensure that the `bpsynth` binary matches the installed NetBackup version. Retry the synthetic backup job. If the problem persists, contact customer support and send appropriate logs.  
A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 604**  
**Message:** no target storage unit specified for the new job  
**Explanation:** A mismatch occurred between storage units that are known to NetBackup and the specified target storage unit.  
**Recommended Action:** Retry the synthetic backup job. If the problem persists, contact customer support and provide appropriate logs.  
A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 605**  
**Message:** received error notification for the job  
**Explanation:** This error code is no longer used.  
**Recommended Action:** Submit a problem report along with appropriate logs.  
A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 606**  
**Message:** no robot on which the media can be read  
**Explanation:** `bpsynth` returns this error when it cannot find a robot on which to read a particular media ID that contains backup images to be synthesized. The media ID is included in the message that `bpsynth` logs. This error should not occur.
Recommended Action: Contact customer support and provide appropriate logs. A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 607
Message: no images were found to synthesize
Explanation: The database query to obtain the images to synthesize for the given policy did not return any images.
Recommended Action: Ensure that a synthetic full backup has one full image (real or synthetic) and one or more subsequent incremental images (differential or cumulative) to synthesize. For a cumulative synthetic backup, there must be two or more incremental (differential or cumulative) images to synthesize. Adjust your schedules so the appropriate backup jobs complete successfully before the synthetic job is run. The scheduler does not retry a synthetic backup job that fails with this error code.

NetBackup status code: 608
Message: storage unit query failed
Explanation: The database query to obtain all storage units failed.
Recommended Action: Verify that the bpdbm process is running and that no errors were logged to the NetBackup error log. Restart the bpdbm process (on UNIX and Linux), or the NetBackup Database Manager Service (on Windows) and retry the synthetic backup job. If the problem persists, contact customer support and send the appropriate logs.
A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 609
Message: reader failed
Explanation: The bptm or the bpdm reader process was terminated with an error.
Recommended Action: Refer to the NetBackup error log for the errors that the bpsynth and bptm or bpdm reader logged. The error message should contain the actual error that the bptm or the bpdm reader reports. Refer to the NetBackup Troubleshooting Guide for information on the error that the bptm or the bpdm reader reports. The media may not be present or is defective or the drive that was
used for reading the media is defective. If the problem persists, contact customer support and send appropriate logs.

A complete list of required logs and configuration information is available. See "Logs to accompany problem reports for synthetic backup" on page 111.

**NetBackup status code: 610**

**Message:** end point terminated with an error

**Explanation:** An error indication was received on the connection to the `bptm` or the `bpdm` process.

**Recommended Action:** Review the errors in the NetBackup error log that the following processes logged: `bpsynth` and `bptm` or `bpdm`. Refer to the debug logs for these processes for more information. The connection may have broken due to the following: an error condition that the `bptm` or the `bpdm` process detects or network problems between the master and the media server. Check the network connectivity between the master and the media server. Retry the job and if the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 611**

**Message:** no connection to reader

**Explanation:** A connection to the `bptm` or the `bpdm` reader process does not exist to communicate with the reader.

**Recommended Action:** This error should not occur. Submit a problem report along with the appropriate logs.

A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 612**

**Message:** cannot send extents to bpsynth

**Explanation:** This error code is no longer used.

**Recommended Action:** Submit a problem report along with appropriate logs. A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.
NetBackup status code: 613

Message: cannot connect to read media server

Explanation: The `bpsynth` process was unable to connect to the media server to read a backup image.

Recommended Action: Ensure that network connectivity exists between the master server and the specified media server. Examine the NetBackup error log for any error messages that `bpsynth` logged. For more information, refer to the debug logs for `bpsynth` on the master server and `bpcd` and `bptm` or `bpdm` on the media server.

A complete list of required logs and configuration information is available.
See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 614

Message: cannot start reader on the media server

Explanation: The `bpsynth` process was unable to start the `bptm` or the `bpdm` process to read a backup image to be synthesized.

Recommended Action: Do the following, as appropriate:

- Examine the NetBackup error log for any errors that `bpsynth` logged. For more information, refer to the following debug logs: for `bpsynth` on the master server and for `bpcd` and `bptm` or `bpdm` on the media server. Ensure that the `bptm` or the `bpdm` binaries on the media server are executable and are not corrupt. Try running `bptm` or `bpdm` commands locally on the media server to ensure that the binary is executable and not corrupt. For instance, you can run the following command

```
/bp/bin/bptm -count -rn 0 -rt 8
```

where robot number is 0 and the robot type is 8. The robot type that corresponds to the robot number can be taken from the command line that is logged in the debug log for `bptm`. This command displays the counts for the up, shared, and assigned drives in the robot.

A complete list of required logs and configuration information is available.
See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 615

Message: internal error 615

Explanation: This error code is no longer used.
**Recommended Action:** Submit a problem report along with appropriate logs. A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 616**

**Message:** internal error 616

**Explanation:** This error code is no longer used.

**Recommended Action:** Submit a problem report along with appropriate logs. A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 617**

**Message:** no drives available to start the reader process

**Explanation:** No drives are available to start the `bptm` process to read a backup image to be synthesized.

**Recommended Action:** Ensure that sufficient drives are available before you re-start the job.

**NetBackup status code: 618**

**Message:** internal error 618

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send the appropriate logs. A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 619**

**Message:** internal error 619

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send the appropriate logs. A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.
NetBackup status code: 620
Message: internal error 620
Explanation: This error code is no longer used.
Recommended Action: Contact customer support and send the appropriate logs.
A complete list of required logs and configuration information is available.
See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 621
Message: unable to connect to bpcoord
Explanation: This error code is no longer used.
Recommended Action: Submit a problem report along with appropriate logs.
A complete list of required logs and configuration information is available.
See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 622
Message: connection to the peer process does not exist
Explanation: The underlying connection to the peer bptm or bpdm process does not exist. This error should not occur.
Recommended Action: Contact customer support and send appropriate logs.
A complete list of required logs and configuration information is available.
See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 623
Message: execution of a command in a forked process failed
Explanation: The failure normally occurs during the execution of a command on a media server through bpcd. Examine the NetBackup error log for additional error messages. Also refer to the debug logs for bpsynth (on the master server) and bpcd (on the media server) to get an explanation of the failure. A common cause of the failure is insufficient memory, file system full, or insufficient swap space.
Recommended Action: Retry the job and if the problem persists, contact customer support and send appropriate logs.
A complete list of required logs and configuration information is available.
NetBackup status code: 624
Message: unable to send a start command to a reader or a writer process on media server
Explanation: The bpsynth process is unable to send a command to the bptm or the bpdm process on the media server.
Recommended Action: Ensure that network connectivity exists between the master and the media server. Look for additional error messages in the NetBackup error log. More detailed information is present in the debug logs for bpsynth (on master server) and bptm or bpdm on the media server. If the problem persists, contact customer support and send appropriate logs. A complete list of required logs and configuration information is available.
See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 625
Message: data marshalling error
Explanation: Problems were encountered while sending data over the connection. This error should not occur.
Recommended Action: Contact customer support and send appropriate logs. A complete list of required logs and configuration information is available.
See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 626
Message: data un-marshalling error
Explanation: Problems were encountered in the parsing of the messages that bpsynth received. This error should not occur.
Recommended Action: Contact customer support and send the appropriate logs. A complete list of required logs and configuration information is available.
See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 627
Message: unexpected message received from bpsynth
Explanation: This error code is no longer used.
**Recommended Action:** Submit a problem report along with appropriate logs. A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 628**

**Message:** insufficient data received

**Explanation:** This error occurs in the following situation: partial data is read from the input socket and cannot be parsed until the remaining data that comprises the message is read. The lower layers encounter this error; it should not cause a process to be terminated.

**Recommended Action:** If this error causes the bpsynth binary to hang or malfunction, contact customer support and send appropriate logs. A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 629**

**Message:** no message was received from bptm

**Explanation:** This error is returned when no message is received from bptm process in response to the command or query executed by using bptm.

**Recommended Action:** Look for additional error messages in the following logs: the NetBackup error log and the debug logs for bpsynth on the master server and bptm on the media server. A system condition (insufficient memory, file system full, insufficient swap space) on the media server may prevent the bptm process from sending the response. Verify the network connectivity between the master and the media server. If no explanation is found for the failure and the problem persists, contact customer support and send appropriate logs. A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 630**

**Message:** unexpected message was received from bptm

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send appropriate logs. A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.
NetBackup status code: 631

Message: received an error from bptm request to suspend media

Explanation: The bpsynth process was unable to suspend a media that contained one or more images to be synthesized. A message in the bpsynth legacy log lists the media IDs to be suspended. The bpsynth log also includes a failure message to indicate which particular media in the list was not suspended. media (ordinal) indicates the unsuspended media by means of its order in the list. For example, if the unsuspended media was the second media in the list, the failure message says media (1).

Recommended Action: Examine the bptm debug log for more information on the reason for the suspend failure. The bpsynth process ignores this error and continues to process. It has the potential to fail later if the media with the images to be read gets assigned to another backup or restore job. If the synthetic backup job fails, fix the condition that lead to the suspend failure and retry the job.

NetBackup status code: 632

Message: received an error from bptm request to un-suspend media

Explanation: The bpsynth process was unable to un-suspend a media that it suspended at the start of the synthetic backup job. A message in the bpsynth legacy log lists the media IDs to be un-suspended. The bpsynth log also includes a failure message to indicate which particular media in the list was not un-suspended. media (ordinal) indicates the media by means of its order in the list. For example, if the media that was not un-suspended was the second media in the list, the failure message says media (1).

Recommended Action: Look at the debug log for the bptm process on the media server for an explanation of the un-suspend failure and the media ID. Try to un-suspend the tape manually by using the bpmedia command.

NetBackup status code: 633

Message: unable to listen and register service via vnetd

Explanation: This error code is no longer used.

Recommended Action: Submit a problem report along with appropriate logs. A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.
NetBackup status code: 634

**Message:** no drives available to start the writer process

**Explanation:** The `bpsynth` process cannot start the synthetic backup job because no drives were available in the target storage unit for the writer. The storage unit may be in use by a restore or another synthetic backup job.

**Recommended Action:** Ensure that the target storage unit that is configured for the synthetic backup schedule has an available drive to write the synthetic backup image.

NetBackup status code: 635

**Message:** unable to register handle with the reactor

**Explanation:** Unable to register a handle with the ACE reactor to monitor events on the handle. This error can occur in `bpsynth`.

**Recommended Action:** Examine NetBackup error log for any errors that were logged for the job. Refer to the debug logs for `bpsynth` for more information. Retry the synthetic backup job. If the problem persists, contact customer support and send the appropriate logs.

A complete list of required logs and configuration information is available.

See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 636

**Message:** read from input socket failed

**Explanation:** The read from an input socket failed. The underlying connection has been broken.

**Recommended Action:** The `bpsynth` process encountered an error while reading from an input socket. The socket may be between `bpsynth` and `bptm` or `bpdm`.

The `errno` that was logged to the NetBackup error log indicates the reason for the failure. For more information, refer to the following: the debug log for `bpsynth` (on the master server) and for the `bptm` or the `bpdm` reader or writer processes (on the media server). Check the network connectivity between the master and the media server. Rerun the synthetic backup job. If the problem persists, contact customer support and send appropriate logs.

A complete list of required logs and configuration information is available.

See “Logs to accompany problem reports for synthetic backup” on page 111.
NetBackup status code: 637

**Message:** write on output socket failed

**Explanation:** The write to an output socket failed. The underlying connection has been broken.

**Recommended Action:** The `bpsynth` process encountered an error while writing to an output socket. The socket is between `bpsynth` and `bptm` or `bpdm`.

The errno that logged to the NetBackup error log indicates the reason for the failure. For more information, refer to the following: the debug log for `bpsynth` (on the master server) and for the `bptm` or the `bpdm` reader or writer process (on the media server). Check the connectivity between the master and the media server. Retry the synthetic backup job. If the problem persists, contact customer support and send appropriate logs.

A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 638

**Message:** invalid arguments specified

**Explanation:** The `bpsynth` command fails with this error code if incorrect arguments were specified.

**Recommended Action:** Refer to the `bpsynth` command line arguments (by using `-help`) for the correct argument specification. If the synthetic backup job was started manually by the command line, correct the arguments to `bpsynth` and rerun the job. If the synthetic backup job was scheduled or started with the console, ensure that the `bpsynth` and the `nbjm` binaries match the installed NetBackup version.

NetBackup status code: 639

**Message:** specified policy does not exist

**Explanation:** The policy that was specified on the `bpsynth` command does not exist in the database. Either the command line or `nbjm` initiated the `bpsynth` command. If `nbjm` initiated it, the policy may have been deleted after `nbjm` started `bpsynth` and before `bpsynth` issued the database query.

**Recommended Action:** If `bpsynth` is initiated with the command line, rerun the command for an existing policy. If the problem persists after you verify the following, contact customer support and send the appropriate logs:
The synthetic backup job was scheduled or started by using the NetBackup Administration console (manual start).

The policy exists in the `bpplist` command configuration.

Check the logs for `nbjm`, which uses unified logging (OID 117).

A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 640**

**Message:** specified schedule was not found

**Explanation:** The schedule on the `bpsynth` command did not exist in the specified policy definition in the database due to either of the following:

- The command line initiated the `bpsynth` command
- The specified schedule was deleted from the policy after `nbjm` started `bpsynth`, before `bpsynth` issued the database query.

**Recommended Action:** If the command line initiated `bpsynth`, do the following: rerun the command with the correct synthetic schedule label defined in the policy of the synthetic backup job to be run. If the synthetic backup job was scheduled or started with the NetBackup Administration console, define a new schedule in the policy and retry the job. If the problem persists, contact customer support and send appropriate logs.

A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 641**

**Message:** invalid media type specified in the storage unit

**Explanation:** The media type that was specified in the target storage unit is invalid for synthetic backup. Synthetic Backup images can only be written to disk, disk staging, and Media Manager type of storage units.

**Recommended Action:** Ensure that the target storage unit that was configured for synthetic backup is a disk, disk staging, or Media Manager type (not NDMP type). Rerun synthetic backup with the appropriate storage unit.

**NetBackup status code: 642**

**Message:** duplicate backup images were found
**Explanation:** The database query returned duplicate backup IDs. This error should not occur.

**Recommended Action:** Contact customer support and send appropriate logs. A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 643**

**Message:** unexpected message received from \texttt{bpcoord}

**Explanation:** This error code is no longer used.

**Recommended Action:** Submit a problem report along with appropriate logs. A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 644**

**Message:** extent directive contained an unknown media id

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send appropriate logs. A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 645**

**Message:** unable to start the writer on the media server

**Explanation:** The \texttt{bpsynth} process was unable to start the following: the \texttt{bptm} or the \texttt{bpdm} process on the media server that is associated with the target storage unit to write the synthetic image.

**Recommended Action:**

Examine the NetBackup error log for any messages that \texttt{bpsynth} logged. For more information, refer to the following: the debug logs for \texttt{bpsynth} on the master server and \texttt{bpcd} and \texttt{bptm} or \texttt{bpdm} on the media server. Ensure that the \texttt{bptm} or the \texttt{bpdm} binaries on the media server are executable and are not corrupt. Try to run the \texttt{bptm} or the \texttt{bpdm} commands locally on the media server to ensure that the binary is executable and not corrupt. For instance, you can run the following command:

\begin{verbatim}
install_path/netbackup/bin/bptm --count -rn 0 -rt 8
\end{verbatim}
where robot number is 0 and robot type is 8. The robot type that corresponds to
the robot number can be taken from the command line that is logged in the debug
log for \texttt{bptm}. This command displays the counts for the up, shared, and assigned
drives in the robot. In case the synthetic image is to be written to a disk storage
unit, verify the \texttt{bpdm} binary by running the following command:

\begin{verbatim}
install_path/netbackup/bin/bpdm
\end{verbatim}

It should print the following: "\texttt{bpdm: media manager operation not specified}".
Retry the synthetic backup job. If the problem persists, contact customer support
and send appropriate logs.

A complete list of required logs and configuration information is available.
See “\texttt{Logs to accompany problem reports for synthetic backup}” on page 111.

**NetBackup status code: 646**

**Message:** unable to get the address of the local listen socket

**Explanation:** The \texttt{bpsynth} process cannot obtain the address of the opened listen
socket. The \texttt{bpsynth} process needs the address to receive incoming connections
from the \texttt{bptm} or the \texttt{bpdm} processes, which were started to read the source images.
This problem should not happen. The library call used to retrieve the address of
the listen socket relies on the underlying system call to obtain the socket address.
The \texttt{errno} that the system call reports is included in the error message and should
help to diagnose the problem.

**Recommended Action:** Rerun the synthetic backup job. If the problem persists,
contact customer support and send appropriate logs.

A complete list of required logs and configuration information is available.
See “\texttt{Logs to accompany problem reports for synthetic backup}” on page 111.

**NetBackup status code: 647**

**Message:** validation of synthetic image failed

**Explanation:** This error is returned when \texttt{bpsynth} receives an error from the
database call to validate the synthetic image.

**Recommended Action:** This error may indicate a problem in the synthetic backup
process. Examine the NetBackup error log for any messages that the following
processes logged: \texttt{bpsynth} and \texttt{bptm} or \texttt{bpdm}. Look at the debug logs for these
processes for additional information. If you cannot resolve the problem, contact
customer support and send appropriate logs.

A complete list of required logs and configuration information is available.
See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 648**

**Message:** unable to send extent message to BPXM

**Explanation:** The `bpsynth` process cannot send extent information to the `bptm` or the `bpdm` process that was started to read a specified backup image to synthesize.

**Recommended Action:** This error indicates a communication problem between `bpsynth` and the `bptm` or `bpdm` reader process on the media server. Ensure that the media server is accessible and that the `bptm` or the `bpdm` process is running on the media server. Examine the NetBackup error log for any errors that the following logged: `bpsynth` (on the master server) and the `bptm` or the `bpdm` reader process (on the media server). Examine the debug logs for `bpsynth` and `bptm` or `bpdm` for additional information. Rerun the synthetic backup job. If the problem persists, contact customer support and send appropriate logs.

A complete list of required logs and configuration information is available.

See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 649**

**Message:** unexpected message received from BPXM

**Explanation:** This error code is no longer used.

**Recommended Action:** Submit a problem report along with appropriate logs.

A complete list of required logs and configuration information is available.

See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 650**

**Message:** unable to send extent message to `bpcoord`

**Explanation:** This error code is no longer used.

**Recommended Action:** Submit a problem report along with appropriate logs.

A complete list of required logs and configuration information is available.

See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 651**

**Message:** unable to issue the database query for policy
Explanation: The `bpsynth` process was unable to send the database query for policy.

Recommended Action: This error indicates a communication problem between `bpsynth` and `bpdbm`. Ensure that `bpdbm` is running and the `bpdbm` binary matches the installed NetBackup version. Examine the NetBackup error log for any errors that `bpdbm` and `bpsynth` logged. Examine the debug logs for `bpsynth` and `bpdbm` for additional information. Restart the `bpdbm` process (on UNIX and Linux) or the NetBackup Database Manager Service (on Windows) and rerun the synthetic backup job. If the problem persists, contact customer support and send appropriate logs.

A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 652
Message: unable to issue the database query for policy information
Explanation: The `bpsynth` process was unable to send the database query for detailed information about the policy.
Recommended Action: This error indicates a communication problem between `bpsynth` and `bpdbm`. Ensure that `bpdbm` is running. Examine the NetBackup error log for any errors that `bpdbm` and `bpsynth` logged. Examine the debug logs for `bpsynth` and `bpdbm` for additional information. Restart the `bpdbm` process (on UNIX and Linux) or the NetBackup Database Manager Service (on Windows) and rerun the synthetic backup job. If the problem persists, contact customer support and send appropriate logs.

A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 653
Message: unable to send a message to `bpccord`
Explanation: This error code is no longer used.
Recommended Action: Contact customer support and send appropriate logs.
A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 654
Message: internal error 654
**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send appropriate logs.

A complete list of required logs and configuration information is available.

See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 655**

**Message:** no target storage unit was specified via command line

**Explanation:** No target storage unit was specified on the `bpsynth` command line (-S).

**Recommended Action:** Rerun `bpsynth` with the target storage unit specified by the -S option.

**NetBackup status code: 656**

**Message:** unable to send start synth message to `bpcoord`

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send appropriate logs.

A complete list of required logs and configuration information is available.

See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 657**

**Message:** unable to accept connection from the reader

**Explanation:** The `bpsynth` process was unable to accept the connection from the `bptm` or the `bpdm` reader process that runs on the media server.

**Recommended Action:** Examine the NetBackup error log for any errors that `bpsynth` and `bptm` or the `bpdm` reader process logged. The message that `bpsynth` logged includes the error (errno) reported by the system call. Refer to the debug logs for `bpsynth` on the master server and `bptm` or the `bpdm` process on the media servers for more information. Ensure that network connectivity exists between the master and the media servers. If the problem persists, contact customer support and send appropriate logs.

A complete list of required logs and configuration information is available.

See “Logs to accompany problem reports for synthetic backup” on page 111.
NetBackup status code: 658

**Message:** unable to accept connection from the writer

**Explanation:** The bpsynth process was unable to accept the connection from the bptm or the bpdm writer process that runs on the media server.

**Recommended Action:** Examine the NetBackup error log for any errors that bpsynth and the bptm or the bpdm writer process logged. The message that bpsynth logged includes the error (errno) reported by the system call. Also refer to the debug logs for bpsynth on the master server and bptm or the bpdm process on the media server for more information. Ensure that network connectivity exists between the master and the media servers. If the problem persists, contact customer support and send appropriate logs.

A complete list of required logs and configuration information is available.

See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 659

**Message:** unable to send a message to the writer child process

**Explanation:** The bpsynth process was unable to send the message that contains the following to the bptm or the bpdm writer: the hostname and the port number of the bptm or the bpdm reader.

**Recommended Action:** Examine the NetBackup error log for any errors that bpsynth and the bptm or the bpdm writer process logged. Refer to the following for more information: the debug logs for bpsynth on the master server and the bptm or the bpdm process on the media server. Ensure that network connectivity exists between the master and the media servers. If the problem persists, contact customer support and send appropriate logs.

A complete list of required logs and configuration information is available.

See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 660

**Message:** a synthetic backup request for media resources failed

**Explanation:** The request for resources failed due to an internal NetBackup error.

**Recommended Action:** Create logs as explained in the following topics:

See “Logs to accompany problem reports for synthetic backup” on page 111.

Rerun the job. Then send the logs to customer support. More information is available about unified logs.
See “Submitting unified logging files to &Company; support” on page 100.

**NetBackup status code: 661**

**Message:** unable to send exit message to the BPXM reader

**Explanation:** The *bpsynth* process cannot send the exit message to indicate the end of extents messages to the following: *bptm* or the *bpdm* reader process on the media server. The network connection between the master and the media server may have terminated or the *bptm* or the *bpdm* reader process has terminated.

**Recommended Action:** Check the network connectivity between the master and the media server. Examine the NetBackup error log for any errors that *bpsynth* and *bptm* or the *bpdm* reader process logged. Examine the debug logs for *bpsynth* on the master server and *bptm* or the *bpdm* reader process on the media servers for more detailed information. If the problem persists, contact customer support and provide the appropriate logs.

A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 662**

**Message:** unknown image referenced in the synth context message from BPXM

**Explanation:** The *bpsynth* process received an extent message from the *bptm* or the *bpdm* reader with reference to a media ID that was unknown to *bpsynth*. This error should not occur.

**Recommended Action:** Contact customer support and provide the appropriate logs.

A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.

**NetBackup status code: 663**

**Message:** image does not have a fragment map

**Explanation:** The *bpsynth* process received an image without a fragment map from *bpdbm*. This error should not occur.

**Recommended Action:** Contact customer support and provide the appropriate logs.

A complete list of required logs and configuration information is available. See “Logs to accompany problem reports for synthetic backup” on page 111.
NetBackup status code: 664

**Message:** zero extents in the synthetic image, cannot proceed

**Explanation:** The `bpsynth` process receives zero extents from `bpdbm`. This error should not occur.

**Recommended Action:** Contact customer support and provide the appropriate logs.

A complete list of required logs and configuration information is available.

See “Logs to accompany problem reports for synthetic backup” on page 111.

---

NetBackup status code: 665

**Message:** termination requested by `bpcoord`

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send appropriate logs.

A complete list of required logs and configuration information is available.

See “Logs to accompany problem reports for synthetic backup” on page 111.

---

NetBackup status code: 667

**Message:** unable to open pipe between bpsynth and bpcoord

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send appropriate logs.

A complete list of required logs and configuration information is available.

See “Logs to accompany problem reports for synthetic backup” on page 111.

---

NetBackup status code: 668

**Message:** pipe fgets call from bpcoord failed

**Explanation:** This error code is no longer used.

**Recommended Action:** Contact customer support and send appropriate logs.

A complete list of required logs and configuration information is available.

See “Logs to accompany problem reports for synthetic backup” on page 111.
NetBackup status code: 669
Message: bpcoord startup validation failure
Explanation: This error code is no longer used.
Recommended Action: Contact customer support and send appropriate logs.
A complete list of required logs and configuration information is available.
See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 670
Message: send buffer is full
Explanation: This error code is no longer used.
Recommended Action: Contact customer support and provide the appropriate logs.
A complete list of required logs and configuration information is available.
See “Logs to accompany problem reports for synthetic backup” on page 111.

NetBackup status code: 671
Message: query for list of component images failed
Explanation: A new synthetic image cannot be formed because of a problem with the required component images. For example: a new, synthetic full backup is tried from the previous full image from Sunday and from the five differential incremental images from Monday through Friday. This error occurs if any of those images (except the most recent image on Friday) has expired.
Recommended Action: Run a non-synthetic backup (either a new full or new cumulative), depending on the type of backup that failed.

NetBackup status code: 800
Message: resource request failed
Explanation: The nbjm process was unable to get the required resources for a job. An EMM reason string that appears in the Activity Monitor job details display and in the nbjm debug log accompanies this status code. The EMM reason string identifies the reason for the failed resource request.
Recommended Action: Locate the EMM reason string, correct the problem, and rerun the job.
Some generic EMM reason strings (such as "Disk volume is down") may require generating some reports to determine the cause of the failure. Generate the report
by using either bperror or various log entry reports, such as Reports > Disk Reports > Disk Logs in the Administration Console.

NetBackup status code: 801

Message: JM internal error

Explanation: The nbjm process encountered an internal error.

Recommended Action: If the problem persists, submit a report with the following items.

- Unified logging files on the NetBackup server for nbpem (originator ID 116), nbjm (117), nbrb (118), and PBX (103). All unified logging is written to /usr/openv/logs (UNIX and Linux) or install_path\NetBackup\logs (Windows).

- Legacy logs:
  - On the NetBackup master server for bpbrm, bpjobd, bpcompatd, bpdbm, and nbproxy
  - On the media server for bpcd, bpbrm, and bptm or bpdm
  - On the client for bpcd and pbkbar

Legacy logs are in subdirectories under /usr/openv/netbackup/logs/ (UNIX and Linux) or install_path\Netbackup\logs\ (Windows). If the directories do not exist, create directories for each of these processes and rerun the job.

- Contents of /usr/openv/db/jobs/trylogs (UNIX and Linux) or install_path\NetBackup\db\jobs\trylogs (Windows).

- bpdbjobs output: run bpdbjobs to obtain the state and status of all jobs.

NetBackup status code: 802

Message: JM internal protocol error

Explanation: nbjm returns this error whenever a protocol error occurs with an external process that tries to communicate with nbjm. External processes include bptm, tpreq, bplabel, dqts, vmphyinv, or nbpem.

Recommended Action:

Ensure that the NetBackup software on the master and the media server is from an official NetBackup release.

If the problem persists, submit a report with the following items.

- Unified logging files on the NetBackup server for nbpem (originator ID 116), nbjm (117), nbrb (118), and PBX (103). All unified logging is written to
/usr/openv/logs (UNIX and Linux) or install_path\NetBackup\logs (Windows).

- Legacy logs:
  - On the NetBackup master server for bpbrm, bpjobd, bpcompatd, bpdbm, and nbproxy
  - On the media server for bpcd, bpbrm, and bptm or bpdm
  - On the client for bpcd and bpbkar

Legacy logs are in subdirectories under /usr/openv/netbackup/logs/ (UNIX and Linux) or install_path\NetBackup\logs\ (Windows). If the directories do not exist, create directories for each of these processes and rerun the job.

- Contents of /usr/openv/db/jobs/trylogs (UNIX and Linux) or install_path\NetBackup\db\jobs\trylogs (Windows).

- bpdbjobs output: run bpdbjobs to obtain the state and status of all jobs.

NetBackup status code: 803

Message: JM terminating

Explanation: A service request for an existing or a new job was received when the nbjm process was shutting down.

Recommended Action: If nbjm was not terminated explicitly (by entering the /usr/openv/netbackup/bin/bp.kill_all command on UNIX and Linux or install_path\NetBackup\bin\bpdow on Windows), submit a report with the following items.

- Unified logging files on the NetBackup server for nbpem (originator ID 116), nbjm (117), nbrb (118), and PBX (103). All unified logging is written to /usr/openv/logs (UNIX and Linux) or install_path\NetBackup\logs (Windows).

- Legacy logs:
  - On the NetBackup master server for bpbrm, bpjobd, bpcompatd, bpdbm, and nbproxy
  - On the media server for bpcd, bpbrm, and bptm or bpdm
  - On the client for bpcd and bpbkar

Legacy logs are in subdirectories under /usr/openv/netbackup/logs/ (UNIX and Linux) or install_path\NetBackup\logs\ (Windows). If the directories do not exist, create directories for each of these processes and rerun the job.
Contents of /usr/openv/db/jobs/trylogs (UNIX and Linux) or
install_path\NetBackup\db\jobs\trylogs (Windows).

bpdbjobs output: run bpdbjobs to obtain the state and status of all jobs.

NetBackup status code: 805
Message: Invalid jobid
Explanation: The nbjm process received an invalid job ID in the request.
Recommended Action:
The requested operation may refer to a job that no longer exists or is not known
to nbjm. Or the job ID is invalid (less than or equal to 0). Ensure that the command
used to start the job did not specify a job ID already in use by another job.
If the problem persists, submit a report with the following items.

Unified logging files on the NetBackup server for nbpem (originator ID 116),
nbjm (117), nbbr (118), and PBX (103). All unified logging is written to
/usr/openv/logs (UNIX and Linux) or install_path\NetBackup\logs
(Windows).

Legacy logs:
On the NetBackup master server for bpbrm, bpjobd, bpcompatd, bpdsm,
and nbproxy
On the media server for bpcd, bpbrm, and bptm or bpdm
On the client for bpcd and bpbkar

Legacy logs are in subdirectories under /usr/openv/netbackup/logs/ (UNIX
and Linux) or install_path\NetBackup\logs\ (Windows). If the directories
do not exist, you must create directories for each of these processes and rerun
the job.

Contents of /usr/openv/db/jobs/trylogs (UNIX and Linux) or
install_path\NetBackup\db\jobs\trylogs (Windows).

bpdbjobs output: run bpdbjobs to obtain the state and status of all jobs.

NetBackup status code: 806
Message: this mpx group is unjoinable
Explanation: This error is a timing problem. It can happen if the job was added
to a multiplexed group when bpbrm terminates due to an error condition. Note
that the resource broker (nbbr) does the allocation of a multiplexed group, whereas
the job manager (nbjm) starts and monitors the bpbrm process.
**Recommended Action:** If the failed job is scheduled and the retry count allows it, nbpem submits the job again. If the failed job was initiated manually, submit it again.

**NetBackup status code: 807**

**Message:** not externalized

**Explanation:** Not available.

**Recommended Action:** Not available.

**NetBackup status code: 811**

**Message:** failed to communicate with resource requester

**Explanation:** Job manager (nbjm) tries to notify a process (usually bptm) of the status of a resource it requested. That notification fails because of a communication problem.

**Recommended Action:** Do the following, as appropriate:

- Verify connectivity between the master and the media server.
- Verify Private Branch Exchange (PBX) configuration and permissions. For information on PBX is available. See “Resolving PBX problems” on page 66.

**NetBackup status code: 812**

**Message:** failed to communicate with resource broker

**Explanation:** Job manager (nbjm) tries to make a request to the resource broker (nbrb). The request fails because of a communication problem.

**Recommended Action:** Do the following, as appropriate:

- Verify connectivity between the master server and the EMM server.
- Verify Private Branch Exchange (PBX) configuration and permissions. For information on PBX is available. See “Resolving PBX problems” on page 66.

**NetBackup status code: 813**

**Message:** duplicate reference string specified

**Explanation:** The reference string is the file name specified on the -f option of the tpreq command. The specified file name on tpreq is already in use by another tpreq.
Recommended Action: Choose a unique name not already in use.

NetBackup status code: 818
Message: retention level mismatch
Explanation: A job fails with this error code if the retention level of the allocated media does not match the retention level configured in the policy.
Recommended Action: Contact NetBackup Technical Support and provide relevant supporting materials.

NetBackup status code: 819
Message: unable to communicate with JM proxy
Explanation: The job manager cannot communicate with nbproxy.
Recommended Action: Restart the job manager. If the condition persists, please contact NetBackup Support and provide relevant supporting materials.

NetBackup status code: 823
Message: no BRMComm to join
Explanation: The job was unable to join the multiplex group. This error is an internal error.
Recommended Action: Submit a report with the following items.
- Unified logging files on the NetBackup server for nb pem (originator ID 116), nb j m (117), nb rb (118), and PBX (103). All unified logging is written to /usr/openv/logs (UNIX and Linux) or \install_path\NetBackup\logs (Windows).
- The following legacy logs:
  - On the NetBackup master server for bp brm, bpjobd, b p c o m p a t d, bp db m, and nb proxy
  - On the media server for bp cd, bp brm, and b pt m or bp dm
  - On the client for bp cd and bp b k ar
 Legacy logs are in subdirectories under /usr/openv/netbackup/logs/ (UNIX and Linux) or \install_path\Netbackup\logs\ (Windows). If the directories do not exist, create directories for each of these processes and rerun the job.
- Contents of /usr/openv/db/jobs/trylogs (UNIX and Linux) or \install_path\NetBackup\db\jobs\trylogs (Windows).
- bp db j obs output: run bp db j obs to obtain the state and status of all jobs.
**NetBackup status code: 830**

**Message:** drive(s) unavailable or down

**Explanation:** All configured drive that can be used for this job are down.

One of the following has occurred:

- No drives are configured for the media requested for the job.
- The job requires an NDMP drive path, but no NDMP drive paths are up or configured.
- The job cannot use an NDMP drive path, but these are the only drive paths that are up or configured for the drive.

**Recommended Action:** Do the following:

- Make sure the drives and drive paths are up and correct for the media that you configure.
- Verify that `ltid` is running on the required media server, and that the media server is active for tape.
- Use the device monitor to start up the drives paths if they are down.
- If the drives are downed again, clean the drives.

**NetBackup status code: 831**

**Message:** image has been validated

**Explanation:** A job retry attempt fails because the image from the previous attempt has already been validated. This error can occur if nbjm shuts down before it receives the job success status. This status code indicates a timing problem only.

**Recommended Action:** No corrective action is required.

**NetBackup status code: 900**

**Message:** retry nbrb request later

**Explanation:** The NetBackup Resource Broker (nbrb service) was unable to respond to a request.

**Recommended Action:** Do the following, as appropriate:

- For detailed information, examine the unified logging files on the NetBackup server for the nbrb service (originator ID 118). All unified logging is written to `/usr/openv/logs` (UNIX and Linux) or `install_path\NetBackup\logs` (Windows).
If necessary, set global logging to a higher level by using Host Properties > Master Server > Properties > Logging. Retry the operation and examine the nbrb logs.

**NetBackup status code: 901**

**Message:** RB internal error

**Explanation:** The NetBackup Resource Broker (nbrb service) encountered an internal error.

**Recommended Action:** Do the following, as appropriate:

- For detailed information, examine the unified logging files on the NetBackup server for the nbrb service (originator ID 118). All unified logging is written to `/usr/openv/logs` (UNIX and Linux) or `install_path\NetBackup\logs` (Windows).

- If necessary, set global logging to a higher level, by using Host Properties > Master Server > Properties > Logging. Retry the operation and examine the nbrb logs.

**NetBackup status code: 902**

**Message:** RB invalid argument

**Explanation:** The NetBackup Resource Broker (nbrb service) detected an invalid argument.

**Recommended Action:** Do the following, as appropriate:

- For detailed information, examine the unified logging files on the NetBackup server for the nbrb service (originator ID 118). All unified logging is written to `/usr/openv/logs` (UNIX and Linux) or `install_path\NetBackup\logs` (Windows).

- If necessary, set global logging to a higher level, by using Host Properties > Master Server > Properties > Logging. Retry the operation and examine the nbrb logs.

**NetBackup status code: 903**

**Message:** RB communication error

**Explanation:** The NetBackup Resource Broker (nbrb service) encountered a communication error.

**Recommended Action:** Do the following, as appropriate:
- For detailed information, examine the unified logging files on the NetBackup server for the nbrb service (originator ID 118). All unified logging is written to /usr/openv/logs (UNIX and Linux) or install_path\NetBackup\logs (Windows).

- If necessary, set global logging to a higher level, by using Host Properties > Master Server > Properties > Logging. Retry the operation and examine the nbrb logs.

**NetBackup status code: 904**

**Message:** RB max reallocation tries exceeded

**Explanation:** Under some conditions, failed mounts are retried; the number of retries for the resource request has been exceeded.

**Recommended Action:** For detailed information, examine the unified logging files on the NetBackup server for the nbrb service (originator ID 118) and for nbemm (originator ID 111). All unified logging is written to /usr/openv/logs (UNIX and Linux) or install_path\NetBackup\logs (Windows). Also examine the legacy bptm log.

**NetBackup status code: 905**

**Message:** RB media server mismatch

**Explanation:** If you have any storage units that are specified for multiple copies, they must be on the same media server.

**Recommended Action:** Do the following, as appropriate:

- Configure the backup schedule with a storage unit or storage unit groups that can be run on the same media server.

- For detailed information, examine the unified logging files on the NetBackup server for the nbrb service (originator ID 118). All unified logging is written to /usr/openv/logs (UNIX and Linux) or install_path\NetBackup\logs (Windows).

**NetBackup status code: 906**

**Message:** RB operator denied mount request

**Explanation:** By using the Device Management node in the NetBackup Administration Console or the vmoprcmd command, the operator denied a mount request.

**Recommended Action:** Do the following, as appropriate:
Determine the cause of the mount request denial and retry the job.

For detailed information, examine the unified logging files on the NetBackup server for the nbrb service (originator ID 118). All unified logging is written to /usr/openv/logs (UNIX and Linux) or install_path\NetBackup\logs (Windows).

NetBackup status code: 907

Message: RB user cancelled resource request

Explanation: A user-initiated action caused a Resource Broker (nbrb) request to be canceled.

Recommended Action: Do the following, as appropriate:

- Determine the action that resulted in cancellation of the resource request.
- For detailed information, examine the unified logging files on the NetBackup server for the nbrb service (originator ID 118). All unified logging is written to /usr/openv/logs (UNIX and Linux) or install_path\NetBackup\logs (Windows).

NetBackup status code: 908

Message: RB was reset

Explanation: The NetBackup Resource Broker (nbrb) resources and database were reset. Any nbrb requests that remain may fail when RB is reset. (An example of a process that resets the database is catalog recovery.)

Recommended Action: Do the following, as appropriate:

- Determine the action that reset nbrb resources and the nbemm database.
- For detailed information, examine the unified logging files on the NetBackup server for the nbrb service (originator ID 118). All unified logging is written to /usr/openv/logs (UNIX and Linux) or install_path\NetBackup\logs (Windows).

NetBackup status code: 912

Message: RB disk volume mount failed

Explanation: The attempt to mount a disk volume failed. Possible reasons are hardware problems, inconsistent EMM database, or a NetBackup Resource Broker (nbrb) error.

Recommended Action: Do the following, as appropriate:
For detailed information, examine the unified logging files on the NetBackup server for the nbrb service (originator ID 118). Unified logging is written to /usr/openv/logs (UNIX and Linux) or install_path\NetBackup\logs (Windows).

If necessary, set global logging to a higher level: Host Properties > Master Server > Properties > Logging. Retry the operation and examine the nbrb logs.

**NetBackup status code: 914**

**Message:** RB media reservation not found

**Explanation:** The read media for a duplicate or synthetic backup job must be reserved at the start of the job. Status 914 occurs when the NetBackup Resource Broker (nbrb) receives an allocation request for a read media that was never reserved. It can result from an internal error in bpduplicate, nbjm, or nbrb.

**Recommended Action:** Do the following, as appropriate:

- Examine the unified logging files on the NetBackup server for the nbrb service (originator ID 118). Unified logging is written to /usr/openv/logs (UNIX and Linux) or to install_path\NetBackup\logs (Windows).

- If necessary, set global logging to a higher level: Host Properties > Master Server > Properties > Logging. Retry the operation and examine the nbrb logs.

**NetBackup status code: 915**

**Message:** RB disk volume mount must retry

**Explanation:** A shared disk job has failed because RB is unable to mount the disk volume. Shared disk requires that volume file systems be unmounted and remounted before other media servers can use them.

**Recommended Action:** Do the following, as appropriate:

- Verify that processes are not in the disk volume mount directories, which prevents them from being unmounted. If the problem persists, restart NetBackup on the media server.

**NetBackup status code: 916**

**Message:** Resource request timed out

**Explanation:** A job request for resources has failed because resources were not available before the configured time limit expired. Some jobs may specify a timeout when they ask for drives or other resources. If jobs consistently cause this error, more jobs may be scheduled than the number of available drives. The drives in
the resbroker job queue are not completed soon enough to allow new jobs to start before they time out.

**Recommended Action:** Distribute the scheduled job start times over a wider period of time.

**NetBackup status code: 1000**

**Message:** Client is offline

**Explanation:** An attempt was made to run a manual job for a client that is offline.

**Recommended Action:** Wait until the client is brought online or manually bring the client online by using the GUI or the `bpclient` command before you submit the manual job.

**NetBackup status code: 1500**

**Message:** Invalid storage unit

**Explanation:** The storage unit or storage unit group specified for one or more destinations in storage lifecycle policy is not valid.

**Recommended Action:** Do the following, as appropriate:

- Verify that the specified storage unit or storage unit group exists in the NetBackup database.
- Verify that the specified storage unit is not of type `BasicDisk`, `SnapVault`, or `Staging`, because storage lifecycle policies do not support them.
- Verify that the storage unit is not specified for snapshot destinations in storage lifecycle policy. Snapshot destinations do not require a storage unit in the storage lifecycle policy.

**NetBackup status code: 1501**

**Message:** Invalid source

**Explanation:** The source specified for one or more duplication destinations in storage lifecycle policy is not valid.

**Recommended Action:** Do the following, as appropriate:

- Verify that the specified source refers to a valid destination in the list of destinations in storage lifecycle policy.
- Verify that the `Backup` or `Snapshot` destination type does not have any source specified. If you are using `nbstl` to configure storage lifecycle policy, use value zero (0) as the source for a backup or snapshot destination type.
Verify that the destination that refers to the specified source is not a **Snapshot** destination type. NetBackup cannot duplicate a backup image that uses snapshot copy as a source.

Verify that the specified source does not refer to the destination itself for which the source is mentioned.

Verify that the specified list of destinations in a storage lifecycle has a circular dependency for the source.

**NetBackup status code: 1502**

**Message:** Invalid retention type

**Explanation:** The retention type specified for one or more destinations in storage lifecycle policy is not valid.

**Recommended Action:** Do the following, as appropriate:

- Verify that the retention type specified in storage lifecycle policy is either of **Fixed**, **Staged capacity managed**, or **Expire after duplication**.
- Verify that the **Expire after duplication** retention type is used for a destination only if it is specified as a source to other destinations in storage lifecycle policy.
- Verify that the **Staged capacity managed** retention type is used in storage lifecycle policy only for disk destinations that support **Capacity management** capabilities.
- Verify that the **Snapshot** destination type in storage lifecycle policy uses **Fixed** retention type only.

**NetBackup status code: 1503**

**Message:** Invalid volume pool

**Explanation:** The volume pool specified for one or more destinations in storage lifecycle policy is not valid.

**Recommended Action:** Do the following, as appropriate:

- Verify that the specified volume pool exists in NetBackup database.
- Verify that the volume pool is not specified for the **Backup** destination type in storage lifecycle policy.
- Verify that the volume pool is not specified for the **Snapshot** destination type in storage lifecycle policy.
- Verify that the volume pool is not specified for the **Duplication** destination type that is using disk storage units in storage lifecycle policy.
NetBackup status code: 1504

Message: Invalid source

Explanation: The media server group specified for one or more destinations in storage lifecycle policy is not valid.

Recommended Action: Do the following, as appropriate:

■ Verify that the specified media server group exists in NetBackup database.

■ Verify that the media server group is not specified for Backup destination types in storage lifecycle policy.

■ Verify that the server group is not specified for Snapshot destination types in storage lifecycle policy.

■ Verify that the media server group is not specified for Duplication destination types that are using disk storage unit in storage lifecycle policy.

NetBackup status code: 1505

Message: Invalid alternate read server

Explanation: The alternate read server specified for one or more destinations in storage lifecycle policy is not valid.

Recommended Action: Do the following, as appropriate:

■ Verify that the specified alternate read server exists in the NetBackup database.

■ Verify that the alternate read server is not specified for Backup destination types in storage lifecycle policy.

■ Verify that the alternate read server is not specified for Snapshot destination types in storage lifecycle policy.

NetBackup status code: 1506

Message: Invalid data classification

Explanation: The data classification specified in storage lifecycle policy is not valid.

Recommended Action: Verify that the specified data classification exists in the NetBackup database.

NetBackup status code: 1508

Message: Storage lifecycle policy exceeds maximum copies
**Explanation:** The list of destinations specified in storage lifecycle policy exceeds maximum number of allowed backup copies.

**Recommended Action:** Do the following, as appropriate:

- Verify that the number of destinations specified in storage lifecycle policy does not exceed maximum backup copies configured in NetBackup.
- Modify maximum backup copies to allow the expected number of destinations in storage lifecycle policy or reduce the number of destinations to not exceed maximum backup copies.

**NetBackup status code: 1509**

**Message:** Storage lifecycle policy exceeds maximum backup destinations

**Explanation:** The number of Backup type destinations specified in storage lifecycle policy exceeds the maximum number of simultaneous copies allowed.

**Recommended Action:** Verify that the number of Backup type destinations specified in storage lifecycle policy is less than or equal to 4. (The default value of the maximum number of allowed simultaneous copies parameter is 4.)

**NetBackup status code: 1510**

**Message:** Storage lifecycle policy cannot have more than one snapshot destination.

**Explanation:** The list of destinations specified in storage lifecycle policy exceeds the maximum number of allowed snapshot destinations.

**Recommended Action:** Verify that the storage lifecycle policy is not configured with more than one “Snapshot” type of destinations.

**NetBackup status code: 1511**

**Message:** Storage lifecycle policy must have at least one fixed retention destination.

**Explanation:** The specified storage lifecycle policy does not have any destination with a retention type of Fixed.

**Recommended Action:** Verify that the specified storage lifecycle policy has at least one destination configured with a Fixed retention type.

**NetBackup status code: 1512**

**Message:** Storage lifecycle policy must have at least one backup destination.

**Explanation:** The specified storage lifecycle policy does not have any backup destination.
**Recommended Action:** Verify that the storage lifecycle policy has at least one **Backup** type of destination.

**NetBackup status code: 1513**

**Message:** Invalid duplication priority

**Explanation:** The duplication priority specified in storage lifecycle policy is not valid.

**Recommended Action:** Verify that the duplication priority specified in storage lifecycle policy is in the range or 0 to 99999.

**NetBackup status code: 1514**

**Message:** Invalid destination type

**Explanation:** The destination type specified on one or more destinations in storage lifecycle policy is not valid.

**Recommended Action:** Do the following, as appropriate:

- Verify that the destination type specified on each destination in storage lifecycle policy is either **Backup**, **Duplication**, or **Snapshot**.

- If you are use the `nbstl` or `bpadm` command to configure storage lifecycle policy, the following are the valid values for the destination type: 0 indicates **Backup**, 1 indicates **Duplication**, and 2 indicates **Snapshot**.

**NetBackup status code: 1515**

**Message:** Invalid preserve multiplexing value

**Explanation:** The preserve multiplexing flag specified on one or more destinations is not valid.

**Recommended Action:** Do the following, as appropriate:

- If you use the `nbstl` command to configure storage lifecycle policy, then verify that the valid values are used to indicate the preserve multiplexing flag for each destination. The value “T” or “t” indicates true (Preserve multiplexing). The value “F” or “f” indicates false (do not preserve multiplexing).

- Verify that destinations of type **Backup** are not configured to preserve multiplexing.

- Verify that destinations of type **Snapshot** are not configured to preserve multiplexing.

- Verify that destinations of type **Duplication** that are using disk storage units are not configured to preserve multiplexing.
NetBackup status code: 1516
Message: All storage units or groups must be on the same media server.
Explanation: The destinations of type **Backup** specified in storage lifecycle policy are not accessible by the same media server.
Recommended Action: Verify that all the destinations of type **Backup** are accessible by at least one common media server.

NetBackup status code: 1517
Message: Invalid retention level
Explanation: The retention level specified for one or more destinations in storage lifecycle policy is not valid.
Recommended Action: Verify that the retention level specified on each destination in storage lifecycle policy is in the range of 0 to 24.

NetBackup status code: 1518
Message: Image is un-supported by storage lifecycle policy
Explanation: The backup image is un-supported by the configured storage lifecycle policy.
Recommended Action: Do the following, as appropriate:
- Verify that if a NetBackup policy is configured to perform snapshot backups and uses storage lifecycle policy as its storage destination, then the specified storage lifecycle policy must be configured with a snapshot destination. Otherwise, backup images created by those NetBackup policies are not processed further by storage lifecycle policy for any lifecycle operations.
- Verify that NetBackup policies using storage lifecycle policy as a storage destination are not configured to perform "snapshots-only" operations and they must create backups in addition to snapshots. Storage lifecycle policy even though configured with a snapshot destination would perform lifecycle operations on such images only if they have at least one backup copy.

NetBackup status code: 1800
Message: Invalid client list
Explanation: For Enterprise Vault-type policies, verify that multiple clients are not added to the list of clients if you specify any of the following Enterprise Vault 8.0 directives in the backup selection:
- **EV_INDEX_LOCATION**=
Recommended Action: Specify only one client in the policy, or remove the directive from the backup selection that does not support multiple client.

See the Troubleshooting section of the *NetBackup for Enterprise Vault Agent Administrator’s Guide*.

**NetBackup status code: 2000**

**Message:** Unable to allocate new media for backup, storage unit has none available.

**Explanation:** The NetBackup Media and Device Selection component (MDS) did not allocate a new tape volume for backups. This error indicates that the storage unit has no more volumes available in the volume pool for this backup. NetBackup does not change storage units during the backup.

**Recommended Action:** Try the following:

- **Recommended Action:** Check the NetBackup Problems report to determine the storage unit that is out of media.

- If the storage unit is a robot with empty slots, add more volumes and specify the correct volume pool. If no empty slots exist, move some media to nonrobotic and add new volumes. If you have difficulty keeping track of your available volumes, try the available_media script located in the following directory:
  
  On UNIX: `/usr/openv/netbackup/bin/goodies/available_media`
  
  On Windows: `install_path\NetBackup\bin\goodies\available_media.cmd`

  This script lists all volumes in the volume configuration, and augments that list with information on the volumes currently assigned to NetBackup.

- Set up a scratch volume pool as a reserve of unassigned tapes. If NetBackup needs a new tape and none are available in the current volume pool, it moves a tape from the scratch pool into the volume pool that the backup uses.

- If the storage unit and volume pool appear to have media, verify the following:
  
  - Use the NetBackup Media List report to check that the volume is not FROZEN or SUSPENDED. If the volume is frozen or suspended, use the `bpmedia` command to unfreeze or unsuspend it, if so desired.
  
  - Volume has not expired or exceeded its maximum number of mounts.
The EMM database host name for the device is correct. If you change the EMM database host name, stop and restart the following: the Media Manager device daemon, \texttt{ltid}, (if the server is UNIX) or the NetBackup Device Manager service (if the server is a Windows system).

The correct host is specified for the storage unit in the NetBackup configuration. The host connection must be the server (master or media) with drives connected to it.

The Media and Device Management volume configuration has media in the correct volume pool. Unassigned or active media is available at the required retention level. Use the NetBackup Media List report to show the retention levels, volume pools, and status for all volumes. Use the NetBackup Media Summary report to check for active volumes at the correct retention levels.

Create the \texttt{bptm} debug log directory, and set \texttt{mds} VxUL logging (oid 143) to debug level 2, then retry the operation.

If this storage unit is new and this attempt to use it is the first, stop and restart NetBackup on the master server. The \texttt{mds} unified logging files (OID 143) at debug level 2 usually show the NetBackup media selection process.

**NetBackup status code: 2001**

**Message:** No drives are available for this job

**Explanation:** A job requested a tape drive, but no eligible drive path was configured for the job.

**Recommended Action:** Try the following:

- Verify that the required drives and robots are configured and up.
- Verify that \texttt{ltid} is active and a drive path exists that is configured on the drive for the media server that the storage unit requires.
- If the job requires an NDMP drive path, verify that one exists.

**NetBackup status code: 2002**

**Message:** Invalid STU identifier type

**Explanation:** A job has asked for allocation using an invalid Storage Unit identifier type. The only valid Storage Unit identifier types are 0 (specific STU), 1 (group) or 2 (ANY).

**Recommended Action:** This error is internal. Call NetBackup support for resolution.

Check the following logs:
- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

**NetBackup status code: 2003**

**Message:** Drive is not allocated.

**Explanation:** MDS has been asked to deallocate a drive that is not allocated.

**Recommended Action:** This error is internal to the MDS component of NetBackup.

Check the following logs:
- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

**NetBackup status code: 2004**

**Message:** Drive is already allocated

**Explanation:** MDS has been erroneously asked to allocate a drive that is already allocated.

**Recommended Action:** A drive may have been reset while it was allocated for a job. Wait for the jobs that use the drive to complete.

**NetBackup status code: 2005**

**Message:** MDS has received an invalid message from a media server.

**Explanation:** `bptm` or `bpdm` on a media server has sent an improperly formatted message to MDS.

**Recommended Action:** This error is internal. Call NetBackup support if this error causes jobs to fail.

Check the following logs:
- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.
- The `bptm` legacy log from the media server, with VERBOSE=5.
NetBackup status code: 2006

**Message:** NDMP credentials are not defined in EMM.

**Explanation:** No eligible media server is configured with NDMP credentials to access the NDMP storage unit. Or, NetBackup tried to restore an NDMP image from a disk storage unit when the media server is not at NetBackup Release 6.5.2 or later.

**Recommended Action:** If the job uses an NDMP device, verify that the media server being used has NDMP credentials configured for the filer.

NetBackup status code: 2007

**Message:** Storage unit is not compatible with requesting job

**Explanation:** A job has asked for a storage unit that cannot be used for the job.

**Recommended Action:** This error can occur when a job tries to run on a media server that is not at a recent enough NetBackup revision level to run the job. The job may require a feature that is not available on the media server being requested. Verify that the storage unit type and media server called out by the policy and storage unit support the feature the job is trying to use.

This error can occur when the policy being run is not compatible with the storage units requested by the policy:

- SnapVault storage units are requested for multiple copy jobs.
- Catalog backups are directed to shared disk storage units.
- Multiplexed jobs are directed to storage units that do not have the multiplex feature configured.
- NDMP backup policies are directed to non-NDMP storage units.

NetBackup status code: 2008

**Message:** All compatible drive paths are down

**Explanation:** All configured drive that can be used for this job are down.

**Recommended Action:** Verify that `ltid` is running on the required media server, and the media server is active for tape. Using device monitor, bring up the drive paths if they are down. If drives are downed again, clean the drives.

NetBackup status code: 2009

**Message:** All compatible drive paths are down but media is available

**Explanation:** All configured drives that can be used for this job are down.
**Recommended Action:** Verify that `ltid` is running on the required media server, and the media server is active for tape. Using device monitor, bring up the drive paths if they are down. If drives are downed again, clean the drives.

**NetBackup status code: 2010**

**Message:** Job type is invalid

**Explanation:** The job type that is specified in an allocation request to the resource broker is not valid for the operation requested.

**Recommended Action:** This error is internal. Call NetBackup support if this error causes jobs to fail.

Check the following logs:
- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

**NetBackup status code: 2011**

**Message:** The media server reported a system error.

**Explanation:** An allocation for the media server is in an inconsistent state.

**Recommended Action:** This error is internal. Call NetBackup support if this error causes jobs to fail.

Check the following logs:
- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

**NetBackup status code: 2012**

**Message:** Media has conflicts in EMM

**Explanation:** Requested media for job cannot be used because it is marked as having conflicts in the `nbemm` database.

**Recommended Action:** The media is marked as having conflicts. The upgrade from NetBackup 5.x has found multiple volume databases where two tapes in different volume databases have the same media ID. Call technical support to resolve this situation.
**NetBackup status code: 2013**

**Message:** Error record insert failed

**Explanation:** A database record insert has failed.

**Recommended Action:** This error is internal. Call NetBackup support if this error causes jobs to fail.

Check the following logs:
- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

**NetBackup status code: 2014**

**Message:** Media is not assigned

**Explanation:** A job requires assigned media, but the requested media is not assigned.

**Recommended Action:** Verify that the job requested the desired media. For example, if you ask to list contents of the media, make sure you have specified the correct media ID.

Check the following logs:
- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

**NetBackup status code: 2015**

**Message:** Media is expired

**Explanation:** A job is trying to write to media that has already expired.

**Recommended Action:** Make sure that non-expired media is available for the job.

Check the following logs:
- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.
NetBackup status code: 2016

Message: Media is assigned to another server

Explanation: A job cannot use the media on the storage server, because the media is assigned to another storage server.

Recommended Action: Check the following logs:

- The mds unified logging files (OID 143) from the master server at debug level 2.
- The nbrb unified logging files (OID 118) from the master server at debug level 3.

NetBackup status code: 2017

Message: Media needs to be unmounted from a drive

Explanation: The requested media needs to be unmounted from the drive it is in before it can be used for another job.

Recommended Action: Identify the media requested by the job that returns this error. If it is used by another job, wait for that job to complete.

NetBackup status code: 2018

Message: Number of cleanings is invalid

Explanation: A cleaning media has an invalid number of cleanings that remain.

Recommended Action: On the Change Media screen, set the number of cleanings remaining for the cleaning media to a number greater than or equal to zero (0).

NetBackup status code: 2019

Message: Media is in a drive that is not configured on local system

Explanation: A job is configured to use a media volume that has no drive path configured to an eligible media server for the job. A media volume is misplaced or all drive paths are down for the media server accessible by the storage unit configured for a job.

Recommended Action: If drive paths are down, identify the media server configured for use by the storage unit, and bring up the drive path to that media server.

NetBackup status code: 2020

Message: Robotic library is down on server
**Explanation:** NetBackup has marked the robot as down for the required media server.

**Recommended Action:** Verify that the media server required for this allocation is running, and verify that \texttt{ltid} is up on that media server.

**NetBackup status code: 2021**

**Message:** Allocation record insert failed

**Explanation:** The NetBackup \texttt{mds} component was unable to update the database for a device allocation.

**Recommended Action:** This error is internal. Check the following logs:

- The \texttt{mds} unified logging files (OID 143) from the master server at debug level 2.
- The \texttt{nbrb} unified logging files (OID 118) from the master server at debug level 3.

**NetBackup status code: 2022**

**Message:** Allocation status record insert failed

**Explanation:** The NetBackup \texttt{mds} component was unable to update the database with device allocation status information.

**Recommended Action:** This error is internal. Check the following logs to help identify the problem:

- The \texttt{mds} unified logging files (OID 143) from the master server at debug level 2.
- The \texttt{nbrb} unified logging files (OID 118) from the master server at debug level 3.

**NetBackup status code: 2023**

**Message:** Allocation identifier is not known to EMM

**Explanation:** The NetBackup \texttt{mds} component cannot find the device allocation record needed to allocate the device for this job.

**Recommended Action:** This error is internal. Check the following logs to help identify the problem:

- The \texttt{mds} unified logging files (OID 143) from the master server at debug level 2.
The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

**NetBackup status code: 2024**

**Message:** Allocation request update failed

**Explanation:** The NetBackup `mds` component was unable to update the database for a device allocation.

**Recommended Action:** This error is internal. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

**NetBackup status code: 2025**

**Message:** Allocation request delete failed

**Explanation:** The NetBackup `mds` component was unable to delete a device allocation from the database.

**Recommended Action:** This error is internal. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

**NetBackup status code: 2026**

**Message:** Allocation status request delete failed

**Explanation:** The NetBackup `mds` component was unable to modify an allocation status record for this job.

**Recommended Action:** This error is internal. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.
NetBackup status code: 2027

Message: Media server is not active

Explanation: This job requires a media server that is not currently available.

Recommended Action:
Do one or more of the following:
■ Verify that the media server required for this allocation is running.
■ If this is a tape job, verify that ltid is running on the media server. If a media server has gone offline and returned online, a delay of several minutes may occur before a job can use that media server.
■ Use the vmoprcmd command to show the state of the media server. If the job is trying to access a disk storage unit, verify that the nbrmms process is running on the media server. If the job is trying to access a tape storage unit, verify that ltid is running on the media server.

NetBackup status code: 2028

Message: Media is reserved

Explanation: The NetBackup mds component cannot allocate media because another job has that media exclusively reserved.

Recommended Action: If multiple duplication jobs are attempting to use the same tape media for read, each will reserve the media. NetBackup should allow more than one job to get a reservation for the tape media.

This error is internal. Check the following logs to help identify the problem:
■ The mds unified logging files (OID 143) from the master server at debug level 2.
■ The nbrb unified logging files (OID 118) from the master server at debug level 3.

NetBackup status code: 2029

Message: EMM database is inconsistent

Explanation: An inconsistency in the NetBackup database is preventing allocations for this job.

Recommended Action: This error is internal. Check the following logs to help identify the problem:
■ The mds unified logging files (OID 143) from the master server at debug level 2.
The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

Run the `nbrbutil -resetall` command to get the NetBackup allocation database back into a consistent state. Note that this command cancels all jobs including those that are currently running.

**NetBackup status code: 2030**

**Message:** Insufficient disk space or high water mark would be exceeded

**Explanation:** Insufficient disk space is available to run this job.

**Recommended Action:** Try the following possible solutions:

- If there are images on disk that can be expired, expire them, and run `nbdelete` to delete the images from disk.
- It may be that NetBackup is creating disk images more quickly than they are expiring. If so, modifications to policies may be necessary to change the rate of image creation/expiration for the disk.
- It may be helpful to lower the high water mark and/or low water mark for the disk group.

**NetBackup status code: 2031**

**Message:** Media is not defined in EMM

**Explanation:** The media required for this job is not defined in the EMM database.

**Recommended Action:** A media volume required for a restore job has been deleted from the EMM database. If the media is available, use `bpimport` to import it.

**NetBackup status code: 2032**

**Message:** Media is in use according to EMM

**Explanation:** The NetBackup database indicates that the media is in use but is not allocated to another job.

**Recommended Action:** This error is internal. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.
NetBackup status code: 2033

Message: Media has been misplaced

Explanation: Job requires media that is not in the expected robotic slot.

Recommended Action: Verify that the media required by the job is in the proper robotic slot as shown by vmquery.

If the error persists, the following logs may be useful in understanding the problem:
- The mds unified logging files (OID 143) from the master server at debug level 2.
- The nbrb unified logging files (OID 118) from the master server at debug level 3.
- The verbose bptm logs on the media server(s) that access this media.

NetBackup status code: 2034

Message: Retry the allocation request later

Explanation: Resources required for a job are currently in use.

Recommended Action: This error should never appear as a job return status. In the mds and nbrb vxul logs, it indicates that a job should queue because resources are busy.

NetBackup status code: 2035

Message: Request needs to pend

Explanation: A job requires operator intervention before it can continue.

Recommended Action: This error should never appear as a job return status. In the mds and nbrb vxul logs, it indicates that a job should post a request for operator intervention to the NetBackup device monitor.

NetBackup status code: 2036

Message: Drive is in a robotic library that is up

Explanation: Operator has attempted to assign a pending tape mount request to a drive that is in a robot that is up.

Recommended Action: A request for non-robotic media may have caused a pending request in the device monitor, and the operator has assigned the request to a drive that is not a standalone drive. This error is not fatal. The request will pend again in the NetBackup device monitor. Assign the pending mount to a standalone drive or to a drive that is in AVR mode (non-robotic).
NetBackup status code: 2037

*Message:* Drive is not ready

*Explanation:* The required tape is in a drive, but the drive is not in a ready state.

*Recommended Action:* This error may occur when a request for non-robotic media had caused a pending request in the device monitor, and the operator has assigned the request to a drive that is not in a ready state. This is not a fatal error, the request will pend again in the NetBackup device monitor. Verify that required tape is in the drive it is being assigned to, and that the drive ready light has come on. It may take some time for the drive to become ready after the tape has been inserted. If the drive never goes to a ready state after a tape has been inserted, there may be a problem with the drive.

NetBackup status code: 2038

*Message:* Media loaded in drive is not write-enabled

*Explanation:* This error may occur when a storage unit request for non-robotic media had caused a pending request in the device monitor, and the operator has inserted media that is not write enabled into the drive.

*Recommended Action:* This is not a fatal error, the request will pend again in the NetBackup device monitor. If you are sure it is OK to write on this tape, verify that the required tape has its write enable switch set to allow write.

NetBackup status code: 2039

*Message:* SCSI reservation conflict detected

*Explanation:* The NetBackup bptm component was unable to read or write a tape drive because another job unexpectedly holds a SCSI reservation for the drive.

*Recommended Action:* This error should never occur at job resource allocation time, but may occur during i/o for a tape job. The verbose bptm logs on the media server may be useful in understanding the problem.

NetBackup status code: 2040

*Message:* Maximum job count has been reached for the storage unit

*Explanation:* Storage cannot be allocated because it would exceed maximum job count. The maximum job count is configurable for each storage unit. Multiple copy jobs may cause this same error, if more copies are targeted for a storage unit than the storage unit is configured for.

*Recommended Action:* Target a different storage unit with one of the copies, or increase the maximum job count for the storage unit.
NetBackup status code: 2041
Message: Storage unit is down
Explanation: A disk storage unit has been designated as down and cannot be used.
Recommended Action: Run the `bperror -disk` command to indicate why the disk is considered down.

NetBackup status code: 2042
Message: Density mismatch detected
Explanation: This error is an internal NetBackup error. A job has requested media with the wrong density. A mismatch may exist between the image catalog and the media database.
Recommended Action: Restore the job's request tape media by media ID density. If the requested density does not match the configured density for the media, it cannot be allocated.

NetBackup status code: 2043
Message: Requested slot is empty
Explanation: Media is not found in the expected slot in the robot.
Recommended Action: The robot may need to be inventoried.

NetBackup status code: 2044
Message: Media is assigned to another application
Explanation: Requested media cannot be allocated because it is assigned to an application other than NetBackup.
Recommended Action: Verify that media required for the job is assigned to NetBackup.

NetBackup status code: 2045
Message: Storage unit is disabled since max job count is less than 1
Explanation: Storage unit cannot be used because its maximum job count is set to 0.
Recommended Action: Increase the maximum job count (or maximum concurrent drive count) to a value greater than 0.
NetBackup status code: 2046
Message: Media is unmountable
Explanation: Media has been marked as unusable due to mount errors.
Recommended Action: Clean the drives in the media's robot. Determine whether any of the media is bad.

NetBackup status code: 2047
Message: Media is write protected
Explanation: The media cannot be used for a write job because it is write protected.
Recommended Action: Make sure that media in the scratch pool is not write protected.

NetBackup status code: 2048
Message: Media is in use by the ACS robotic library
Explanation: ACS media required by this job is in use on another system.
Recommended Action: Make sure that the required media is not in use by another application.

NetBackup status code: 2049
Message: Media not found in the ACS robotic library
Explanation: Media needed by this job is not found in the ACS robotic library.
Recommended Action: Make sure that the required media is available in the ACS robot.
For more information, refer to the section on configuring ACSLS robots in the NetBackup Device Configuration Guide.

NetBackup status code: 2050
Message: ACS media has an unreadable external label
Explanation: This job needs ACS media that cannot be used because its external label or barcode is unreadable.
Recommended Action: Correct the barcode label problem for this media.
For more information, refer to the section on configuring ACSLS robots in the NetBackup Device Configuration Guide.
NetBackup status code: 2051
Message: ACS media is not in the drive's domain
Explanation: Media required for this job is in an ACS robot that is not accessible.
Recommended Action: Verify that the robot that contains the required media is accessible to a NetBackup media server.
For more information, refer to the section on configuring ACSLS robots in the NetBackup Device Configuration Guide.

NetBackup status code: 2052
Message: An ACS Library Storage Module (LSM) is offline
Explanation: The required ACS LSM is offline.
Recommended Action: Bring the ACS LSM online.
For more information, refer to the section on configuring ACSLS robots in the NetBackup Device Configuration Guide.

NetBackup status code: 2053
Message: Media is in an inaccessible drive
Explanation: The required media is currently loaded in a DOWN or otherwise inaccessible drive.
Recommended Action: Locate the media and correct the problem that has caused the drive or drive path to be down.

NetBackup status code: 2054
Message: Media is in a drive that is currently in a DOWN state
Explanation: Required media is currently loaded in a drive that is down.
Recommended Action: Locate the media and correct the problem that has caused the drive or drive path to be downed.

NetBackup status code: 2055
Message: ACS physical drive is not available
Explanation: The media server cannot load ACS media because a drive is not available.
Recommended Action:

NetBackup status code: 2056

**Message:** The file name used for the mount request already exists

**Explanation:** The `tpreq` command cannot load this media because the specified file name already exists.

**Recommended Action:** Specify a different file name for `tpreq`, or run the `tpunmount` command for the media which has been loaded using `tpreq` with the conflicting file name.

NetBackup status code: 2057

**Message:** The scan host of the drive is not active

**Explanation:** The scan host for a standalone drive is offline, so the drive cannot be allocated.

**Recommended Action:** If the problem persists, restart the NetBackup media servers that have paths to this drive.

NetBackup status code: 2058

**Message:** LTID needs to be restarted on media servers before the device can be used

**Explanation:** A drive cannot be used because an `ltid` restart is required. This error may occur when configuration changes have been made on a media server, but `ltid` has not been subsequently restarted.

**Recommended Action:** When the media server is not in a busy state, stop and restart `ltid` on that media server.

NetBackup status code: 2059

**Message:** The robotic library is not available

**Explanation:** The robot required for a drive cannot be found in the `nbemm` database.

**Recommended Action:** Verify that the robot required by jobs is properly configured. If the error persists, the following logs may be useful in understanding the problem: The `mds` unified logging files (OID 143) from the master server at debug level 2.
NetBackup status code: 2060
Message: Media needs to be rewound or unmounted from a drive
Explanation: The NetBackup mds component uses this error internally to inform the resource broker that a tape needs to be unloaded. It should never appear as a job error status.
Recommended Action:

NetBackup status code: 2061
Message: The host is not an active node of a cluster
Explanation: A cluster failover has occurred while a job is running. A job may be waiting for a span on a media server that has failed over.
Recommended Action: Restart the failed job.

NetBackup status code: 2062
Message: Throttled job count has been reached for the storage unit
Explanation: This error will never be returned as a job status.

NetBackup status code: 2063
Message: Server is not licensed for the Remote Client Option
Explanation: The media server required for this job does not have the Remote Client Option enabled. A SAN media server is asked to backup a client that is not also a media server, or a VMware backup is tried on a SAN media server.
Recommended Action: Back up this client on a media server that is licensed to do so. Verify that the media server has connectivity to the master server when adding its licenses.

NetBackup status code: 2064
Message: Job history indicates that no media is available
Explanation: When a job is run on a media server installed with pre NetBackup 6.0 software, there are some situations where the job starts, but media is not available for the job. In this case, the master server stops using that storage unit for a period of time (12 hours), and returns this error for jobs requested the storage unit.
Recommended Action: Make sure media is available for the storage unit. Add media if necessary. If media is available, wait 12 hours until the storage unit can
be used again. To make the storage unit immediately usable, run the following command on the master server to release:

**Recommended Action:** `nbrbutil -releaseAllocHolds`

**NetBackup status code: 2065**

**Message:** Job history indicates that no drive is available

**Explanation:** When a job is run on a media server installed with pre NetBackup 6.0 software, there are some situations where the job starts, but the drives designated for the job are busy or otherwise unavailable, causing the job to fail. In this case, the NetBackup master server stops using that drive for a period of time (several minutes), and returns this error for jobs requesting that drive.

**Recommended Action:** Make sure all of the drives in the storage unit are up and available for use. Clean all drives that need cleaning.

**NetBackup status code: 2066**

**Message:** Disk pool not found

**Explanation:** A job has been targeted for a disk pool that does not exist in the nbemm database.

**Recommended Action:** Verify that the storage unit used by this job is configured for use with a properly configured disk pool.

**NetBackup status code: 2067**

**Message:** Disk volume not found

**Explanation:** A read job requires a disk volume that does not exist in the nbemm database. Or a write job is configured for a disk pool with no configured volumes.

**Recommended Action:** Verify that the disk storage used by this job is configured for use with a disk pool that has volumes configured. For a read job, verify that the volume required for reading exists in the nbemm database.

**NetBackup status code: 2068**

**Message:** Disk volume mount point not found

**Explanation:** A disk volume is not configured with a mount point or not completely configured in the nbemm database.

**Recommended Action:** Verify that the configuration is correct for the disk group and for the disk volumes in the disk group.
NetBackup status code: 2069

Message: Disk volume mount point record insert failed

Explanation: A database updata has failed while trying to allocate a disk job.

Recommended Action: This error is internal. If the problem persists, please call NetBackup support for resolution. Check the following logs to help identify the problem:

- The mds unified logging files (OID 143) from the master server at debug level 2.
- The nbrb unified logging files (OID 118) from the master server at debug level 3.

NetBackup status code: 2070

Message: The specified mount path will not fit in the allocated space

Explanation: A disk volume mount point path is larger than the allowed maximum.

Recommended Action: This error is internal. If the problem persists, please call NetBackup support for resolution. Check the following logs to help identify the problem:

- The mds unified logging files (OID 143) from the master server at debug level 2.
- The nbrb unified logging files (OID 118) from the master server at debug level 3.

NetBackup status code: 2071

Message: Unable to find any storage servers for the request

Explanation: NetBackup was unable to find a storage server for this disk job.

Recommended Action: Verify that storage servers serving the disk group required by the job are configured and enabled. Verify that they are in an UP state.

NetBackup status code: 2072

Message: Invalid operation on static mount point

Explanation: An incorrectly configured mount point has been found for a disk volume.

Recommended Action: This error is internal. If the problem persists, please call NetBackup support for resolution. Check the following logs to help identify the problem:
The mds unified logging files (OID 143) from the master server at debug level 2.

The nbrb unified logging files (OID 118) from the master server at debug level 3.

NetBackup status code: 2073

Message: Disk pool is down
Explanation: Required disk pool cannot be used because it is in a DOWN state.
Recommended Action: Run the berror -disk command to determine why the disk pool was put into a DOWN state. Correct the problem, and use the nbdevconfig command to return the disk pool to an UP state.

NetBackup status code: 2074

Message: Disk volume is down
Explanation: Required disk volume cannot be used because it is in a DOWN state.
Recommended Action: You may be able to see why the disk volume was put into a DOWN state by running 'berror -disk'. Correct the problem, and use nbdevconfig to return the disk volume to an UP state.

NetBackup status code: 2075

Message: Fibre Transport resources are not available
Explanation: A job is configured to require Fibre Transport for this SAN client, but no available Fibre Transport connection exists.
Recommended Action: Configure the job to switch to LAN transport if Fibre Transport is not available. Verify that the job type being run is compatible with Fibre Transport. Using nbdevquery, verify that the Disk Pool being requested is enabled for use with Fibre Transport. Verify that there are Fibre Transport connections that are up between the client and media server required for the job. Check the following logs to help identify the problem:

- The mds unified logging files (OID 143) from the master server at debug level 2.
- The nbrb unified logging files (OID 118) from the master server at debug level 3.

NetBackup status code: 2076

Message: DSM returned an unexpected error
Explanation: The Disk Service Manager component of NetBackup has returned an unexpected error.

Recommended Action: This error is internal. If the problem persists, please call NetBackup support for resolution. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

NetBackup status code: 2077

Message: DSM has already mounted the volume

Explanation: Mount of a SharedDisk volume (NetBackup 6.5 media servers only) has failed because it is already mounted.

Recommended Action: This error is internal. If the problem persists, please call NetBackup support for resolution. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

NetBackup status code: 2078

Message: The maximum number of mounts for the disk volume have been exceeded

Explanation: A disk volume cannot be used by a job because it is mounted by too many other users.

Recommended Action: This error is internal. If the problem persists, please call NetBackup support for resolution. Check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.
NetBackup status code: 2079

Message: DSM has detected that an invalid filesystem is mounted on the volume
Explanation: NetBackup did not find the file system it expected on a disk volume.
Recommended Action: Verify that disk volumes and their associated mount points that NetBackup uses, are not being used by other applications.

NetBackup status code: 2080

Message: Disk volume has no max writers count
Explanation: Disk volume is not properly configured for a usable number of mountpoints.
Recommended Action: Verify proper disk configuration using nbdevquery. This error is internal. If the problem persists, please call NetBackup support for resolution. Check the following logs to help identify the problem:
- The mds unified logging files (OID 143) from the master server at debug level 2.
- The nbrb unified logging files (OID 118) from the master server at debug level 3.

NetBackup status code: 2081

Message: Disk volume has no max readers count
Explanation: Disk volume is not properly configured for a usable number of mountpoints.
Recommended Action: Verify proper disk configuration using nbdevquery. This error is internal. If the problem persists, please call NetBackup support for resolution. Check the following logs to help identify the problem:
- The mds unified logging files (OID 143) from the master server at debug level 2.
- The nbrb unified logging files (OID 118) from the master server at debug level 3.

NetBackup status code: 2082

Message: The drive needs to be marked as available
Explanation: Drive cannot be used because it is allocated with loaded media, but MDS has not made it available for use.
**Recommended Action:** Run the `nbrbutil -dump` command on the master server to show allocations for this job. If the problem persists, run the `nbrbutil -releaseMDS` command to release the allocation for the drive so it can be used.

**NetBackup status code: 2083**

**Message:** The media affinity group is not defined in EMM

**Explanation:** MDS expected to find a group of reservations for this media, but did not find the expected reservation group.

**Recommended Action:** This error is internal. If the problem persists, check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

**NetBackup status code: 2084**

**Message:** Media affinity group record insert failed

**Explanation:** MDS could not update reservation group information for this tape media.

**Recommended Action:** This error is internal. If the problem persists, check the following logs to help identify the problem:

- The `mds` unified logging files (OID 143) from the master server at debug level 2.
- The `nbrb` unified logging files (OID 118) from the master server at debug level 3.

**NetBackup status code: 2085**

**Message:** Disk volume is not available

**Explanation:** The job requires more disk volumes than are currently configured.

**Recommended Action:** Ensure that the disk group has disk volumes configured. A multiple copy job cannot target two copies for the same disk volume.

**NetBackup status code: 2086**

**Message:** Disk volume cannot be used for more than one copy in the same job
**Explanation:** Not enough eligible disk volumes are configured for this multiple copy job.

**Recommended Action:** Use the `nbdevquery -listdv` command to verify that the expected disk volume is configured. For a multiple copy job, ensure that unique eligible disk volumes exist for each copy. A multiple copy job cannot target two copies for the same disk volume.

**NetBackup status code: 2087**

**Message:** Media allocation would exceed maximum partially full media limit

**Explanation:** You cannot run this job because it would exceed configured limit of maximum partially full media.

**Recommended Action:** This error may occur with a multiple copy job or a duplication job. If the problem persists, you may need to increase maximum partially full media setting on the disk pool.

**NetBackup status code: 2088**

**Message:** Cleaning media is not available

**Explanation:** You cannot run a cleaning job because no cleaning media is configured for the drive.

**Recommended Action:** Add a cleaning volume to the robot containing the drive.

**NetBackup status code: 2089**

**Message:** FT client is not running

**Explanation:** This job requires Fibre Transport, but the Fibre Transport client is not running on the client required for this job.

**Recommended Action:** Do one or more of the following:

- Verify that the Private Branch Exchange (PBX) service is installed and running. Run the `bppps -x` command to ensure that `pbx_exchange` is listed in the processes that are running.

- Verify that the client is configured as a SAN Client. Run the `bpclntcmd -sanclient` command to return the current state of the SAN Client. A response of 0 (zero) indicates that SAN Client is not configured. Rerun the command as `bpclntcmd -sanclient 1`.

- Verify that the client is not also a media server, master server, or EMM server. The SAN Client process runs only on a NetBackup client.
■ Verify that a valid license for the SAN Client feature resides on the master server. SAN Client is a separately licensed feature which requires a key called "SAN Client" on the master server.

■ Verify that no server entries for the SAN Client exist on the NetBackup master server. Remove any SERVER=clientname entry in the master server for the SAN Client. If the master server has the SAN Client listed also as a server, it may shut down the SAN Client.

■ Restart the SAN Client service. The SAN Client restarts when the server reboots, but does not automatically restart after you run the bpcclntcmd command. To start the SAN Client service, run the client startup script or use the Service Manager in Windows.

For further information, see the Troubleshooting chapter of the *NetBackup SAN Client and Fibre Transport Guide*.

**NetBackup status code: 2090**

**Message:** FT client has no devices configured

**Explanation:** This job requires Fibre Transport, but Fibre Transport devices are not configured on the client required for this job.

**Recommended Action:** Verify that Fibre Transport devices are installed on the client. For further information, see the Troubleshooting chapter of the *NetBackup SAN Client and Fibre Transport Guide*.

**NetBackup status code: 2091**

**Message:** FT client devices are offline

**Explanation:** This job requires Fibre Transport, but all Fibre Transport devices are offline on the client required for this job.

**Recommended Action:** Do one or more of the following:

■ Verify that the Private Branch Exchange (PBX) service is installed and running. Run the bpps -x command to ensure that pbx_exchange is listed in the processes that are running.

■ Verify that the client is configured as a SAN Client. Run the bpcclntcmd -sanclient command to return the current state of the SAN Client. A response of 0 (zero) indicates that SAN Client is not configured. Rerun the command as bpcclntcmd -sanclient 1.

■ Verify that the client is not also a media server, master server, or EMM server. The SAN Client process runs only on a NetBackup client.
- Verify that a valid license for the SAN Client feature resides on the master server. SAN Client is a separately licensed feature which requires a key called "SAN Client" on the master server.

- Verify that no server entries for the SAN Client exist on the NetBackup master server. Remove any SERVER=clientname entry in the master server for the SAN Client. If the master server has the SAN Client listed also as a server, it may shut down the SAN Client.

- Restart the SAN Client service. The SAN Client restarts when the server reboots, but does not automatically restart after you run the bpclntcmd command. To start the SAN Client service, run the client startup script or use the Service Manager in Windows.

For further information, see the Troubleshooting chapter of the NetBackup SAN Client and Fibre Transport Guide.

**NetBackup status code: 2092**

**Message:** FT server devices for client are offline

**Explanation:** This job requires Fibre Transport, but all Fibre Transport devices are offline on the media server required for this job.

**Recommended Action:** Do one of the following:

- Verify that marked QLogic Target ports exist in the server. The nbftsrvr and nbfdrv64 processes exit if the system has no ports available for Target Mode use.

- Verify that a valid license for the SAN Client feature resides on the master server. SAN Client is a separately licensed feature which requires a key called "SAN Client" on the master server. The Fibre Transport server performs a license check during startup.

- Determine if a reboot is required for the installation of the Fibre Transport server. Solaris installations require that you reboot the media server after you install Fibre Transport to load the Fibre Transport drivers on the marked target ports. In addition, reboot the Linux servers if you choose to not unload the existing QLogic drivers during the installation of Fibre Transport.

For further information, see the Troubleshooting chapter of the NetBackup SAN Client and Fibre Transport Guide.

**NetBackup status code: 2093**

**Message:** No FT servers for this client are running
Explanation: This job requires Fibre Transport, but no Fibre Transport devices are configured with connectivity to the media server required for this job.

Recommended Action: Do one of the following:

- Verify that marked QLogic Target ports exist in the server. The `nbftsrvr` and `nbfdrv64` processes exit if the system has no ports available for Target Mode use.

- Verify that a valid license for the SAN Client feature resides on the master server. SAN Client is a separately licensed feature which requires a key called "SAN Client" on the master server. The Fibre Transport server performs a license check during startup.

- Determine if a reboot is required for the installation of the Fibre Transport server. Solaris installations require that you reboot the media server after you install Fibre Transport to load the Fibre Transport drivers on the marked target ports. In addition, reboot the Linux servers if you choose to not unload the existing QLogic drivers during the installation of Fibre Transport.

Recommended Action: For further information, please refer to the NetBackup SAN Client and Fibre Transport Troubleshooting Guide.

NetBackup status code: 2094

Message: STU cannot run Lifecycle backups

Explanation: The storage lifecycle job cannot run because the targeted disk pool is not enabled for Storage Lifecycles.

Recommended Action: Run the `nbdevquery -listdg` command to check the configuration of the disk pool. If the LifeCycle attribute is not enabled for the disk pool, run the `nbdevconfig -changedp -setattribute` command to enable it.

NetBackup status code: 2095

Message: STU cannot run VMWare backup

Explanation: The media server configured for this job’s storage unit cannot run VMWare backups.

Recommended Action: To run a VMWare backup, a media server must run NetBackup Release 6.5 or greater. Verify that this is so, or configure the backup for a media server that runs NetBackup Release 6.5 or later.

NetBackup status code: 2096

Message: NDMP operation does not support multiple inline copies
**Explanation:** The backup cannot run because it is an NDMP policy and is configured for multiple copies.

**Recommended Action:** NetBackup cannot make multiple copies of NDMP policies. Configure the backup for a single storage unit destination.

**NetBackup status code: 2097**

**Message:** Storage Unit group does not exist in EMM configuration

**Explanation:** You cannot run this job because it is configured to use a storage unit group that does not exist in the NetBackup configuration.

**Recommended Action:** Reconfigure the policy to use a storage unit or storage unit group that exists in the configuration.

**NetBackup status code: 2098**

**Message:** Media pool is not eligible for this job

**Explanation:** This job is configured to use a pool that does not exist in the NetBackup configuration.

**Recommended Action:** Change the configured media pool for the job to use a pool that is configured, or create the required media pool. Make sure that the media pool you have configured for the job is not a scratch pool.

**NetBackup status code: 2099**

**Message:** Required drive or drive path is not configured

**Explanation:** This job requires a drive that does not exist in the NetBackup configuration.

**Recommended Action:** Run the `vmoprcmd` command to verify the drive configuration. Configure the drives that are necessary for the media type that is being used.

**NetBackup status code: 2100**

**Message:** Maximum number of mounts has been exceeded for tape media

**Explanation:** The job cannot run because the required media has exceeded configured maximum mounts.

**Recommended Action:** Increase the maximum allowed mounts for the media. You may need to retire this media if it has exceeded the maximum number of mounts you have configured.
NetBackup status code: 2101

**Message:** Media server not found in EMM database

**Explanation:** The media server required for this job does not exist in the NetBackup database.

**Recommended Action:** For restore from tape, the media server originally used to write the image is used for restore. If this media server does not exist in the NetBackup database, you may use the Force Media Server Restore option to force NetBackup to replace the missing media server with a new media server.

NetBackup status code: 2102

**Message:** Storage unit does not support spanning

**Explanation:** A disk job has requested a span for a disk type that does not support spanning.

**Recommended Action:** Some disk types do not support spanning. Run the `nbdevconfig -listdg` command to determine if a disk group supports spanning. If this error persists, ensure that enough space is available on your disk storage units for the new jobs that are running.

NetBackup status code: 2103

**Message:** Media server mismatch

**Explanation:** This error may occur when a multiple copy job is configured for storage units that have no common media server.

**Recommended Action:** All copies of a multiple copy job must run on the same media server. Configure storage units that have drive paths or disk access from a common media server.

NetBackup status code: 2104

**Message:** Storage units are not available

**Explanation:** This error may occur for multiple copy jobs configured so that no possible storage unit combination can be used.

**Recommended Action:** Verify that all criteria in met for the policy with the storage units that are configured.
NetBackup Messages

This section lists the NetBackup error messages alphabetically. The status code for each message is listed in the right column of the table. Refer to the previous list of status codes for explanations and recommended actions.

Table 5-1 lists the NetBackup error messages alphabetically.

Table 5-1  NetBackup error messages and status codes

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code</th>
</tr>
</thead>
<tbody>
<tr>
<td>/usr/openv/netbackup/bp.conf not found</td>
<td>110</td>
</tr>
<tr>
<td>a protocol error has occurred</td>
<td>232</td>
</tr>
<tr>
<td>access to server backup restore manager denied</td>
<td>206</td>
</tr>
<tr>
<td>access to the client was not allowed</td>
<td>59</td>
</tr>
<tr>
<td>ACS media has an unreadable external label</td>
<td>2050</td>
</tr>
<tr>
<td>ACS media is not in the drive's domain</td>
<td>2051</td>
</tr>
<tr>
<td>ACS physical drive is not available</td>
<td>2055</td>
</tr>
<tr>
<td>action succeeded but auditing failed</td>
<td>108</td>
</tr>
<tr>
<td>afs/dfs command failed</td>
<td>78</td>
</tr>
<tr>
<td>all compatible drive paths are down</td>
<td>2008</td>
</tr>
<tr>
<td>all compatible drive paths are down but media is available</td>
<td>2009</td>
</tr>
<tr>
<td>all configured vault steps failed</td>
<td>351</td>
</tr>
<tr>
<td>all volumes are not available to eject</td>
<td>297</td>
</tr>
<tr>
<td>allocation identifier is not known to EMM</td>
<td>2023</td>
</tr>
<tr>
<td>allocation failed</td>
<td>10</td>
</tr>
<tr>
<td>allocation record insert failed</td>
<td>2021</td>
</tr>
<tr>
<td>allocation request delete failed</td>
<td>2025</td>
</tr>
<tr>
<td>allocation request update failed</td>
<td>2024</td>
</tr>
<tr>
<td>allocation status record insert failed</td>
<td>2022</td>
</tr>
<tr>
<td>allocation status request delete failed</td>
<td>2026</td>
</tr>
<tr>
<td>an ACS Library Storage Module (LSM) is offline</td>
<td>2052</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>an entry in the filelist expanded to too many characters</td>
<td>70</td>
</tr>
<tr>
<td>an exception condition occurred</td>
<td>600</td>
</tr>
<tr>
<td>an extended error status has been encountered, check detailed status</td>
<td>252</td>
</tr>
<tr>
<td>an extension package is needed but was not installed</td>
<td>9</td>
</tr>
<tr>
<td>an invalid entry was encountered</td>
<td>223</td>
</tr>
<tr>
<td>another NB database backup is already in progress</td>
<td>125</td>
</tr>
<tr>
<td>archive file removal failed</td>
<td>4</td>
</tr>
<tr>
<td>a session is already running for this vault</td>
<td>275</td>
</tr>
<tr>
<td>a synthetic backup request for media resources failed</td>
<td>660</td>
</tr>
<tr>
<td>authentication failed</td>
<td>160</td>
</tr>
<tr>
<td>Backup Exec operation failed</td>
<td>151</td>
</tr>
<tr>
<td>backup restore manager failed to read the file list</td>
<td>53</td>
</tr>
<tr>
<td>backups are not allowed to span media</td>
<td>166</td>
</tr>
<tr>
<td>bpcord startup validation failure</td>
<td>669</td>
</tr>
<tr>
<td>bpjava-msvc: the client is not compatible with this server version</td>
<td>513</td>
</tr>
<tr>
<td>server_version</td>
<td></td>
</tr>
<tr>
<td>bpstart_notify failed</td>
<td>73</td>
</tr>
<tr>
<td>cannot connect on socket</td>
<td>25</td>
</tr>
<tr>
<td>cannot connect to nbvault server</td>
<td>282</td>
</tr>
<tr>
<td>cannot connect to read media server</td>
<td>613</td>
</tr>
<tr>
<td>cannot connect to server backup restore manager</td>
<td>205</td>
</tr>
<tr>
<td>Can not connect to the NB-Java authentication service on the configured port</td>
<td>505</td>
</tr>
<tr>
<td>configured_port_number. Check the log file for more details.</td>
<td></td>
</tr>
<tr>
<td>Can not connect to the NB-Java authentication service via VNETD on host on port</td>
<td>525</td>
</tr>
<tr>
<td>vnetd_configured_port_number. Check the log file for more details.</td>
<td></td>
</tr>
<tr>
<td>Error message</td>
<td>Status code</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Can not connect to the NB-Java user service on port <code>port_number</code>. Check the log file for more details.</td>
<td>506</td>
</tr>
<tr>
<td>Can not connect to the NB-Java user service via VNETD on (host) or port (configured_port_number)</td>
<td>517</td>
</tr>
<tr>
<td>cannot consolidate reports of sessions from container and slot-based vaults</td>
<td>289</td>
</tr>
<tr>
<td>Can not execute program</td>
<td>509</td>
</tr>
<tr>
<td>cannot find configuration database record for requested NB database backup</td>
<td>120</td>
</tr>
<tr>
<td>cannot find requested volume pool in EMM database</td>
<td>167</td>
</tr>
<tr>
<td>cannot find robot in vault configuration file</td>
<td>323</td>
</tr>
<tr>
<td>cannot find robot, vault, or profile in the vault configuration</td>
<td>266</td>
</tr>
<tr>
<td>cannot find the local host name</td>
<td>267</td>
</tr>
<tr>
<td>cannot find vault in vault configuration file</td>
<td>322</td>
</tr>
<tr>
<td>cannot get a bound socket</td>
<td>146</td>
</tr>
<tr>
<td>cannot make required directory</td>
<td>35</td>
</tr>
<tr>
<td>cannot modify - stale view</td>
<td>342</td>
</tr>
<tr>
<td>cannot overwrite media, data on it is protected</td>
<td>168</td>
</tr>
<tr>
<td>cannot perform specified media import operation</td>
<td>176</td>
</tr>
<tr>
<td>cannot position to correct image</td>
<td>94</td>
</tr>
<tr>
<td>cannot read backup header, media may be corrupted</td>
<td>173</td>
</tr>
<tr>
<td>cannot read media header, may not be NetBackup media or is corrupted</td>
<td>172</td>
</tr>
<tr>
<td>\cannot register handler for accepting new connections</td>
<td>603</td>
</tr>
<tr>
<td>cannot send extents to bpsynth</td>
<td>612</td>
</tr>
<tr>
<td>cannot set non blocking mode on the listen socket</td>
<td>602</td>
</tr>
<tr>
<td>cannot start reader on the media server</td>
<td>614</td>
</tr>
<tr>
<td>Can not write file</td>
<td>508</td>
</tr>
</tbody>
</table>
### Table 5-1  NetBackup error messages and status codes *(continued)*

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code</th>
</tr>
</thead>
<tbody>
<tr>
<td>can't connect to client</td>
<td>58</td>
</tr>
<tr>
<td>child process killed by signal</td>
<td>27</td>
</tr>
<tr>
<td>Cleaning media is not available</td>
<td>2088</td>
</tr>
<tr>
<td>client backup failed to read the file list</td>
<td>67</td>
</tr>
<tr>
<td>client backup failed to receive the CONTINUE BACKUP message</td>
<td>66</td>
</tr>
<tr>
<td>client backup was not attempted</td>
<td>195</td>
</tr>
<tr>
<td>client backup was not attempted because backup window closed</td>
<td>196</td>
</tr>
<tr>
<td>client cannot read the mount table</td>
<td>60</td>
</tr>
<tr>
<td>client connection refused</td>
<td>57</td>
</tr>
<tr>
<td>client did not start</td>
<td>49</td>
</tr>
<tr>
<td>client hostname could not be found</td>
<td>48</td>
</tr>
<tr>
<td>client is not validated to perform the requested operation</td>
<td>135</td>
</tr>
<tr>
<td>client is not validated to use the server</td>
<td>131</td>
</tr>
<tr>
<td>client name mismatch</td>
<td>39</td>
</tr>
<tr>
<td>client process aborted</td>
<td>50</td>
</tr>
<tr>
<td>client timed out reading file</td>
<td>76</td>
</tr>
<tr>
<td>client timed out waiting for bpstart_notify to complete</td>
<td>75</td>
</tr>
<tr>
<td>client timed out waiting for bpstart_notify to complete</td>
<td>74</td>
</tr>
<tr>
<td>client timed out waiting for the continue message from the media manager</td>
<td>65</td>
</tr>
<tr>
<td>client timed out waiting for the file list</td>
<td>68</td>
</tr>
<tr>
<td>client’s network is unreachable</td>
<td>56</td>
</tr>
<tr>
<td>client/server handshaking failed</td>
<td>26</td>
</tr>
<tr>
<td>communication interrupted</td>
<td>234</td>
</tr>
<tr>
<td>connection refused by server backup restore manager</td>
<td>204</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>connection to the peer process does not exist</td>
<td>622</td>
</tr>
<tr>
<td>container cannot hold any media from the specified robot</td>
<td>321</td>
</tr>
<tr>
<td>container database close operation failed</td>
<td>317</td>
</tr>
<tr>
<td>container database lock operation failed</td>
<td>318</td>
</tr>
<tr>
<td>container database open operation failed</td>
<td>319</td>
</tr>
<tr>
<td>container database truncate operation failed</td>
<td>314</td>
</tr>
<tr>
<td>container does not exist in container database</td>
<td>313</td>
</tr>
<tr>
<td>container_id is not unique in container database</td>
<td>316</td>
</tr>
<tr>
<td>continue</td>
<td>221</td>
</tr>
<tr>
<td>could not deassign media due to Media Manager error</td>
<td>177</td>
</tr>
<tr>
<td>could not get group information</td>
<td>38</td>
</tr>
<tr>
<td>could not get passwd information</td>
<td>30</td>
</tr>
<tr>
<td>could not set group id for process</td>
<td>32</td>
</tr>
<tr>
<td>could not set user id for process</td>
<td>31</td>
</tr>
<tr>
<td>daemon fork failed</td>
<td>148</td>
</tr>
<tr>
<td>daemon is already running</td>
<td>145</td>
</tr>
<tr>
<td>data marshalling error</td>
<td>625</td>
</tr>
<tr>
<td>data un-marshalling error</td>
<td>626</td>
</tr>
<tr>
<td>database system error</td>
<td>220</td>
</tr>
<tr>
<td>density is incorrect for the media id</td>
<td>179</td>
</tr>
<tr>
<td>density mismatch detected</td>
<td>2042</td>
</tr>
<tr>
<td>disk is full</td>
<td>155</td>
</tr>
<tr>
<td>Disk pool is down</td>
<td>2073</td>
</tr>
<tr>
<td>Disk pool not found</td>
<td>2066</td>
</tr>
<tr>
<td>Disk storage unit is full</td>
<td>129</td>
</tr>
</tbody>
</table>
## Table 5-1  NetBackup error messages and status codes (continued)

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk volume cannot be used for more than one copy in the same job</td>
<td>2086</td>
</tr>
<tr>
<td>Disk volume has no max readers count</td>
<td>2081</td>
</tr>
<tr>
<td>Disk volume has no max writers count</td>
<td>2080</td>
</tr>
<tr>
<td>Disk volume is down</td>
<td>2074</td>
</tr>
<tr>
<td>Disk volume is not available</td>
<td>2085</td>
</tr>
<tr>
<td>Disk volume mount point not found</td>
<td>2068</td>
</tr>
<tr>
<td>Disk volume mount point record insert failed</td>
<td>2069</td>
</tr>
<tr>
<td>Disk volume not found</td>
<td>2067</td>
</tr>
<tr>
<td>done</td>
<td>222</td>
</tr>
<tr>
<td>drive is already allocated</td>
<td>2004</td>
</tr>
<tr>
<td>drive is in a robotic library that is up</td>
<td>2036</td>
</tr>
<tr>
<td>drive is not allocated</td>
<td>2003</td>
</tr>
<tr>
<td>drive is not ready</td>
<td>2037</td>
</tr>
<tr>
<td>DSM has already mounted the volume</td>
<td>2077</td>
</tr>
<tr>
<td>DSM has detected that an invalid filesystem is mounted on the volume</td>
<td>2079</td>
</tr>
<tr>
<td>DSM returned an unexpected error</td>
<td>2076</td>
</tr>
<tr>
<td>duplicate backup images were found</td>
<td>642</td>
</tr>
<tr>
<td>duplicate MAP</td>
<td>346</td>
</tr>
<tr>
<td>duplicate reference string specified</td>
<td>813</td>
</tr>
<tr>
<td>EC_badop (there is no explanation for this status code)</td>
<td>113</td>
</tr>
<tr>
<td>EC_end (there is no explanation for this status code)</td>
<td>115</td>
</tr>
<tr>
<td>EC_error (there is no explanation for this status code)</td>
<td>114</td>
</tr>
<tr>
<td>eject process could not obtain information about the robot</td>
<td>295</td>
</tr>
<tr>
<td>eject process failed to start</td>
<td>292</td>
</tr>
<tr>
<td>eject process has already been run for the requested vault session</td>
<td>307</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>eject process has been aborted</td>
<td>293</td>
</tr>
<tr>
<td>eject process is complete</td>
<td>279</td>
</tr>
<tr>
<td>EMM database is inconsistent</td>
<td>2029</td>
</tr>
<tr>
<td>end point terminated with an error</td>
<td>610</td>
</tr>
<tr>
<td>error creating or getting message queue</td>
<td>209</td>
</tr>
<tr>
<td>error encountered attempting backup of catalog (multiple tape catalog backup)</td>
<td>302</td>
</tr>
<tr>
<td>error encountered executing Media Manager command</td>
<td>303</td>
</tr>
<tr>
<td>error getting information from EMM database</td>
<td>332</td>
</tr>
<tr>
<td>error getting information from media manager command line</td>
<td>333</td>
</tr>
<tr>
<td>error obtaining date of last backup for client</td>
<td>207</td>
</tr>
<tr>
<td>error occurred during initialization, check configuration file</td>
<td>103</td>
</tr>
<tr>
<td>error(s) occurred during vault report distribution</td>
<td>284</td>
</tr>
<tr>
<td>error receiving information on message queue</td>
<td>210</td>
</tr>
<tr>
<td>error record insert failed</td>
<td>2013</td>
</tr>
<tr>
<td>error requesting media (tpreq)</td>
<td>98</td>
</tr>
<tr>
<td>error sending information on message queue</td>
<td>212</td>
</tr>
<tr>
<td>error(s) occurred during vault report generation</td>
<td>283</td>
</tr>
<tr>
<td>Evaluation software has expired. See <a href="http://www.symantec.com">www.symantec.com</a> for ordering information</td>
<td>161</td>
</tr>
<tr>
<td>events out of sequence - image inconsistency</td>
<td>229</td>
</tr>
<tr>
<td>execution of a command in a forked process failed</td>
<td>623</td>
</tr>
<tr>
<td>execution of a vault notify script failed</td>
<td>272</td>
</tr>
<tr>
<td>execution of the specified system command returned a nonzero status</td>
<td>77</td>
</tr>
<tr>
<td>extent directive contained an unknown media id</td>
<td>644</td>
</tr>
<tr>
<td>failed accessing daemon lock file</td>
<td>158</td>
</tr>
</tbody>
</table>
### Table 5-1: NetBackup error messages and status codes (continued)

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code</th>
</tr>
</thead>
<tbody>
<tr>
<td>failed appending to container database</td>
<td>315</td>
</tr>
<tr>
<td>failed closing mail pipe</td>
<td>102</td>
</tr>
<tr>
<td>failed opening mail pipe</td>
<td>101</td>
</tr>
<tr>
<td>failed reading policy database information</td>
<td>218</td>
</tr>
<tr>
<td>failed reading global config database information</td>
<td>215</td>
</tr>
<tr>
<td>failed reading retention database information</td>
<td>216</td>
</tr>
<tr>
<td>failed reading storage unit database information</td>
<td>217</td>
</tr>
<tr>
<td>failed to communicate with resource broker</td>
<td>812</td>
</tr>
<tr>
<td>failed to communicate with resource requester</td>
<td>811</td>
</tr>
<tr>
<td>failed to get job data</td>
<td>257</td>
</tr>
<tr>
<td>failed to send signal</td>
<td>260</td>
</tr>
<tr>
<td>failed trying to allocate memory</td>
<td>36</td>
</tr>
<tr>
<td>failed trying to exec a command</td>
<td>29</td>
</tr>
<tr>
<td>failed trying to fork a process</td>
<td>28</td>
</tr>
<tr>
<td>failed waiting for child process</td>
<td>34</td>
</tr>
<tr>
<td>failed while trying to send mail</td>
<td>33</td>
</tr>
<tr>
<td>failure occurred while suspending media for eject</td>
<td>335</td>
</tr>
<tr>
<td>failure occurred while updating session information</td>
<td>336</td>
</tr>
<tr>
<td>failure occurred while updating the eject.mstr file</td>
<td>337</td>
</tr>
<tr>
<td>fatal NB media database error</td>
<td>91</td>
</tr>
<tr>
<td>Fibre Transport resources are not available</td>
<td>2075</td>
</tr>
<tr>
<td>File already exists: <em>file_name</em></td>
<td>510</td>
</tr>
<tr>
<td>file close failed</td>
<td>15</td>
</tr>
<tr>
<td>file does not exist</td>
<td>142</td>
</tr>
<tr>
<td>file open failed</td>
<td>12</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code</td>
</tr>
<tr>
<td>------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>file path specified is not absolute</td>
<td>141</td>
</tr>
<tr>
<td>file pathname exceeds the maximum length allowed</td>
<td>105</td>
</tr>
<tr>
<td>file read failed</td>
<td>13</td>
</tr>
<tr>
<td>file write failed</td>
<td>14</td>
</tr>
<tr>
<td>found no images or media matching the selection criteria</td>
<td>190</td>
</tr>
<tr>
<td>FT client devices are offline</td>
<td>2091</td>
</tr>
<tr>
<td>FT client has no devices configured</td>
<td>2090</td>
</tr>
<tr>
<td>FT client is not running</td>
<td>2089</td>
</tr>
<tr>
<td>FT server devices for client are offline</td>
<td>2092</td>
</tr>
<tr>
<td>getservbyname failed</td>
<td>19</td>
</tr>
<tr>
<td>handshaking failed with server backup restore manager</td>
<td>201</td>
</tr>
<tr>
<td>host is unreachable</td>
<td>47</td>
</tr>
<tr>
<td>image does not have a fragment map</td>
<td>663</td>
</tr>
<tr>
<td>inadequate buffer space</td>
<td>235</td>
</tr>
<tr>
<td>incorrect catalog backup policy</td>
<td>349</td>
</tr>
<tr>
<td>Incorrect password</td>
<td>504</td>
</tr>
<tr>
<td>Incorrect server platform identifier</td>
<td>162</td>
</tr>
<tr>
<td>incorrect vault catalog backup schedule</td>
<td>350</td>
</tr>
<tr>
<td>insufficient data received</td>
<td>628</td>
</tr>
<tr>
<td>insufficient disk space or high water mark would be exceeded</td>
<td>2030</td>
</tr>
<tr>
<td>internal error 615</td>
<td>615</td>
</tr>
<tr>
<td>internal error 616</td>
<td>616</td>
</tr>
<tr>
<td>internal error 618</td>
<td>618</td>
</tr>
<tr>
<td>internal error 619</td>
<td>619</td>
</tr>
<tr>
<td>internal error 620</td>
<td>620</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>internal error 654</td>
<td>654</td>
</tr>
<tr>
<td>Internal error - a bad status packet was returned by NB-Java application server that did not contain an exit status code</td>
<td>512</td>
</tr>
<tr>
<td>invalid arguments specified</td>
<td>638</td>
</tr>
<tr>
<td>invalid command parameter</td>
<td>20</td>
</tr>
<tr>
<td>invalid command protocol</td>
<td>143</td>
</tr>
<tr>
<td>invalid command usage</td>
<td>144</td>
</tr>
<tr>
<td>invalid container database entry</td>
<td>312</td>
</tr>
<tr>
<td>invalid container description</td>
<td>331</td>
</tr>
<tr>
<td>invalid container id</td>
<td>328</td>
</tr>
<tr>
<td>invalid database host</td>
<td>330</td>
</tr>
<tr>
<td>invalid data found in retention map file for duplication</td>
<td>324</td>
</tr>
<tr>
<td>invalid date specified</td>
<td>109</td>
</tr>
<tr>
<td>invalid date specified</td>
<td>109</td>
</tr>
<tr>
<td>invalid file pathname</td>
<td>104</td>
</tr>
<tr>
<td>invalid file pathname found, cannot process request</td>
<td>106</td>
</tr>
<tr>
<td>invalid filelist specification</td>
<td>69</td>
</tr>
<tr>
<td>invalid job id</td>
<td>273 and 805</td>
</tr>
<tr>
<td>invalid media type specified in the storage unit</td>
<td>640</td>
</tr>
<tr>
<td>Invalid NBJAVA_CLIENT_PORT_WINDOW configuration option value: (option_value)</td>
<td>519</td>
</tr>
<tr>
<td>Invalid operation on static mount point</td>
<td>2072</td>
</tr>
<tr>
<td>invalid recall status</td>
<td>329</td>
</tr>
<tr>
<td>invalid request</td>
<td>133</td>
</tr>
<tr>
<td>invalid STU identifier type</td>
<td>2002</td>
</tr>
<tr>
<td>invalid username</td>
<td>503</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>invalid value for NB-Java configuration option <em>(option_name)</em>: <em>(option_value)</em></td>
<td>520</td>
</tr>
<tr>
<td>Iron Mountain report is already created for this session</td>
<td>311</td>
</tr>
<tr>
<td>JM internal error</td>
<td>801</td>
</tr>
<tr>
<td>JM internal protocol error</td>
<td>802</td>
</tr>
<tr>
<td>JM terminating</td>
<td>803</td>
</tr>
<tr>
<td>job history indicates that no drive is available</td>
<td>2065</td>
</tr>
<tr>
<td>job history indicates that no media is available</td>
<td>2064</td>
</tr>
<tr>
<td>job type is invalid</td>
<td>2010</td>
</tr>
<tr>
<td>licensed use has been exceeded</td>
<td>159</td>
</tr>
<tr>
<td>logic error encountered</td>
<td>256</td>
</tr>
<tr>
<td>LTID needs to be restarted on media servers before the device can be used</td>
<td>2058</td>
</tr>
<tr>
<td>master server request failed</td>
<td>149</td>
</tr>
<tr>
<td>maximum job count has been reached for the storage unit</td>
<td>2040</td>
</tr>
<tr>
<td>Maximum number of mounts has been exceeded for tape media</td>
<td>2100</td>
</tr>
<tr>
<td>MDS has received an invalid message from a media server</td>
<td>2005</td>
</tr>
<tr>
<td>Media affinity group record insert failed</td>
<td>2084</td>
</tr>
<tr>
<td>Media allocation would exceed maximum partially full media limit</td>
<td>2087</td>
</tr>
<tr>
<td>media block size changed prior to resume</td>
<td>163</td>
</tr>
<tr>
<td>media close error</td>
<td>87</td>
</tr>
<tr>
<td>media has been misplaced</td>
<td>2033</td>
</tr>
<tr>
<td>media has conflicts in EMM</td>
<td>2012</td>
</tr>
<tr>
<td>media id is either expired or will exceed maximum mounts</td>
<td>169</td>
</tr>
<tr>
<td>media id is not in NetBackup volume pool</td>
<td>178</td>
</tr>
<tr>
<td>media id must be 6 or less characters</td>
<td>171</td>
</tr>
</tbody>
</table>
Table 5-1  NetBackup error messages and status codes (continued)

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code</th>
</tr>
</thead>
<tbody>
<tr>
<td>media id is not assigned to this host in the EMM database</td>
<td>95</td>
</tr>
<tr>
<td>media is assigned to another application</td>
<td>2044</td>
</tr>
<tr>
<td>media is assigned to another server</td>
<td>2016</td>
</tr>
<tr>
<td>media is expired</td>
<td>2015</td>
</tr>
<tr>
<td>media is in a drive that is currently in a DOWN state</td>
<td>2054</td>
</tr>
<tr>
<td>media is in a drive that is not configured on local system</td>
<td>2019</td>
</tr>
<tr>
<td>media is in an inaccessible drive</td>
<td>2053</td>
</tr>
<tr>
<td>media is in use according to EMM</td>
<td>2032</td>
</tr>
<tr>
<td>media is in use by the ACS robotic library</td>
<td>2048</td>
</tr>
<tr>
<td>media is not assigned</td>
<td>2014</td>
</tr>
<tr>
<td>media is not defined in EMM</td>
<td>2031</td>
</tr>
<tr>
<td>media is reserved</td>
<td>2028</td>
</tr>
<tr>
<td>media is unmountable</td>
<td>2046</td>
</tr>
<tr>
<td>media is write protected</td>
<td>2047</td>
</tr>
<tr>
<td>media loaded in drive is not write-enabled</td>
<td>2038</td>
</tr>
<tr>
<td>Media Manager device daemon (ltid) is not active</td>
<td>80</td>
</tr>
<tr>
<td>Media Manager volume daemon (vmd) is not active</td>
<td>81</td>
</tr>
<tr>
<td>media manager detected image that was not in tar format</td>
<td>92</td>
</tr>
<tr>
<td>media manager found wrong tape in drive</td>
<td>93</td>
</tr>
<tr>
<td>media manager killed by signal</td>
<td>82</td>
</tr>
<tr>
<td>media manager received no data for backup image</td>
<td>90</td>
</tr>
<tr>
<td>media manager - system error occurred</td>
<td>174</td>
</tr>
<tr>
<td>media needs to be rewound or unmounted from a drive</td>
<td>2060</td>
</tr>
<tr>
<td>media needs to be unmounted from a drive</td>
<td>2017</td>
</tr>
<tr>
<td>media not found in the ACS robotic library</td>
<td>2049</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>media open error</td>
<td>83</td>
</tr>
<tr>
<td>Media pool is not eligible for this job</td>
<td>2098</td>
</tr>
<tr>
<td>media position error</td>
<td>86</td>
</tr>
<tr>
<td>media read error</td>
<td>85</td>
</tr>
<tr>
<td>media server is not active</td>
<td>2027</td>
</tr>
<tr>
<td>Media server mismatch</td>
<td>2103</td>
</tr>
<tr>
<td>Media server not found in EMM database</td>
<td>2101</td>
</tr>
<tr>
<td>media write error</td>
<td>84</td>
</tr>
<tr>
<td>Member already exists in server group</td>
<td>409</td>
</tr>
<tr>
<td>Member’s NetBackup version not compatible with Server Group</td>
<td>407</td>
</tr>
<tr>
<td>Member’s server type not compatible with Server Group</td>
<td>405</td>
</tr>
<tr>
<td>multiple profiles exist</td>
<td>305</td>
</tr>
<tr>
<td>NB database backup failed, a path was not found or is inaccessible</td>
<td>124</td>
</tr>
<tr>
<td>NB database backup header is too large, too many paths specified</td>
<td>126</td>
</tr>
<tr>
<td>NB database recovery failed, a process has encountered an exceptional condition</td>
<td>128</td>
</tr>
<tr>
<td>NB image database contains no image fragments for requested backup id/copy number</td>
<td>165</td>
</tr>
<tr>
<td>NB-Java application server interface error: Java exception</td>
<td>511</td>
</tr>
<tr>
<td>NB-Java application server protocol error</td>
<td>523</td>
</tr>
<tr>
<td>NB-Java: bpjava-msvc is not compatible with this application version</td>
<td>514</td>
</tr>
<tr>
<td>(application_version). You may try login to a different NetBackup host or exit</td>
<td></td>
</tr>
<tr>
<td>the application. The remote NetBackup host will have to be configured with</td>
<td></td>
</tr>
<tr>
<td>the same version of NetBackup as the host you started the application on.</td>
<td></td>
</tr>
<tr>
<td>NB-Java Configuration file (file_name) does not exist</td>
<td>521</td>
</tr>
<tr>
<td>NB-Java Configuration file (file_name) is not readable due to the</td>
<td>522</td>
</tr>
<tr>
<td>following error: (message)</td>
<td></td>
</tr>
</tbody>
</table>
Table 5-1  NetBackup error messages and status codes *(continued)*

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code</th>
</tr>
</thead>
<tbody>
<tr>
<td>NDMP backup failure</td>
<td>99</td>
</tr>
<tr>
<td>NDMP credentials are not defined in EMM</td>
<td>2006</td>
</tr>
<tr>
<td>NDMP operation does not support multiple inline copies</td>
<td>2096</td>
</tr>
<tr>
<td>network connection broken</td>
<td>40</td>
</tr>
<tr>
<td>network connection timed out</td>
<td>41</td>
</tr>
<tr>
<td>network read failed</td>
<td>42</td>
</tr>
<tr>
<td>network write failed</td>
<td>44</td>
</tr>
<tr>
<td>no active policies contain schedules of the requested type for this client</td>
<td>198</td>
</tr>
<tr>
<td>no active policies in the configuration database are of the correct client type</td>
<td>246</td>
</tr>
<tr>
<td>No authorization entry exists in the auth.conf file for username <em>username</em> None of the NB-Java applications are available to you.</td>
<td>502</td>
</tr>
<tr>
<td>no BRMComm to join</td>
<td>823</td>
</tr>
<tr>
<td>no connection to reader</td>
<td>611</td>
</tr>
<tr>
<td>no drives are available for this job</td>
<td>2001</td>
</tr>
<tr>
<td>no drives available to start the reader process</td>
<td>617</td>
</tr>
<tr>
<td>no drives available to start the writer process</td>
<td>634</td>
</tr>
<tr>
<td>no entity was found</td>
<td>227</td>
</tr>
<tr>
<td>no files specified in the file list</td>
<td>112</td>
</tr>
<tr>
<td>No FT servers for this client are running</td>
<td>2093</td>
</tr>
<tr>
<td>no images duplicated</td>
<td>308</td>
</tr>
<tr>
<td>no images were found to synthesize</td>
<td>607</td>
</tr>
<tr>
<td>no images were successfully processed</td>
<td>191</td>
</tr>
<tr>
<td>no media ejected for the specified vault session</td>
<td>327</td>
</tr>
<tr>
<td>no media is defined for the requested NB database backup</td>
<td>121</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>no message was received from bptm</td>
<td>629</td>
</tr>
<tr>
<td>No ports available in range ((port_number)) through ((port_number)) per the NBJAVA_CLIENT_PORT_WINDOW configuration option</td>
<td>518</td>
</tr>
<tr>
<td>no profile was specified</td>
<td>274</td>
</tr>
<tr>
<td>no robot on which the media can be read</td>
<td>606</td>
</tr>
<tr>
<td>no schedules of the correct type exist in this policy</td>
<td>240</td>
</tr>
<tr>
<td>no storage units available for use</td>
<td>213</td>
</tr>
<tr>
<td>no target storage unit specified for the new job</td>
<td>604</td>
</tr>
<tr>
<td>no target storage unit was specified via command line</td>
<td>655</td>
</tr>
<tr>
<td>no vault session id was found</td>
<td>269</td>
</tr>
<tr>
<td>none of the files in the file list exist</td>
<td>71</td>
</tr>
<tr>
<td>none of the requested files were backed up</td>
<td>2</td>
</tr>
<tr>
<td>not all requested files were restored</td>
<td>175</td>
</tr>
<tr>
<td>number of cleanings is invalid</td>
<td>2018</td>
</tr>
<tr>
<td>number of media has exceeded the capacity of MAP</td>
<td>291</td>
</tr>
<tr>
<td>one or more errors detected during consolidated eject processing</td>
<td>290</td>
</tr>
<tr>
<td>operation not allowed during this time period</td>
<td>199</td>
</tr>
<tr>
<td>operation requested by an invalid server</td>
<td>37</td>
</tr>
<tr>
<td>operation would cause an illegal duplication</td>
<td>242</td>
</tr>
<tr>
<td>permission denied by client during rcmd</td>
<td>55</td>
</tr>
<tr>
<td>pipe close failed</td>
<td>18</td>
</tr>
<tr>
<td>pipe fgets call from bpcoord failed</td>
<td>668</td>
</tr>
<tr>
<td>premature eof encountered</td>
<td>233</td>
</tr>
<tr>
<td>problems encountered during setup of shared memory</td>
<td>89</td>
</tr>
<tr>
<td>process called but nothing to do</td>
<td>296</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>process was killed by a signal</td>
<td>63</td>
</tr>
<tr>
<td>profile already exists</td>
<td>345</td>
</tr>
<tr>
<td>query for list of component images failed</td>
<td>671</td>
</tr>
<tr>
<td>RB communication error</td>
<td>903</td>
</tr>
<tr>
<td>RB disk volume mount failed</td>
<td>912</td>
</tr>
<tr>
<td>RB disk volume mount must retry</td>
<td>915</td>
</tr>
<tr>
<td>RB internal error</td>
<td>901</td>
</tr>
<tr>
<td>RB invalid argument</td>
<td>902</td>
</tr>
<tr>
<td>RB max reallocation tries exceeded</td>
<td>904</td>
</tr>
<tr>
<td>RB media reservation not found</td>
<td>914</td>
</tr>
<tr>
<td>RB media server mismatch</td>
<td>905</td>
</tr>
<tr>
<td>RB operator denied mount request</td>
<td>906</td>
</tr>
<tr>
<td>RB user cancelled resource request</td>
<td>907</td>
</tr>
<tr>
<td>RB was reset</td>
<td>908</td>
</tr>
<tr>
<td>read from input socket failed</td>
<td>636</td>
</tr>
<tr>
<td>reader failed</td>
<td>609</td>
</tr>
<tr>
<td>received an error from bptm request to suspend media</td>
<td>631</td>
</tr>
<tr>
<td>received an error from bptm request to un-suspend media</td>
<td>632</td>
</tr>
<tr>
<td>received error notification for the job</td>
<td>605</td>
</tr>
<tr>
<td>report requested without eject being run</td>
<td>309</td>
</tr>
<tr>
<td>request attempted on a non reserved port</td>
<td>45</td>
</tr>
<tr>
<td>request needs to pend</td>
<td>2035</td>
</tr>
<tr>
<td>requested media id is in use, cannot process request</td>
<td>97</td>
</tr>
<tr>
<td>requested slot is empty</td>
<td>2043</td>
</tr>
<tr>
<td>Required drive or drive path is not configured</td>
<td>2099</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code</td>
</tr>
<tr>
<td>----------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>required or specified copy was not found</td>
<td>147</td>
</tr>
<tr>
<td>required value not set</td>
<td>152</td>
</tr>
<tr>
<td>resource request failed</td>
<td>800</td>
</tr>
<tr>
<td>resource request timed out</td>
<td>916</td>
</tr>
<tr>
<td>retry nbrb request later</td>
<td>900</td>
</tr>
<tr>
<td>Retry the allocation request later</td>
<td>2034</td>
</tr>
<tr>
<td>robot already exists</td>
<td>343</td>
</tr>
<tr>
<td>robotic library is down on server</td>
<td>2020</td>
</tr>
<tr>
<td>schedule windows overlap</td>
<td>231</td>
</tr>
<tr>
<td>scheduler found no backups due to run</td>
<td>200</td>
</tr>
<tr>
<td>SCSI reservation conflict detected</td>
<td>2039</td>
</tr>
<tr>
<td>send buffer is full</td>
<td>670</td>
</tr>
<tr>
<td>server backup restore manager’s network is unreachable</td>
<td>203</td>
</tr>
<tr>
<td>Server Group Active State is not valid</td>
<td>403</td>
</tr>
<tr>
<td>Server Group Already Exists</td>
<td>401</td>
</tr>
<tr>
<td>Server Group Already Exists with a different type</td>
<td>402</td>
</tr>
<tr>
<td>Server Group does not exist</td>
<td>404</td>
</tr>
<tr>
<td>Server Group is in use</td>
<td>408</td>
</tr>
<tr>
<td>Server Group Type is Invalid</td>
<td>400</td>
</tr>
<tr>
<td>server is not licensed for the Remote Client Option</td>
<td>2063</td>
</tr>
<tr>
<td>server is not the master server</td>
<td>153</td>
</tr>
<tr>
<td>server name not found in the bp.conf file</td>
<td>254</td>
</tr>
<tr>
<td>server not allowed access</td>
<td>46</td>
</tr>
<tr>
<td>SERVER was not specified in /usr/openv/netbackup/bp.conf</td>
<td>111</td>
</tr>
<tr>
<td>Session id assignment failed</td>
<td>263</td>
</tr>
</tbody>
</table>
Table 5-1  NetBackup error messages and status codes (continued)

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session id file is empty or corrupt</td>
<td>265</td>
</tr>
<tr>
<td>Snapshot error encountered</td>
<td>156</td>
</tr>
<tr>
<td>socket close failed</td>
<td>22</td>
</tr>
<tr>
<td>Socket connection to the NB-Java user service has been broken. Please retry your last operation. Check the log file for more details.</td>
<td>507</td>
</tr>
<tr>
<td>socket open failed</td>
<td>21</td>
</tr>
<tr>
<td>socket read failed</td>
<td>23</td>
</tr>
<tr>
<td>socket write failed</td>
<td>24</td>
</tr>
<tr>
<td>specified device path does not exist</td>
<td>122</td>
</tr>
<tr>
<td>specified disk path is not a directory</td>
<td>123</td>
</tr>
<tr>
<td>specified file contains no valid entry</td>
<td>326</td>
</tr>
<tr>
<td>specified media or path does not contain a valid NB database backup header</td>
<td>127</td>
</tr>
<tr>
<td>specified policy does not exist</td>
<td>639</td>
</tr>
<tr>
<td>specified profile not found</td>
<td>304</td>
</tr>
<tr>
<td>specified report does not exist</td>
<td>348</td>
</tr>
<tr>
<td>specified schedule was not found</td>
<td>640</td>
</tr>
<tr>
<td>storage unit characteristics mismatched to request</td>
<td>154</td>
</tr>
<tr>
<td>Storage Unit group does not exist in EMM configuration</td>
<td>2097</td>
</tr>
<tr>
<td>storage unit is disabled since max job count is less than 1</td>
<td>2045</td>
</tr>
<tr>
<td>Storage unit is down</td>
<td>2041</td>
</tr>
<tr>
<td>Storage unit is not compatible with requesting job</td>
<td>2007</td>
</tr>
<tr>
<td>storage unit query failed</td>
<td>608</td>
</tr>
<tr>
<td>Storage units are not available</td>
<td>2104</td>
</tr>
<tr>
<td>STU cannot run Lifecycle backups</td>
<td>2094</td>
</tr>
<tr>
<td>STU cannot run VMWare backup</td>
<td>2095</td>
</tr>
</tbody>
</table>
Table 5-1  NetBackup error messages and status codes (continued)

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code</th>
</tr>
</thead>
<tbody>
<tr>
<td>suspend requested by administrator</td>
<td>157</td>
</tr>
<tr>
<td>system call failed</td>
<td>11</td>
</tr>
<tr>
<td>system error occurred</td>
<td>130</td>
</tr>
<tr>
<td>system error occurred while processing user command</td>
<td>100</td>
</tr>
<tr>
<td>tar did not find all the files to be restored</td>
<td>185</td>
</tr>
<tr>
<td>tar had an unexpected error</td>
<td>184</td>
</tr>
<tr>
<td>tar received an invalid archive</td>
<td>183</td>
</tr>
<tr>
<td>tar received an invalid argument</td>
<td>181</td>
</tr>
<tr>
<td>tar received an invalid file name</td>
<td>182</td>
</tr>
<tr>
<td>tar received no data</td>
<td>186</td>
</tr>
<tr>
<td>tar was successful</td>
<td>180</td>
</tr>
<tr>
<td>termination requested by administrator</td>
<td>150</td>
</tr>
<tr>
<td>termination requested by bpcoord</td>
<td>665</td>
</tr>
<tr>
<td>text exceeded allowed length</td>
<td>225</td>
</tr>
<tr>
<td>the archive failed to back up the requested files</td>
<td>7</td>
</tr>
<tr>
<td>the backup failed to back up the requested files</td>
<td>6</td>
</tr>
<tr>
<td>the catalog image .f file has been archived</td>
<td>253</td>
</tr>
<tr>
<td>the client is not in the configuration</td>
<td>243</td>
</tr>
<tr>
<td>the client type is incorrect in the configuration database</td>
<td>72</td>
</tr>
<tr>
<td>the database contains conflicting or erroneous entries</td>
<td>238</td>
</tr>
<tr>
<td>The drive needs to be marked as available</td>
<td>2082</td>
</tr>
<tr>
<td>the entity already exists</td>
<td>226</td>
</tr>
<tr>
<td>the file list is incomplete</td>
<td>249</td>
</tr>
<tr>
<td>the file name used for the mount request already exists</td>
<td>2056</td>
</tr>
<tr>
<td>The host is not an active node of a cluster</td>
<td>2061</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>the image was not created with TIR information</td>
<td>250</td>
</tr>
<tr>
<td>the library is not ready to eject volumes</td>
<td>298</td>
</tr>
<tr>
<td>the machine specified is not a member of the server group specified</td>
<td>406</td>
</tr>
<tr>
<td>the maximum number of jobs per client is set to 0</td>
<td>194</td>
</tr>
<tr>
<td>The maximum number of mounts for the disk volume have been exceeded</td>
<td>2078</td>
</tr>
<tr>
<td>The media affinity group is not defined in EMM</td>
<td>2083</td>
</tr>
<tr>
<td>the media server reported a system error</td>
<td>2011</td>
</tr>
<tr>
<td>the requested operation was partially successful</td>
<td>1</td>
</tr>
<tr>
<td>the requested operation was successfully completed</td>
<td>0</td>
</tr>
<tr>
<td>the required storage unit is unavailable</td>
<td>219</td>
</tr>
<tr>
<td>the restore failed to recover the requested files</td>
<td>5</td>
</tr>
<tr>
<td>the robotic library is not available</td>
<td>2059</td>
</tr>
<tr>
<td>the scan host of the drive is not active</td>
<td>2057</td>
</tr>
<tr>
<td>the server is not allowed to write to the client’s filesystems</td>
<td>189</td>
</tr>
<tr>
<td>the specified container is not empty</td>
<td>320</td>
</tr>
<tr>
<td>the specified mount path will not fit in the allocated space</td>
<td>2070</td>
</tr>
<tr>
<td>the specified policy does not exist in the configuration database</td>
<td>230</td>
</tr>
<tr>
<td>the specified policy is not active</td>
<td>247</td>
</tr>
<tr>
<td>the specified policy is not of the correct client type</td>
<td>245</td>
</tr>
<tr>
<td>the specified client does not exist in an active policy within the configuration database</td>
<td>236</td>
</tr>
<tr>
<td>the specified client does not exist in the specified policy</td>
<td>239</td>
</tr>
<tr>
<td>the specified schedule does not exist in an active policy in the configuration database</td>
<td>237</td>
</tr>
<tr>
<td>the specified schedule does not exist in the specified policy</td>
<td>197</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>the specified schedule is the wrong type for this request</td>
<td>241</td>
</tr>
<tr>
<td>the TIR information is zero length</td>
<td>251</td>
</tr>
<tr>
<td>the vault session directory is either missing or inaccessible</td>
<td>268</td>
</tr>
<tr>
<td>there are no active policies in the configuration database</td>
<td>248</td>
</tr>
<tr>
<td>there are no volumes to eject</td>
<td>280</td>
</tr>
<tr>
<td>there is no available MAP for ejecting</td>
<td>299</td>
</tr>
<tr>
<td>there was a conflicting specification</td>
<td>224</td>
</tr>
<tr>
<td>third-party copy backup failure</td>
<td>170</td>
</tr>
<tr>
<td>this mpx group is unjoinable</td>
<td>806</td>
</tr>
<tr>
<td>throttled job count has been reached for the storage unit</td>
<td>2062</td>
</tr>
<tr>
<td>timed out connecting to client</td>
<td>54</td>
</tr>
<tr>
<td>timed out connecting to server backup restore manager</td>
<td>202</td>
</tr>
<tr>
<td>timed out waiting for database information</td>
<td>51</td>
</tr>
<tr>
<td>timed out waiting for media manager to mount volume</td>
<td>52</td>
</tr>
<tr>
<td>timed out waiting for the client backup to start</td>
<td>64</td>
</tr>
<tr>
<td>tir info was pruned from the image file</td>
<td>136</td>
</tr>
<tr>
<td>unable to accept connection from the reader</td>
<td>657</td>
</tr>
<tr>
<td>unable to accept connection from the writer</td>
<td>658</td>
</tr>
<tr>
<td>unable to allocate new media for backup, storage unit has none available</td>
<td>96 and 2000</td>
</tr>
<tr>
<td>unable to collect pre eject information from the API</td>
<td>278</td>
</tr>
<tr>
<td>unable to connect to bpcoord</td>
<td>621</td>
</tr>
<tr>
<td>unable to determine the status of rbak</td>
<td>8</td>
</tr>
<tr>
<td>unable to find any storage servers for the request</td>
<td>2071</td>
</tr>
<tr>
<td>unable to find policy/schedule for image using retention mapping</td>
<td>325</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>unable to get the address of the local listen socket</td>
<td>646</td>
</tr>
<tr>
<td>unable to issue the database query for policy</td>
<td>651</td>
</tr>
<tr>
<td>unable to issue the database query for policy information</td>
<td>652</td>
</tr>
<tr>
<td>unable to listen and register service via vnetd</td>
<td>633</td>
</tr>
<tr>
<td>unable to locate vault directory</td>
<td>285</td>
</tr>
<tr>
<td>unable to mount media because its in a DOWN drive or misplaced</td>
<td>164</td>
</tr>
<tr>
<td>unable to obtain process id, getpid failed</td>
<td>270</td>
</tr>
<tr>
<td>unable to open listen socket</td>
<td>601</td>
</tr>
<tr>
<td>unable to open pipe between bpsynth and bpcoord</td>
<td>667</td>
</tr>
<tr>
<td>unable to process request</td>
<td>228</td>
</tr>
<tr>
<td>unable to process request because the server resources are busy</td>
<td>134</td>
</tr>
<tr>
<td>unable to receive response from robot; robot not ready</td>
<td>334</td>
</tr>
<tr>
<td>unable to register handle with the reactor</td>
<td>635</td>
</tr>
<tr>
<td>unable to send a message to bpcoord</td>
<td>653</td>
</tr>
<tr>
<td>unable to send a message to the writer child process</td>
<td>659</td>
</tr>
<tr>
<td>unable to send a start command to a reader/writer process on media server</td>
<td>624</td>
</tr>
<tr>
<td>unable to send exit message to the BPXM reader</td>
<td>661</td>
</tr>
<tr>
<td>unable to send extent message to bpcoord</td>
<td>650</td>
</tr>
<tr>
<td>unable to send extent message to BPXM</td>
<td>648</td>
</tr>
<tr>
<td>unable to send start synth message to bpcoord</td>
<td>656</td>
</tr>
<tr>
<td>unable to start the writer on the media server</td>
<td>645</td>
</tr>
<tr>
<td>unexpected message received</td>
<td>43</td>
</tr>
<tr>
<td>unexpected message received from bpcoord</td>
<td>643</td>
</tr>
<tr>
<td>unexpected message received from bpsynth</td>
<td>627</td>
</tr>
</tbody>
</table>
### Table 5-1: NetBackup error messages and status codes (continued)

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code</th>
</tr>
</thead>
<tbody>
<tr>
<td>unexpected message received from BPXM</td>
<td>649</td>
</tr>
<tr>
<td>unexpected message was received from bptm</td>
<td>630</td>
</tr>
<tr>
<td>unimplemented error code</td>
<td>114</td>
</tr>
<tr>
<td>unimplemented feature</td>
<td>16</td>
</tr>
<tr>
<td>unknown image referenced in the SYNTH CONTEXT message from BPXM</td>
<td>662</td>
</tr>
<tr>
<td>unsupported image format for the requested database query</td>
<td>79</td>
</tr>
<tr>
<td>Updating of Media Manager database failed</td>
<td>310</td>
</tr>
<tr>
<td>user id was not superuser</td>
<td>140</td>
</tr>
<tr>
<td>user is not validated to use the server</td>
<td>132</td>
</tr>
<tr>
<td>valid archive image produced, but no files deleted due to non-fatal problems</td>
<td>3</td>
</tr>
<tr>
<td>validation of synthetic image failed</td>
<td>647</td>
</tr>
<tr>
<td>vault already exists</td>
<td>344</td>
</tr>
<tr>
<td>vault catalog backup failed</td>
<td>294</td>
</tr>
<tr>
<td>vault configuration cache not initialized</td>
<td>347</td>
</tr>
<tr>
<td>vault configuration file format error</td>
<td>339</td>
</tr>
<tr>
<td>vault configuration file not found</td>
<td>259</td>
</tr>
<tr>
<td>vault configuration serialization failed</td>
<td>341</td>
</tr>
<tr>
<td>vault configuration tag not found</td>
<td>340</td>
</tr>
<tr>
<td>vault core error</td>
<td>281</td>
</tr>
<tr>
<td>vault duplication partially succeeded</td>
<td>306</td>
</tr>
<tr>
<td>vault duplication was aborted by administrator request</td>
<td>258</td>
</tr>
<tr>
<td>vault eject failed</td>
<td>287</td>
</tr>
<tr>
<td>vault eject partially succeeded</td>
<td>288</td>
</tr>
<tr>
<td>vault eject timed out</td>
<td>338</td>
</tr>
</tbody>
</table>
### Table 5-1  
NetBackup error messages and status codes *(continued)*

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code</th>
</tr>
</thead>
<tbody>
<tr>
<td>vault internal error 261</td>
<td>261</td>
</tr>
<tr>
<td>vault internal error 262</td>
<td>262</td>
</tr>
<tr>
<td>vault internal error 286</td>
<td>286</td>
</tr>
<tr>
<td>vault XML version mismatch</td>
<td>271</td>
</tr>
<tr>
<td>vmchange api_eject command failed</td>
<td>301</td>
</tr>
<tr>
<td>vmchange eject verify not responding</td>
<td>300</td>
</tr>
<tr>
<td>VxSS access denied</td>
<td>117</td>
</tr>
<tr>
<td>VxSS authentication failed</td>
<td>116</td>
</tr>
<tr>
<td>VxSS authorization failed</td>
<td>118</td>
</tr>
<tr>
<td>VxSS authentication is requested but not allowed</td>
<td>193</td>
</tr>
<tr>
<td>VxSS authentication is required but not available</td>
<td>192</td>
</tr>
<tr>
<td>write on output socket failed</td>
<td>637</td>
</tr>
<tr>
<td>You are not authorized to use this application</td>
<td>501</td>
</tr>
<tr>
<td>zero extents in the synthetic image, cannot proceed</td>
<td>664</td>
</tr>
</tbody>
</table>
Media and device management status codes and messages

This chapter includes the following topics:

- About media and device management status codes and messages
- Media and device management messages

About media and device management status codes and messages

This chapter lists media and device management status codes and messages. In each of the following subsections, the status codes are listed in numerical order, with an explanation and a recommended action.

An alphabetical list of all media and device management messages is at the end of this chapter in "Messages." Following each message is a pointer to the section in this chapter that contains detailed information about the message.

The &CompanyName; technical support site has a wealth of information that can help you solve NetBackup problems.

Using debug logs

To solve many of the error conditions that this chapter describes, 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) and install_path\Volmgr\ (Windows).
3. Restart the daemons and services or run the command’s verbose option, if available.

The term media server, as distinct from master server or server, does not apply to the NetBackup Server product. In this case, the media server is the master server. When you troubleshoot a Server installation, ignore any references to media server. (This does not apply to NetBackup Enterprise Server.)

Media Manager status codes

These status codes appear in the following: exit status and command output for most media and device management commands, media and device management user interfaces, and system or debug logs.

Media Manager status code: 1

Message: request completed

Explanation: A requested operation was completed. The operation may have been one of several related operations for a particular task.

Recommended Action: None.

Media Manager status code: 2

Message: system error

Explanation: A system call failed. This status code is used for a generic system call failure that does not have its own status code.

- Check for other error messages in the command or the interface output to determine which system call failed.

See “Using debug logs” on page 422.
Check the system application log for error and warning messages.

Verify that the system is not running out of virtual memory. If virtual memory is the problem, shut down unused applications or increase the amount of virtual memory.

To increase virtual memory on Windows, do the following in the order presented:

- Display the Control Panel.
- Double-click System.
- On the Performance tab, set Virtual Memory to a higher value.

Verify that all product binaries are properly installed.

Verify that no unexpected media and device management processes are in operation by running vmps. Some processes are expected to continue running. Others that continue to run can indicate a more serious problem, such as a hung system call.

**Media Manager status code: 3**

**Message:** user id was not superuser

**Explanation:** A user or process that did not have root privileges (on UNIX and Linux) or administrator privileges (on Windows) started the process.

**Recommended Action:** If appropriate, give the user or the process administrator privileges (on Windows) or root privileges (on UNIX and Linux) and retry the operation.

**Media Manager status code: 4**

**Message:** invalid command usage

**Explanation:** A media and device management command was run with improper options, or an incompatibility between components or versions of the product exists.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Check the usage statement for expected usage and compare with the parameters being sent to start the new process.

- Verify that all media and device management binaries are at a compatible version level.
Media Manager status code: 5

**Message:** daemon resources are busy

**Explanation:** A requested operation cannot be processed because resources were busy.

**Recommended Action:** Check the status of any resources that the requested operation uses. On a robotic inventory request, verify that the inventory operation completes within a reasonable time.

Media Manager status code: 6

**Message:** invalid protocol request

**Explanation:** An invalid request was sent to a robotic process or operator request process.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Identify the target components (for example, vmd, nbemm, and robotic processes on local or remote hosts). Then verify that all media and device management binaries are at compatible version level.

Media Manager status code: 7

**Message:** daemon terminated

**Explanation:** The process is inactive or terminates (or has terminated) from the following: an event or signal or as a direct result of a request from an authorized user or process.

**Recommended Action:** If the targeted product component is needed but has terminated, restart the daemons or services on the targeted host.

Media Manager status code: 8

**Message:** invalid media ID

**Explanation:** When a process performed a media-related operation, it encountered an empty or an incorrectly formatted media identifier. Or a media ID that was passed to it cannot be operated on as requested.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Ensure that the media ID, where requested, is not blank.
Ensure that the specified media IDs contain valid characters only: alphanumeric characters, the period (.), the plus sign (+), and the underscore (_). A hyphen (-) is also a valid character when not the first character in the media ID.

- If media are specified to be ejected from a library, ensure the following: they exist in the EMM database and are associated with the correct robot number.
- Ensure that the media ID is from 1 to 6 characters in length.
- Ensure that a valid media and seed were specified.
- If the operation is an inventory request for an ACS robot, use the `robtest` utility to verify the following: the ACS interface returns cleaning media IDs both in the query volume list and in the query cleaning volume list.

**Media Manager status code: 9**

**Message:** invalid media type

**Explanation:** A process that performed a media-related operation encountered an unknown, missing, or incompatible media type specifier.

- If you run a robot inventory on a robot of type ACS, TLH, or TLM, ensure the following: the installed version of NetBackup supports and recognizes the vendor media type that the robot control software returns.
- If using a command line interface directly, verify that a valid media type has been passed, according to `vmadd(1m)` command line documentation.
- Ensure that an operation valid only for cleaning media has not been requested on a media ID that does not correspond to cleaning tape.
- Ensure that the media type in all bar code rules is a valid media type or the ordinal zero (0), to represent the default media type.

**Media Manager status code: 10**

**Message:** invalid barcode

**Explanation:** When a process performed a media-related operation, it encountered an unknown, missing, or incompatible bar code.

- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.
- Ensure that the bar code, where requested, is not blank.
- Ensure that the specified bar codes contain valid characters only: alphanumeric characters, and the period (.), plus sign (+), and underscore (_). A hyphen (-) is also a valid character when not the first character in the media ID.
Ensure that the number of characters in the bar code does not exceed the maximum that is allowed for the robot type.

Ensure that the bar code tag in all bar code rules is a subset of a valid, supported bar code format.

**Media Manager status code: 11**

**Message:** invalid description

**Explanation:** The volume description exceeds 25 ASCII characters in length, or contains unprintable characters.

**Recommended Action:** When you add or change a volume record or bar code rule record, ensure that the description field contains the following: no more than 25 ASCII characters that can be printed.

**Media Manager status code: 12**

**Message:** invalid robot type

**Explanation:** A requested operation encountered a case where a specified robot type or a volume’s robot type is different. It differs from the type of robot that is required to perform the operation in the current configuration.

Examine command output, debug logs, and system logs for a more detailed message on the error.

Specify a robot type that supports the volume’s media type.

Check the EMM database and ensure that the specified robot type agrees with the type for all volumes having the specified robot number.

If a robot type is required for the requested operation, ensure that a robot type has been specified.

**Media Manager status code: 13**

**Message:** invalid robot number

**Explanation:** The robot number was not specified or was not within the allowable range.

Specify a robot number in the range of 0 to 32767.

If you run `vmphyinv`, the global device database may not be updated, or the specified robot number may not be configured.
Media Manager status code: 14

Message: invalid robot host

A requested operation encountered a case where the following is true of the robot control host:

■ It is not specified.
■ It is not valid for the given robot type.
■ It is not in an acceptable format.
■ It exceeds the allowed length of a robot control host name.
■ Examine command output, debug logs, and system logs for a more detailed message on the error
  See “Using debug logs” on page 422.
■ If possible, attempt the requested operation again with another user interface that supports the type of request.

Media Manager status code: 15

Message: invalid volgroup

A requested operation encountered a case where the volume group:

■ Is not specified
■ Is not in an acceptable format
■ Exceeds the allowed length of a volume group name
■ Examine command output, debug logs, and system logs for a more detailed message on the error
  See “Using debug logs” on page 422.
■ Specify a volume group where one is required to ensure that it contains the following:
  ■ 25 ASCII characters or less
  ■ No white space
  ■ No unprintable characters

Media Manager status code: 16

Message: invalid robot coord1
**Explanation:** A requested operation encountered a missing or out-of-range robot slot number. Or a move by volume group residence was attempted when the volume did not originate from a valid robotic library slot.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Specify a slot number (robot coordinate 1) where required and ensure that the number is within the allowable range for the given robot type.

**Media Manager status code: 18**

**Message:** cannot allocate requested memory

**Explanation:** Allocation of system memory failed. This error occurs when insufficient system memory is available. The system may have too little physical and virtual memory to handle the current load of processes.

**Recommended Action:** Free up memory by terminating any unneeded processes that consume a lot of memory. Add more swap space or physical memory.

**Media Manager status code: 19**

**Message:** invalid database host

**Explanation:** A requested operation encountered a missing or an invalid database host. Or a request was sent to a host that is running a version of the product that does not support the requested operation.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Specify a valid EMM database host on which the following is running: a version of `nbemm` (the NetBackup Enterprise Media Manager) or an operator request daemon or process that supports the requested operation.

**Media Manager status code: 20**

**Message:** protocol error

**Explanation:** Message communications (handshaking) was not correct.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.
■ Retry the operation and examine the logs. Ensure that no whitespaces are embedded in the fields that do not allow embedded whitespace.

**Media Manager status code: 21**

**Message:** cannot obtain daemon lockfile

**Explanation:** vmd (NetBackup Volume Manager daemon on UNIX and Linux; NetBackup Volume Manager service on Windows) or operator request daemon or service cannot obtain an internal software lock.

**Recommended Action:** Check for the existence and permissions of the lock file itself and the lock file directory: /usr/openv/volmgr/misc/vmd.lock (UNIX and Linux) or \install_path\Volmgr\misc\vmd.lock (Windows). Create the directory or folder and adjust the permissions as needed so that vmd can obtain the lock: /usr/openv/volmgr/misc/vmd.lock (UNIX and Linux) or \install_path\Volmgr\misc\vmd.lock (Windows).

**Media Manager status code: 22**

**Message:** pool type change is not allowed for <CatalogBackup> pool

**Explanation:** An attempt was made to remove the catalog backup attribute of the default CatalogBackup pool.

**Recommended Action:** Verify that the appropriate pool name was used in this operation.

**Media Manager status code: 23**

**Message:** database server is down

**Explanation:** A request was made to the EMM server, but the underlying database server does not respond.

■ Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 422.

■ This error can occur if a cold catalog backup is in progress. Retry the request after this operation has completed.

**Media Manager status code: 25**

**Message:** failed making the database directory

**Explanation:** nbpushdata cannot create a working directory during upgrade.
**Recommended Action:** Determine why the directory `/usr/openv/tmp` (UNIX and Linux) or `install_path\tmp` (Windows) cannot be created. Check to see what account `nbpushdata` was run under. Compare it against the security properties of the database folder.

**Media Manager status code: 26**

**Message:** database open operation failed

**Explanation:** A database file cannot be opened.

**Recommended Action:**

Check for the existence and permissions of the following files in the `/usr/openv/var/global` directory (UNIX and Linux) or `install_path\NetBackup\var\global` folder (Windows):

- `external_robotics.txt`
- `external_densities.txt`
- `external_drivetypes.txt`
- `external_mediatypes.txt`

**Media Manager status code: 27**

**Message:** database read record operation failed

**Explanation:** `nbpushdata` encountered a read error while reading an EMM database record.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- The EMM database may be corrupted. Restore an older EMM database from a saved version or from catalog backups.

**Media Manager status code: 28**

**Message:** database read operation read too few bytes

**Explanation:** `nbpushdata` encountered a record that was smaller than expected while reading an EMM database record.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.
The EMM database may be corrupted. Restore an older EMM database from a saved version or from catalog backups.

**Media Manager status code: 32**

**Message:** database write record operation failed

**Explanation:** `nbpushdata` encountered an error while writing an EMM database record.

**Recommended Action:**
Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 422.

**Media Manager status code: 34**

**Message:** media ID not unique in database

**Explanation:** A volume entry being added to or changed in the EMM database had a media ID specified. The specified ID was a duplicate of the media ID for another volume already in the EMM database. All volumes in the EMM database must have a unique media ID.

- Examine the daemon and reqlib debug logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- When you add volumes to the EMM database, specify a media ID that is unique.
- If you run `vmphyinv`, there may be two or more media in the tape library with the same media ID.

**Media Manager status code: 35**

**Message:** volume does not exist in database

**Explanation:** A requested operation encountered a case where a volume query did not return a volume entry that matched the search criteria.

- Examine the daemon and reqlib debug logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Ensure that volumes are configured properly on the EMM server that matches the EMM server configured for the robot or set of stand-alone drives. Use `tpconfig -d` to list the configured EMM server.
Do the following so the volume query can find a matching volume: update the volume or the device configurations, specify the correct EMM server, modify volume properties, or adjust search criteria.

If you run `vmphyinv`, none of the media satisfy the search criterion. As such, `vmphyinv` cannot inventory the tape library.

**Media Manager status code: 36**

**Message:** barcode not unique in database

**Explanation:** A specified bar code in an added or a changed volume entry in the EMM database duplicated a volume bar code already in the database. All volumes in the EMM database must have a unique bar code.

Examine command output (if available) and the daemon and reqlib debug logs for a more detailed message on the error.
See “Using debug logs” on page 422.

Query or sort volume records by bar code to identify the volume entry with the duplicate bar code.

**Media Manager status code: 37**

**Message:** robotic volume position is already in use

**Explanation:** A robotic coordinate in an added or a changed volume entry in the EMM database duplicated a volume robotic coordinate in the database. (The robotic coordinate includes the slot number or the slot number and platter side.) All volumes in the EMM database must have unique robotic coordinates.

Examine command output (if available) and the daemon and reqlib debug logs for a more detailed message on the error.
See “Using debug logs” on page 422.

Query or sort volume records by slot number to identify the volume entry with the duplicate robotic coordinate.

Change (update or move volume) or delete the existing volume entry if it does not reflect the following: the correct robotic coordinate corresponding to the volume’s storage position in the robotic library. If a volume is currently in a drive, the EMM database should still reflect the volume’s home slot.

**Media Manager status code: 39**

**Message:** network protocol error

**Explanation:** An attempt to read data from a socket failed.
- Examine command output (if available) and the daemon and reqlib debug logs for a more detailed message on the protocol error. See “Using debug logs” on page 422.

- Verify that the server being connected to is operational.

**Media Manager status code: 40**

**Message:** unexpected data received

**Explanation:** Message communications (handshaking) was not correct.

- Verify that the correct version of software is running on all servers.

- Examine command output (if available) and the daemon and reqlib debug logs for a more detailed message on the protocol error. See “Using debug logs” on page 422.

- Retry the operation and examine the logs.

- Ensure that no embedded whitespaces exist in the fields that do not allow embedded whitespace.

**Media Manager status code: 41**

**Message:** invalid media ID for naming mode

**Explanation:** A request to add multiple volumes with a first media ID and a media ID style failed. It fails because the media ID specified was not compatible with the media ID naming style provided.

**Recommended Action:** Provide a first media ID that fits the selected style. For example, the media ID style is two characters and four digits. Then the least significant four characters in the first media ID must be digits in the range 0 to 9. Alternatively, select a media ID style that fits the specified first media ID.

**Media Manager status code: 42**

**Message:** cannot connect to robotic software daemon

**Explanation:** A connection to a robotic software daemon or process cannot be established. This error can occur when a process tries to connect to the robotic process that is not running. It can also occur if the network or server is heavily loaded and has slow response time.

- Examine command output (if available) and the daemon and reqlib debug logs for a more detailed message on the error. See “Using debug logs” on page 422.
 Identify the robotic process: look at the robot type and at the robot host on the robotic request or the robot host field of the volume being operated on.

 Verify that the robotic process to use for robotic control is available
 See Table B-2 on page 693.
 If necessary, start the robotic process.

 Ensure that only one configured robot control host exists for each TL8, TLD, and TLH robot. Also ensure that all volumes in the volume configuration have a robot host that matches the configured robot control host.

 Change the volumes or reconfigure the robot in the device configuration as needed.

 Check the system log on the robot control host to see if the robotic process processes requests when connections to it are attempted.

**Media Manager status code: 43**

**Message:** failed sending to robotic software daemon

**Explanation:** An attempt to write data to a robotic software daemon or process socket failed.

- Examine command output (if available) and the daemon and reqlib debug logs for a more detailed message error.
  See “Using debug logs” on page 422.

- Identify the robotic process: look at the robot type and at the robot host on the robotic request or the robot host field of the volume being operated on. Verify that the robotic process to use for robotic control is available and that it handles requests.

- Identify the robot control host by checking the device configuration. Only one configured robot control host should exist for each TL8, TLD, and TLH robot. All volumes in the volume configuration should have a robot host that matches the configured robot control host.

- Check the system log on the robot control host to see if the robotic process processes requests when communications with it are attempted.

**Media Manager status code: 44**

**Message:** failed receiving from robotic software daemon

**Explanation:** An attempt to read data from a robotic software daemon or process socket failed.

- Examine command output (if available) and the daemon and reqlib debug logs for a more detailed message on the error.
See “Using debug logs” on page 422.

- Identify the targeted robotic process: look at the robot type and at the robot host on the robotic request or the robot host field of the volume being operated on. Verify that the robotic process to use for robotic control is available and that it handles requests.
  See “Media and device management components” on page 691.

- Identify the robot control host by checking the device configuration. Only one configured robot control host should exist for each TL8, TLD, and TLH robot. All volumes in the volume configuration should have a robot host that matches the configured robot control host.

- Check the system log on the robot control host to see if the robotic process handles requests when communications with it are attempted.
  See “Resolving network communication problems” on page 40.

**Media Manager status code: 45**

**Message:** failed changing terminal characteristics

**Explanation:** When an attempt was made to change the mode for terminal input between cooked and raw, a system call failed.

**Recommended Action:** Examine the user interface output for the system error that is associated with the failed system call. Then troubleshoot according to operating system vendor recommendations.

**Media Manager status code: 46**

**Message:** unexpected data from robotic software daemon

**Explanation:** Message communications (handshaking) between a process and a robotic software daemon or process failed.

- Verify that the correct version of software is running on all servers.
- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Retry the operation and examine the logs.
- Ensure that no embedded whitespaces exist in the fields that do not allow embedded whitespace.
- Check the system log on the robot control host for errors that the robotic software logged.
Media Manager status code: 47
Message: no entries changed

Explanation: A requested operation was completed, but no changes to the volume configuration or Media Manager configuration file were made. The administrator may have terminated an operation instead of continuing with proposed changes. Or the configuration file may already include the configuration entry that was to be added.

- No action is needed if the administrator aborted the change operation.
- Examine command output (if available) and the daemon and reqlib debug logs for a more detailed message on the error. See “Using debug logs” on page 422.

Media Manager status code: 48
Message: no entries deleted

Explanation: A delete volume(s) operation completed. No changes were made to the volume configuration.

- No action is needed, unless the volumes that were requested to be deleted were not in fact deleted.
- Examine command output (if available) and the daemon and reqlib debug logs for a more detailed message on the error. See “Using debug logs” on page 422.

Media Manager status code: 49
Message: no entries inserted

Explanation: An insert volume(s) operation completed. No volumes were added to the volume configuration.

- No action is needed unless the volumes that were requested to be inserted were not inserted.
- Examine command output (if available) and the daemon and reqlib debug logs for a more detailed message on the error. See “Using debug logs” on page 422.

Media Manager status code: 50
Message: invalid change-entry request

Explanation: An invalid request to change volume information was sent to vmd on the EMM server.
Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.

Check the usage statement for expected usage and compare with the parameters being sent to start the new process.

**Media Manager status code: 51**

**Message:** cannot auto-eject this robot type

**Explanation:** A request to change volume residence with media eject was sent to vmd, but the volume’s robot type does not support automated media eject. (vmd is the NetBackup Volume Manager daemon on UNIX and Linux or NetBackup Volume Manager service on Windows.)

Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.

Ensure that change volume residence requests are not sent to vmd on a system that runs an older, incompatible software version level. (The change volume residence requests are requests with eject for the robot type that is involved with a newer release version level.)

**Media Manager status code: 52**

**Message:** cannot auto-inject this robot type

**Explanation:** A request to change volume residence with media inject was sent to vmd, but the volume’s robot type does not support automated media inject. (vmd is the NetBackup Volume Manager daemon on UNIX and Linux or NetBackup Volume Manager service on Windows.)

Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.

Ensure that change volume residence requests are not sent to vmd on a system that runs an older, incompatible software version level. (The change volume residence requests are requests with inject for the robot type that is involved with a newer release version level.)

**Media Manager status code: 53**

**Message:** invalid volume move mode
Explanation: A robotic-related request was made specifying a media movement option that not all affected software components supports.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Ensure that the robotic request is sent to a system that runs a release version of software that supports the particular request.

Media Manager status code: 54

Message: robot number and robot type mismatch

Explanation: A request was made to add or change volumes in the volume configuration. The robot number to be associated with a volume is already in use. It is associated with another volume in a robot with the same number but of another robot type.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Ensure that robot numbers are unique for each physical robot in the EMM database. Delete and re-add a robot. Use a unique robot number if duplicate robot numbers are in use. Use a media management interface to identify robot numbers currently in use for all volumes in the volume configuration. If you use a command line interface, specify the correct robot type for the robot number that is associated with the request.

Media Manager status code: 55

Message: robot number and volume group mismatch

Explanation: A request was made to add or change volumes in the volume configuration. The robot number and volume group that is associated with the volume configuration changes are in conflict with the requirements for volume groups. All volumes in a volume group are required to have the same residence, which includes having the same robot number.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Ensure that the specified robot number and volume group are compatible. If volumes in the volume group have a given robot number, then volumes with a different robot number cannot be added to that volume group. Volumes cannot be moved directly from one robotic volume group to another robotic
volume group. The intermediate steps (some volume entries are changed, some are not) would cause a conflict with robot numbers. Choose a different volume group on the request, or let the volume group be selected automatically. Volume group selection depends on the specific interface being used.

**Media Manager status code: 56**

**Message:** invalid database version header

**Explanation:** `nbpushdata` cannot find a recognizable EMM database version in the EMM database, and cannot initialize with the database currently in place.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- From catalog backups or another source if available, restore an earlier version of the database file: `/usr/openv/volmgr/database/volDB` (UNIX and Linux) or `install_path\Volmgr\database\volDB` (Windows). Then restart `vmd`.

**Media Manager status code: 57**

**Message:** error auto-generating volume group

**Explanation:** A request was made to add or change volumes in the volume configuration by using automatic generation of the volume group name. A unique volume group name cannot be generated because the available combinations were used up.

**Recommended Action:** Consolidate volumes into volume groups within the targeted robot number so that a new volume group can be generated automatically. Or provide a specific volume group name.

**Media Manager status code: 58**

**Message:** daemon cannot obtain socket

**Explanation:** `vmd` cannot bind to its socket. (`vmd` is the NetBackup Volume Manager daemon on UNIX and Linux and the NetBackup Volume Manager service on Windows.) When `vmd` attempts to bind to its configured port number, system call fails. The call fails usually because another process having acquired the port before the vmd daemon or service started.

- Examine the daemon debug log for a more detailed message on the system error.
If another process has the port, use other system commands to determine the process. Based on the result, either change the port number in your services file or map, or terminate the process that has acquired the port.

UNIX and Linux only: Another possible cause for this error is the use of the `kill` command to terminate `vmd`. To stop `vmd`, the recommended method is to use the **Terminate Media Manager Volume Daemon** option on the **Special actions** menu in `vmadm`. (Or use the equivalent command line request, `vmctrldbm -t`). The use of the `kill` command to stop this process can leave it unable to bind to its assigned port the next time it restarts. When the socket problem occurs, the daemon debug log contains lines similar to the following:

```
unable to obtain bound socket, Address already in use (125)
```

**Media Manager status code: 59**

**Message:** daemon failed accepting connection

**Explanation:** `vmd` cannot accept a new connection due to a system call failure. (`vmd` is the NetBackup Volume Manager daemon on UNIX and Linux and the NetBackup Volume Manager service on Windows.)

- Examine the daemon debug log for a more detailed message on the system error. Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “**Using debug logs**” on page 422.

- Obtain the specific system call failure from the debug log, and investigate the operating system functionality that is related to the failure.

**Media Manager status code: 60**

**Message:** cannot perform operation on this host

**Explanation:** A requested operation is not functional on a particular host.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “**Using debug logs**” on page 422.

- Robot inventory update must be initiated only on the host where the robotic control and drives are configured.

**Media Manager status code: 61**

**Message:** robot number and robot host mismatch
Explanation: A request is made to add or change volumes in the volume configuration, or to issue a robot inventory update request. A specified robot host differs from the robot host for other volumes in the same robot (defined as those volumes having the same robot number). All volumes in the EMM database that have a given robot number (for instance, 0) must have the same robot host name.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Specify the robot host in the device configuration to be the same case-sensitive host name on all hosts where the robot is configured. Re-issue the request. As an alternative, use move-by-volume group to move all volumes logically from a robotic volume group to stand-alone and then back into the robot. Specify the robot host as the host name that is used in the robot configuration. Then re-issue the request.

Media Manager status code: 62

Message: failed redirecting input to pipe

Explanation: A system pipe cannot be created.

Recommended Action: Check the interface output for the specific system error and investigate the operating system functionality that is related to the failure.

Media Manager status code: 63

Message: child process killed by signal

Explanation: An unexpected signal terminated a robot inventory update process.

- Examine interface output and debug logs for a more detailed message error. Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

Media Manager status code: 64

Message: no child process to wait for

Explanation: A media management interface attempted to wait for a child process to complete, but unexpectedly found that no such child process existed.

- Examine interface output and debug logs for a more detailed message error. Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
Retry the operation (or try to use a different media management interface) and examine the logs.

**Media Manager status code: 65**

**Message:** volume group does not exist

**Explanation:** During a request process, a volume group cannot be found within the existing volume entries in the EMM database.

1. Examine the daemon debug log for a more detailed message on the system error. Examine command output, debug logs, and system logs for a more detailed message on the error.

   See “Using debug logs” on page 422.

2. Check for data integrity or consistency problems in the EMM database by using a media management interface. Delete or move volume entries so that the volume group issues are corrected.

**Media Manager status code: 67**

**Message:** unable to send exit status

**Explanation:** vmd cannot send the status of a requested operation to the requestor. (vmd is the NetBackup Volume Manager daemon on UNIX and Linux and the NetBackup Volume Manager service on Windows.)

- Examine the daemon debug log for a more detailed message on the system error. Examine command output, debug logs, and system logs for a more detailed message on the error.

  See “Using debug logs” on page 422.

- Obtain the specific send or write system call failure from the debug log, and investigate the operating system functionality that is related to the failure.

- Use the following steps to check whether the command or the application interface that sends the request aborts prematurely: enable reqlib debug logs, retry the operation, check the debug logs, and observe application interface output.

**Media Manager status code: 68**

**Message:** too many volumes in volume group

**Explanation:** A request was made to add or change volumes in the volume configuration but the volume number was at its allowable limit. The limit is based on the number of volumes that is allowed in a particular type of robot.
- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.

- Check to see if volumes are defined in the EMM database. They may be defined in the EMM database, which is associated with a slot number zero that may not exist in the robot. Run a robot inventory Show contents of robot report and observe the starting slot number. If the starting slot number is one and a volume is defined in the robot at slot zero, delete the volume entry. Or move it to stand-alone so that the remaining available media slots can be used.

**Media Manager status code: 69**

**Message:** failed sending request to vmd

**Explanation:** A request cannot be sent to vmd or to oprd, even though the initial connection to the server process was successful. (vmd is the NetBackup Volume Manager daemon on UNIX and Linux or NetBackup Volume Manager service on Windows; oprd is the operator request daemon or process.)

- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.

- Check to see whether the vmd or the oprd process continues to run once it receives the connection from the requestor. Run `netstat -a` or an equivalent socket diagnostic utility. Check the following to see if the server process is hung up: the daemon debug log on the server-side system and the process status of vmd or oprd.

**Media Manager status code: 70**

**Message:** cannot connect to vmd [on host *host name*]

**Explanation:** A process times out while connecting to the following: vmd (the NetBackup Volume Manager daemon on UNIX and Linux or NetBackup Volume Manager service on Windows) or to oprd (the operator request daemon or process). This problem can occur when a connection is attempted and the server process is not running. It also can occur if the network or server is heavily loaded and has slow response time.

- On the host where vmd is the recipient of the connection, verify that the daemon or the service is running. (The host is the Media Manager host, the Device Host, or the EMM server.) If the daemon or the service is not running, start it. On Windows, vmd is the NetBackup Volume Manager service.
If `vmd` is already running, examine command output, debug logs, and system logs for a more detailed message on the error. See “*Using debug logs*” on page 422.

- Verify that the correct host names are defined in the configuration.

- Check the services file. On UNIX and Linux, verify that the `/etc/services` file (and NIS services if NIS is used) has entries for the `vmd` service. (Note that the `vmd` service always starts `oprd`.) On Windows, verify that the `%systemroot%\system32\drivers\etc\services` file has the correct entry for `vmd`. Also verify that the `vmd` port number in the services file agrees with the port number configuration. The port number is noted in the man page for `vmd(1M)`.

- Verify that all operating system patches or service packs are installed.

- Ensure that the Media Manager configuration is not tuned so that the load on `vmd` exceeds its ability to service requests. Look for entries in the `vm.conf` file that increase the load. Consider placing the EMM database on a higher performance server and file system if performance is an issue. To reduce the number of volumes in the volume configuration, use inventory filtering for the robot types that support it.

- Check utilities such as `ipcs -a` to ensure that shared memory functions properly. The `oprd` process may not respond because it cannot attach to shared memory.

**Media Manager status code: 71**

**Message:** failed sending to vmd

**Explanation:** An attempt to write data to a vmd socket failed. `vmd` is the NetBackup Volume Manager daemon (UNIX and Linux) or NetBackup Volume Manager service (Windows).

- Examine command output (if available) and the daemon and reqlib debug logs for a more detailed message on the error. See “*Using debug logs*” on page 422.

- Identify the system where `vmd` is running. The system usually is termed the Media Manager host or EMM server and defaults to the local system in some user interfaces (such as `vmadm`). Possible causes for the error are high network load, missing operating system patches or service packs, or unexpected `vmd` process failure.
Media Manager status code: 72

**Message:** failed receiving from vmd

**Explanation:** An attempt to read data from a vmd socket failed. vmd is the NetBackup Volume Manager daemon (UNIX and Linux) or NetBackup Volume Manager service (Windows).

- Examine command output (if available) and the daemon and reqlib debug logs for a more detailed message on the error. See “Using debug logs” on page 422.
- Identify the system where vmd is running. The system is usually termed the Media Manager host or EMM server and defaults to the local system in some user interfaces (such as vmadm). Possible causes for the error are high network load, missing operating system patches or service packs, or unexpected vmd process failure. Also, the socket read may have failed because the requested operation did not complete within a specified time period. The robotic process and vmd interactions can affect some requests to vmd; check the system log for errors on the robotic control host.

Media Manager status code: 73

**Message:** invalid query type

**Explanation:** An invalid volume query request was attempted.

- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.
- Verify that all Media Manager and user interface binaries are at a compatible version level.

Media Manager status code: 74

**Message:** invalid number of cleanings

**Explanation:** A request was made to change the number of cleanings that remains for one or more volumes in the volume configuration. When the request was made, the specified value was not within the acceptable range. The number of cleanings value may also be invalid in the number of mounts or cleanings field of a bar code rule.

- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.
Specify a number of cleanings value within the acceptable range of 0 to 2,147,483,647.

**Media Manager status code: 75**

**Message:** invalid change type  
**Explanation:** An invalid volume change request was attempted.

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
  See “Using debug logs” on page 422.
- Verify that all Media Manager and user interface binaries are at a compatible version level.

**Media Manager status code: 76**

**Message:** cannot get host name  
**Explanation:** The system call `gethostname(3C)` failed during an attempt to obtain the name of the local host.

- Examine command output, debug logs, and system logs for a more detailed message on the error.  
  See “Using debug logs” on page 422.
- Obtain the specific system call failure from the debug log, and investigate the operating system functionality that is related to the failure. Run the `hostname` system command to see if the command operates correctly.

**Media Manager status code: 78**

**Message:** barcode does not exist in database  
**Explanation:** A query volume by bar code request did not return a volume entry having the specified bar code, or bar code and media type.

- Examine the daemon and reqlib debug logs for a more detailed message on the error.  
  See “Using debug logs” on page 422.
- Ensure that volumes are properly configured in the EMM database. Use `tpconfig -d` to list the configured EMM server. Select the current server (the one being administered) to be the same as the host, which is the correct EMM server. Do the following so that the volume query can find a matching volume: update the volume or the device configurations, modify volume properties, or adjust search criteria as needed. For media in their correct slot locations, run the Rescan or the update bar code request so the following occurs: the bar code
field in the volume configuration matches the actual bar code as interpreted by the robotic library bar code reader.

**Media Manager status code: 79**

**Message:** specified robot is unknown to vmd

**Explanation:** A request was made to query volumes by residence. No volumes were found in the targeted volume configuration that matched the provided robot number, robot type, and robot host.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Ensure that volumes are properly configured in the EMM database. Use `tpconfig -d` to list the configured EMM server. Select the current server (the one being administered) to be the same as the host which is the correct EMM server. Perform the following so the volume residence query can find a matching volume: update the volume or the device configurations, modify volume properties, or adjust search criteria as needed.

**Media Manager status code: 80**

**Message:** cannot update database due to existing errors

`vmphyinv` is unable to update the EMM database because of the existing errors. The errors can be as follows:

- A Media Manager volume record belongs to a different robot with the same media ID as the media ID that the tape header read.

- The media type or media GUID or the volume pool of an assigned volume record needs to be changed.

- A bar code conflict is detected and `vmphyinv` needs to change the bar code of the existing volume record.

**Recommended Action:** `vmphyinv`, in such a scenario, generates a list of errors. Examine the output. You must resolve all these errors before you run the utility again.

**Media Manager status code: 81**

**Message:** robot type and volume group mismatch

**Explanation:** A request was made to add volumes or change volume residences in the volume configuration. The robot type and volume group that is associated with the volume configuration changes are in conflict with the requirements for
volume groups. All volumes in a volume group are required to have the same residence, which includes having the same robot type. A requested operation may have tried to associate the special No Volume Group name "---" with a robotic residence.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Ensure that the specified robot residence and volume group are compatible with other volumes in the volume configuration that are in the specified volume group. Do not move volumes in the special No Volume Group name "----" to a robotic residence without moving them to a new or auto-generated volume group. Choose a different volume group on the request, or let the volume group be automatically selected. Volume group selection depends on the specific interface being used.

**Media Manager status code: 82**

**Message:** robot host and volume group mismatch

**Explanation:** A request was made to add volumes or change volume residences in the volume configuration. The robot host and volume group that is associated with the volume configuration changes are in conflict with the requirements for volume groups. All volumes in a volume group are required to have the same residence. This residence includes having the same robot host, where robot host equivalence is defined as having the same case-sensitive robot host string.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Ensure that the specified robot residence and volume group are compatible with other volumes in the volume configuration that are in the specified volume group. Do not try to add volumes for a robot host by using a different form of the robot host name. For example, "acme" is not the same as "acme.symantec.com." Use the same host name that is used for other volumes in the volume group. If the robot host needs to be changed for volumes in a volume group, do the following: use a single move volume group request (available only in certain media management interfaces) to move the volume group to stand-alone residence. Then move the volume group back to the robotic residence. Specify the robot control host that you want to be associated with the new volume group.
Media Manager status code: 83

**Message:** device management error

**Explanation:** One of the device management errors occurs during the execution of `vmphyinv`.

**Recommended Action:**
Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 422.

Media Manager status code: 84

**Message:** this machine is not the database host

**Explanation:** A request was made to initiate `vmd` on a host other than the local host. `vmd` is the NetBackup Volume Manager daemon (UNIX and Linux) or NetBackup Volume Manager service (Windows).

`vmd` port numbers other than the default or use of unsupported options can affect the referenced host and port in the interfaces that start `vmd`.

- Initiate `vmd` on the local host only, by logging on to the host where `vmd` needs to run. Start `vmd` on that host. On UNIX and Linux, run `/usr/openv/volmgr/bin/vmd [-v]`. On Windows, start the NetBackup Volume Manager service in Services of the system Control Panel.

- If more information is needed to explain the problem, examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.

- Make sure port numbers are consistent.

Media Manager status code: 85

**Message:** volume daemon fork failed

**Explanation:** A Media Manager daemon or service cannot create a child process due to an error from the system. This error probably is intermittent, based on the availability of resources on the system.

- Restart the service at a later time and investigate the system problems that limit the number of processes.

- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.
Media Manager status code: 86
Message: failed opening tmp output file
Explanation: The vm.conf file or temporary working file cannot be opened.
Recommended Action: On UNIX and Linux, check for the existence and permissions of the /usr/openv/volmgr/misc directory, /tmp directory, and /usr/openv/volmgr/vm.conf file. On Windows: check for the existence and the security properties of the install_path\Volmgr\vm.conf file.

Media Manager status code: 87
Message: failed redirecting tmp output file
Explanation: The system call dup2(3C) failed during an attempt to direct interface output from a temporary file to the process’s standard output.
Recommended Action: Investigate the operating system functionality that is related to resource limits on the number of open files. Ensure that extraneous signals do not interrupt processes.

Media Manager status code: 88
Message: failed initiating child process
Explanation: A command cannot be ran. This error can occur due to the following: the command permissions do not allow it to be ran or system resources such as memory and swap space are insufficient.
- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Check the permissions on the vmcheckxxx, vmupdate, and oprd binaries, and (on Windows only) the rdevmi installed binary.

Media Manager status code: 89
Message: another daemon already exists
Explanation: vmd (the NetBackup Volume Manager daemon on UNIX and Linux or NetBackup Volume Manager service on Windows) tries to initialize and found that it was already running, according to the daemon or the service lock file.
Recommended Action: Check to see if vmd is already running. Do not try to start another vmd daemon or service until you first shut down the daemon or the service that is running. Stop the vmd that is running with vmctrldbm -t. On Windows, use the system Services interface. If the daemon or the service unexpectedly
terminated, remove the lock file. The lock file is /usr/openv/volmgr/misc/vmd.lock (UNIX and Linux) or install_path\Volmgr\misc\vmd.lock (Windows). Then restart vmd.

Media Manager status code: 90

**Message:** invalid volume pool

**Explanation:** A request was made to add volumes, change the volume pool for a volume, add a bar code rule, or change a bar code rule. However, the volume pool name or number that is associated with the requested change is in conflict with the requirements for volume pools.

These requirements are as follows:

- Volumes in scratch pools cannot be assigned until they are first moved to another pool.
- Volume pool numbers cannot be negative.
- Volume pool names must consist of from 1 to 20 printable ASCII characters with no embedded whitespace.
- The None volume pool is the only valid pool for the bar code rule entries that specify cleaning a media type.
- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Ensure that the specified volume pool does not violate the requirements noted.
  Use the vmpool command to display the pool information. Use the vmrule command to display the bar code rule information. Add or change volume pools and bar code rules as needed to rectify inconsistencies in cases where the databases are inconsistent or corrupted.

Media Manager status code: 92

**Message:** cannot delete assigned volume

**Explanation:** A delete request was made to a volume, and the volume is currently assigned.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Assigned volumes cannot be deleted. If no worthwhile data is on the volume, unassign the media by using the appropriate application interface (which is bpexpdate for NetBackup). Then retry the delete volume request.
Media Manager status code: 93

**Message:** volume is already assigned

**Explanation:** A request was made to assign a volume, and the volume was already assigned.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Do not try to manually assign any volumes that are already assigned, because it is not valid except for one condition: you can assign volumes for NetBackup catalog backups if the volume is already assigned for NetBackup catalog backups. Always use barcodes that are unique in the six least significant characters, across all media in all robots. Or use media ID generation rules to ensure that unique media IDs are generated in a robot inventory update.

Media Manager status code: 94

**Message:** volume is not in specified pool

**Explanation:** A request was made to assign a volume from a specified volume pool. The volume was in a different volume pool.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- When you assign volumes manually, specify the volume pool that is associated with the volume. Always use barcodes that are unique in the six least significant characters, across all media in all robots. Or use media ID generation rules to ensure that unique media IDs are generated in a robot inventory update.

Media Manager status code: 95

**Message:** media ID is not the specified media type

**Explanation:** A request was made to assign or add a volume of a specified media type. The volume or physically similar volumes have a different media type.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- When you use robot inventory update to make changes to the volume configuration, do the following: ensure that all volumes of the same physical cartridge type (for example, 3590J in TLH robots) map to a single media type
such as HCART. This check ensures that all media in the robotic library can be mounted on drives with a compatible drive type.

- When you assign volumes manually, specify the media type that is associated with the volume. Always use bar codes that are unique with respect to the six least significant characters, across all media in all robots. Or use media ID generation rules to ensure that unique media IDs are generated when you use robot inventory update.

**Media Manager status code: 96**

**Message:** oprd returned abnormal status

**Explanation:** A request that oprd services (the operator request daemon or process) returned an abnormal status.

- On Windows, do the following when you auto-configure devices or initiate the NetBackup Device Manager service from a graphical or a command line interface: ensure that the service is not disabled in the system services configuration.

- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.

- In general, any device management-related errors that occur on a particular host accompany operator request daemon or process and remote device management errors. Check for errors in the following: the debug and the system or the application logs on the host where oprd was started or where it is running. The host is often a targeted device host or scan host.

The kinds of failed requests that oprd services can include the following:

- Down, up, or reset drives
- Change drive comments
- Deny or resubmit mount requests
- Assign drives
- Start or stop ltid
- Obtain ltid status
- Display drive status
- Manage pending actions
- Set NDMP attributes
- Configure devices
- Clean drives
- Obtain host version and device configuration information
- Scan shared drives

**Media Manager status code: 97**

**Message:** rule does not exist in rule database

**Explanation:** A request was made to change or delete a bar code rule, but the bar code rule with the specified bar code tag cannot be found.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- List the configured bar code rules in the EMM database. Adjust the bar code tag that is specified on the change or the delete request or on the targeted host. Then the bar code rule is found when the request is retried.

**Media Manager status code: 101**

**Message:** media type and volume group mismatch

**Explanation:** A request was made to add volumes or change volume residences in the volume configuration. The media type and volume group that are associated with the volume configuration changes are in conflict with the requirements for volume groups. All volumes in a volume group are required to have the same residence, which includes having the same media type. Media types that are used for data and their associated cleaning media types are considered to be the same with regard to volume group restrictions.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Ensure that the specified media type and volume group are compatible with other volumes in the volume configuration that are in the specified volume group. Choose a different volume group on the request, or let the volume group be automatically selected. Volume group selection depends on the interface being used.

**Media Manager status code: 102**

**Message:** invalid pool database entry

**Explanation:** The volume pool database is corrupt. It contains some records that are not compatible with the installed product binaries.
Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.

Use `vmpool` to investigate the integrity of the volume pool database. The daemon debug log file should indicate the expected number of fields and the found number of fields in the pool record. Restore a saved version of the pool database if the pool database cannot be manually corrected.

**Media Manager status code: 104**

**Message:** failed appending to pool database

**Explanation:** A request was made to add, change, or delete a volume pool in the volume pool configuration. But the pool record cannot be appended to the volume pool database file.

Examine the daemon debug log for a more detailed message on the system error. See “Using debug logs” on page 422.

Examine the permissions and available file system space for writing to the database: on UNIX and Linux, `/usr/openv/volmgr/database/poolDB`; on Windows, `install_path\Volmgr\database\poolDB`.

**Media Manager status code: 105**

**Message:** poolname is not unique in pool database

**Explanation:** A request was made to add a volume pool in the volume pool configuration. The pool name specified is a duplicate of the name for an existing volume pool.

**Recommended Action:** On the add volume pool request, specify a volume pool name that is not already in use on the targeted EMM database host.

**Media Manager status code: 109**

**Message:** pool does not exist in pool database

A requested operation encountered a case where the specified volume pool was not found in the volume pool configuration. The requests that can return this error code are as follows:

- Add, change, delete, or query volume pool
- Add or change bar code rule
- Add or change volume
Query scratch volumes

Robot inventory report or update

Examine the daemon and reqlib debug logs for a more detailed message on the error.
See “Using debug logs” on page 422.

Ensure that volumes are properly configured on the EMM server. Use the `tpconfig -d` command to list the configured EMM server. Select the current server (the one being administered) to be the same as the host which is the correct EMM server for a targeted device.

Do the following so the requested operation can find the requested volume pool: update the volume or the device configurations, modify volume properties, or adjust search criteria as needed. Investigate inconsistencies between the EMM database and the volume pool database, and restore or correct those databases from a previous state as needed.

**Media Manager status code: 111**

**Message:** the specified pool is not empty

**Explanation:** A request was made to delete a volume pool. The pool was not empty, or it could not be determined whether or not volumes were still associated with the specified volume pool.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Use a media management interface to query for the volumes that are associated with the pool specified for deletion. Ensure that all volumes in a volume pool are associated again with another pool before trying to delete the volume pool. Use change volume operations to change the volume pool for a volume.

**Media Manager status code: 112**

**Message:** no pools in the pool list

**Explanation:** Unexpectedly, the volume pool list is empty.

**Recommended Action:** The volume pool list should contain a minimum of four pools: None, NetBackup, Catalog Backup, and DataStore. Investigate the integrity of the EMM database. Restore the EMM database from catalog backups.

**Media Manager status code: 113**

**Message:** invalid expiration date
Explanation: A request was made to change the media expiration for one or more volumes in the volume configuration, but the date specified was not valid.

Recommended Action:
When you change the media expiration, provide the date in the format that the media management interface documentation specifies.

Media Manager status code: 114
Message: invalid maximum mounts

Explanation: A request was made to change the limit for the number of times a volume can be mounted with write access for one or more volumes in the volume configuration. The specified value is not within the acceptable range. The maximum number of mounts value may also be invalid in the number of mounts or cleanings field of a bar code rule.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Specify a maximum mounts value within the range of 0 to 2,147,483,647.

Media Manager status code: 115
Message: volume has passed expiration date

Explanation: A request was made to assign a volume, and the volume expiration date has expired in relation to the current system date.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Extend the active life of the physical media: change the volume expiration date to a future date in relation to the current system date or time. Alternatively, replace the media with other media that still contains useful life. Check the system date and time and reset it as needed.

Media Manager status code: 116
Message: volume has exceeded maximum mounts

Explanation: A request was made to assign a volume. The volume’s number of mounts exceeds the maximum number of mounts allowed for the volume.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
See “Using debug logs” on page 422.

- Extend the active life of the physical media: increase the volume’s maximum number of mounts or set the maximum number of mounts to infinite. Alternatively, replace the media with other media that still contains useful life.

**Media Manager status code: 117**

**Message:** operation not allowed on cleaning cartridge

**Explanation:** A request was made to change a volume’s expiration or maximum number of mounts. The operation is not allowed because the volume is a cleaning cartridge.

- If the volume is a cleaning cartridge, perform a valid operation such as changing the number of cleanings that remain for the cleaning cartridge.

- If the volume’s media type cannot be determined, examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.

- If the targeted volume is incorrectly configured as a cleaning tape, delete the cleaning volume. Then update the volume configuration using options to define a new volume with the appropriate media type.

**Media Manager status code: 118**

**Message:** cannot delete one of the default volume pools

**Explanation:** An attempt was made to delete one of the special, pre-defined volume pools. The None, NetBackup, Catalog Backup, and DataStore volume pools are fixed volume pools in the volume pool configuration, and cannot be deleted.

**Recommended Action:** Do not attempt to delete the None, NetBackup, Catalog Backup, and DataStore volume pools.

**Media Manager status code: 119**

**Message:** invalid rule database entry

**Explanation:** The bar code rule database is corrupt. It contains some records that are not compatible with the installed product binaries.

- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.
Use `vmlrule` to investigate integrity of the bar code rule database. The daemon
debug log file should indicate the number of expected fields and the number
of found fields in the bar code rule record. Restore a saved version of the bar
code rule database if the bar code rule database cannot be manually corrected.

**Media Manager status code: 121**

**Message:** failed appending to rule database

**Explanation:** A request was made to add, change, or delete a bar code rule. A bar
code rule record cannot be appended to the bar code rule database file.

**Recommended Action:**

Examine the daemon debug log for a more detailed message on the system error.
See “Using debug logs” on page 422.

**Media Manager status code: 122**

**Message:** barcode tag is not unique in rule database

**Explanation:** A request was made to add a bar code rule. The specified bar code
tag was a duplicate of the tag for an existing bar code rule.

**Recommended Action:** On the add bar code rule request, specify a bar code tag
that is not already in use.

**Media Manager status code: 126**

**Message:** not authorized to connect to vmd

**Explanation:** A caller requesting services from vmd is either not authenticated
or not authorized. Or a problem is encountered when two systems attempt to
authenticate one another.

- See the *NetBackup Security and Encryption Guide* for information on vmd
  security.
  vmd security is based on NetBackup authentication or authorization, but has
  extensions for handling SERVER entries in the Media Manager configuration
  file.

- Examine the debug log files for a more detailed message on the authentication
  or the authorization problem.
  See “Using debug logs” on page 422.

- Correct the vmd security configuration by adjusting the authentication
  configuration, the AUTHORIZATION_REQUIRED entry, and SERVER entries.
If an authentication problem (rather than a configuration issue) is suspected, do the following:

- Ensure that the authentication libraries exist:
  Windows:
  
  ```
  \install_path\NetBackup\lib\libvopie.dll
  \install_path\NetBackup\lib\libvnoauth.dll
  ```

  UNIX and Linux (except HP-UX):
  
  ```
  /usr/openv/lib/libvopie.so
  /usr/openv/lib/libvnoauth.so
  ```

  UNIX and Linux (HP-UX only):
  
  ```
  /usr/openv/lib/libvopie.sl
  /usr/openv/lib/libvnoauth.sl
  ```

- Check the methods_allow.txt files on the systems that have problems to ensure that authentication is enabled. The files are in the following locations:
  Windows: \install_path\NetBackup\var\auth
  UNIX and Linux: /usr/openv/var/auth

- On the systems that have the authentication problem, remove the remote host that is not authenticated from the methods_allow.txt file.
  For example, if Host A and Host B have the problem, remove Host A from the file on Host B, and vice versa.
  Retry the operation.
  If the problem still exists, the connection problems are not related to authentication.
  If connections are successful, proceed to the next step.
  Run `bpauthsync -vopie` on the master server to synchronize the key files on the systems again.
  On Windows:
  
  ```
  \install_path\NetBackup\bin\admincmd\bpauthsync -vopie
  -servers
  ```

  On UNIX and Linux:
  
  ```
  /usr/openv/netbackup/bin/admincmd/bpauthsync -vopie -servers
  ```

- Add back the removed hosts and retry the operation.
Media Manager status code: 127

Message: unable to generate a unique media id

Explanation: A request was made to add volumes in the volume configuration by using robot inventory update or by using a media ID seed. A unique media ID was not generated because the "use seed" option was not specified, or because the available media ID combinations were used up.

Recommended Action: If you use robot inventory update, ensure that all media in the robotic library have readable bar code labels. Or request updates by using a seed to generate media IDs for non-barcoded media automatically. If volumes are added by specifying a seed, use a seed that allows media ID character combinations beyond those already in use. To identify the slot that is associated with the media that may not have a readable bar code, examine the command output.

Media Manager status code: 129

Message: invalid drive name

Explanation: A request was made to the EMM/DA for a shared drive, and the drive name was not recognized.

- Examine the daemon and reqlib debug logs for a more detailed message on the error. See “Using debug logs” on page 422.

- Ensure that the drive name is from 1 to 48 ASCII characters in length. The following special characters are allowed: period (.), plus (+), minus (-), and underscore (_).

- Verify that the correct version of software is running on all servers.

Media Manager status code: 130

Message: requested drive is already reserved

Explanation: A request was made to reserve a shared drive with the EMM/DA, and the drive was already reserved for another host.

This error is a normal occurrence when drive resources are oversubscribed for either of the following reasons:

- Independent schedulers or applications access the same pool of drives

- Hardware or media errors cause some drives that are allocated to jobs to become unavailable.
- Check the system log and application (bptm) debug log to determine if hardware or media errors have caused drives to become unavailable.

- If more information is needed on the drive reservation problem, examine the following for a more detailed message on the error: command output, debug logs, and system logs.
  See “Using debug logs” on page 422.

**Media Manager status code: 131**

**Message:** requested drive is not registered for host

**Explanation:** A request was made to reserve a shared drive with the EMM server. The requesting host did not register the drive, although that host had registered other drives.

This abnormal condition can occur in the following situation: two different hosts with the same name registered different drive lists with the EMM server and one of those hosts requested a drive reservation. (The same host name occurs when SSO_HOST_NAME entries in the `vm.conf` file override the local host name.)

**Recommended Action:** Use unique (non-duplicate) strings for host names and SSO_HOST_NAME configuration file entries.

**Media Manager status code: 132**

**Message:** requested drive is not currently registered

**Explanation:** A request was made to reserve or release a shared drive with the EMM server. The requesting host or any other host has not registered the drive.

**Recommended Action:** This condition is abnormal. It can occur in the following situation: the EMM server was stopped and restarted. This situation is automatically handled, because the requesting host re-registers its drives with the EMM server when this error is encountered.

**Media Manager status code: 133**

**Message:** requested drive is not reserved by host

**Explanation:** A request was made to release a shared drive with the EMM server. The requesting host did not reserve the drive, although it was reserved for another host.

This condition is abnormal. It can occur if a network problem or a suspended process exists. The following are possible scenarios:

- Host A reserves a shared drive.
Host A becomes unavailable for some time, unable to communicate with other hosts.

Host B determines that the host having the reservation (Host A) is no longer available. Host B then makes a request to the EMM/DA denoting Host A as unavailable.

Some other host (such as Host A or Host C) reserves the drive.

The host that originally owned the drive reservation tries to release the drive.

**Recommended Action:** Correct the network or the process problem that led to the communications problem. Ensure that unique non-duplicate strings are used for host names and for SSO_HOST_NAME configuration file entries.

**Media Manager status code: 134**

**Message:** requested drive is not currently reserved

**Explanation:** A request was made to the EMM/DA to release a shared drive, but none of the hosts reserved the drive.

This condition is abnormal. It can occur if there a network problem or a suspended process exists. The following are possible scenarios:

- Host A reserves a shared drive.
- Host A becomes unavailable for some time, unable to communicate with other hosts.
- Host B determines that the host having the reservation (Host A) is no longer available. Host B then makes a request to the EMM/DA denoting Host A as unavailable.
- The host that originally owned the drive reservation tries to release the drive.

**Recommended Action:** Correct the network or the process problem that led to the communications problem. Ensure that unique non-duplicate strings are used for host names and for SSO_HOST_NAME configuration file entries.

**Media Manager status code: 135**

**Message:** requested host is not currently registered

**Explanation:** A request was made to the EMM/DA to reserve or release a shared drive or designate a host as unavailable. The host (that reserved or released the drive or that was designated as unavailable) was not registered with the EMM/DA.

This condition is abnormal and can occur in the following situations.
■ The EMM server was stopped and restarted. This situation is automatically handled, because the requesting host re-registers its drives with the EMM server when this error is encountered.

■ A host was unregistered with the EMM server, and another host declared the host to be unavailable.

**Recommended Action:** If the host was declared unavailable, determine whether it should be available. Correct the underlying network problems or restart `ltid` (the device daemon on UNIX and Linux or NetBackup Device Manager service on Windows).

**Media Manager status code: 136**

**Message:** invalid host name

**Explanation:** A device host was added to the Media Manager configuration. Or a request was made to the EMM server and the host name exceeded the allowable length.

**Recommended Action:** Limit host names to 256 ASCII characters or less.

**Media Manager status code: 137**

**Message:** oprd request is not supported on the remote host

**Explanation:** An invalid request was sent to the operator request process.

■ Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

■ Identify the targeted host. Verify that all Media Manager binaries on that host are at a compatible version level with other hosts that are part of the configuration. Update the software version as needed.

**Media Manager status code: 138**

**Message:** media generation rule already exists

**Explanation:** You or a NetBackup media management interface attempted to add a MEDIA_ID_BARCODE_CHARS rule that already exists. The same rule cannot be added twice.

**Recommended Action:** Examine the listing of the MEDIA_ID_BARCODE_CHARS rules again.

A description of MEDIA_ID_BARCODE_CHARS rules is available.

See Reference Topics in the *NetBackup Administrator’s Guide, Volume II.*
Media Manager status code: 139
Message: media generation rule does not exist
Explanation: You or a NetBackup media management interface attempted to delete a MEDIA_ID_BARCODE_CHARS rule that does not exist.
Recommended Action: Examine a listing of the MEDIA_ID_BARCODE_CHARS rules again.
For a description of MEDIA_ID_BARCODE_CHARS rules, refer to Reference Topics in the NetBackup Administrator’s Guide, Volume II.

Media Manager status code: 140
Message: invalid media generation rule
Explanation: You or a NetBackup media management interface attempted to add an incorrect MEDIA_ID_BARCODE_CHARS rule.
Recommended Action: Ensure that the MEDIA_ID_BARCODE_CHARS rule is composed correctly.
For a description of MEDIA_ID_BARCODE_CHARS rules, refer to Reference Topics in the NetBackup Administrator’s Guide, Volume II.

Media Manager status code: 141
Message: invalid number of mounts
Explanation: A request was made to change the number of times that a volume was mounted, and the value specified was not within the acceptable range.
- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Specify a number of mounts value within the acceptable range of 0 to 2,147,483,647.

Media Manager status code: 142
Message: invalid offsite location
Explanation: The off-site location for a volume exceeds 25 ASCII characters in length, or contains unprintable characters.
Recommended Action: When you add or change a volume record, ensure the following: the off-site location field contains only printable characters and does not exceed 25 ASCII characters in length.
Media Manager status code: 143
Message: invalid offsite sent date
Explanation: A request was made to change the off-site sent date for one or more volumes in the volume configuration, but the date specified was invalid.
Recommended Action: When you change the off-site sent date, provide the date in the format that the Media Management interface documentation specified.

Media Manager status code: 144
Message: invalid offsite return date
Explanation: A request was made to change the off-site return date for one or more volumes in the volume configuration, but the date specified was invalid.
Recommended Action: When you change the off-site return date, provide the date in the format that the Media Management interface documentation specified.

Media Manager status code: 145
Message: requested drive is already reserved by host
Explanation: A request was made to the EMM/DA to reserve a shared drive. The drive was already reserved for the requesting host.
This condition is abnormal. It can occur if two different hosts with the same name registered the same drive name with the EMM/DA. (The same host name occurs when SSO_HOST_NAME entries in the vm.conf file override the local host name.) In this case, one of those hosts has a drive reservation, and the other host tries to reserve the same drive.
Recommended Action: Use unique non-duplicate strings for host names and for SSO_HOST_NAME configuration file entries.

Media Manager status code: 146
Message: incompatible database version
Explanation: A requesting process or vmd encountered an invalid or an unknown database or communications protocol. The possible data stores that an error affects are volume, volume pool, bar code rule, global device database, and shared drive information.
- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
Identify the target components (for example, vmd and daemons or services, or user interfaces on local or remote hosts). Verify that all Media Manager binaries are at a compatible version level. Depending on which requests encountered the invalid version, determine whether or not the database is corrupt. Use an appropriate interface to query for the type of information that is involved in the error condition.

**Media Manager status code: 147**

**Message:** invalid offsite slot

**Explanation:** A request was made to change the off-site slot location for a volume, and the value specified was not within the acceptable range.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Specify an off-site slot value within the range of 0 to 2,147,483,647.

**Media Manager status code: 148**

**Message:** invalid offsite session id

**Explanation:** A request was made to change the off-site session ID for a volume, and the value specified was not within the acceptable range.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Specify an off-site session ID within the range of 0 to 2,147,483,647.

**Media Manager status code: 149**

**Message:** current version does not support this configuration

**Explanation:** A request cannot be performed because it attempted to reference unlicensed functionality. An example request: the attempt to add a volume with a media type that is not valid for the licensed product.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- List the license keys that were installed and verify that the referenced functionality is supported with the currently installed license keys. Check to see that the databases that define externalized object types are in place and not corrupted. These database files are the following, in the
/usr/openv/var/global directory (UNIX and Linux) or \install_path\NetBackup\var\global folder (Windows):

- external_densities.txt
- external_drivetypes.txt
- external_mediatypes.txt
- external_robotics.txt

**Media Manager status code: 150**

**Message:** registering this host would exceed the maximum allowed

**Explanation:** The EMM/DA received a request to register shared drives from a host that was not currently registered. The maximum number of hosts that are registered with this EMM/DA were already reached. The current limit for the number of hosts that can register with the EMM/DA is 255.

- Restrict the size of the SSO configuration to no more than 255 hosts.
- Break up the media and the device management domain into multiple domains, with all domains having 255 or fewer hosts that register shared drives.

**Media Manager status code: 152**

**Message:** global device database record not found

**Explanation:** A request was made to update a global device database record, and the record specified was not found in the global device database. This condition can occur when a device configuration change is made after the global device database host has changed.

**Recommended Action:** If the request to update the record fails because the record does not exist, a request is made to add the missing record. No action is required.

**Media Manager status code: 153**

**Message:** device entry is not unique in global device database

**Explanation:** A request was made to add a global device database record, and the record specified was a duplicate of an existing record. This condition can occur if two processes update simultaneously the device configuration on the same host.

- Coordinate changes to the device configuration so that changes come from a single source.
- Investigate the global device database changes on the server (database) side by examining the daemon debug log file for a more detailed error message.
See “Using debug logs” on page 422.

**Media Manager status code: 155**

**Message:** global device database append operation failed

**Explanation:** A request was made to change the device configuration, and a global device database record cannot be written to the global device database file.

**Recommended Action:**
Examine the daemon debug log for a more detailed message on the error.
See “Using debug logs” on page 422.

**Media Manager status code: 160**

**Message:** the global device database device type is invalid

**Explanation:** An invalid device type appears in a request to modify the device configuration.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Identify the targeted host. Verify that all Media Manager binaries on that host are at a compatible version level with other hosts that are part of the configuration. Update the software version as needed.

**Media Manager status code: 162**

**Message:** the global device database device name is invalid

**Explanation:** An invalid or a missing device name was encountered in a request to modify the device configuration.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Identify the targeted host. Verify that all Media Manager binaries on that host are at a compatible version level with other hosts that are part of the configuration. Update the software version as needed.

**Media Manager status code: 163**

**Message:** the operation requested has failed

**Explanation:** The requested operation failed. The reason was not specified.
Recommended Action: This error code may appear for a number of reasons. Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 422.

**Media Manager status code: 164**

**Message:** the robotic daemon returned an invalid volume GUID

**Explanation:** An invalid RSM GUID was returned from the RSM API. (RSM is the Microsoft Removable Storage Manager. GUID is a Global Unique Identifier.)

- Examine the system’s application log, the Removable Storage system interface, and the daemon and reqlib debug logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Retry the operation and examine the logs. From the daemon debug log file, determine the media ID that has the invalid RSM GUID.

- Make sure that the software components are compatible.

**Media Manager status code: 165**

**Message:** Evaluation period expired. Go to www.symantec.com to order this product.

**Explanation:** The NetBackup evaluation software has expired.

See the address in the message or www.symantec.com/enterprise/ for ordering information.

**Recommended Action:** Obtain a licensed copy of NetBackup.

**Media Manager status code: 166**

**Message:** media access port not available

**Explanation:** A request was made to physically move a volume into or out of a robotic library, but the media access port was unavailable.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Ensure that the move request was not sent to a robotic control daemon or process on a system that runs an older, incompatible software version.

- Ensure that the targeted robotic control daemon or process operates normally.
Media Manager status code: 167

**Message:** ADAMM GUID is not unique in the database

**Explanation:** A volume entry that was added to or changed in the EMM database had a specified ADAMM GUID. It was a duplicate of the ADAMM GUID for another volume already in the EMM database. All volumes in the EMM database must have an ADAMM GUID that is either unique or null. (ADAMM is Advanced Device and Media Management, and a GUID is a Global Unique Identifier.)

- Examine command output (if available) and the daemon and reqlib debug logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- From the daemon debug log file, determine the volume that has an ADAMM GUID conflict with the volume entry that is added or changed.

Media Manager status code: 168

**Message:** ADAMM GUID does not exist in database

**Explanation:** The EMM database was queried for a specified ADAMM (Advanced Device and Media Management) GUID, and no volumes were found matching the specified criteria. (The GUID is a Global Unique Identifier.)

**Recommended Action:**

Run `vmphyinv` for the media whose ADAMM GUID does not exist in the database.

Media Manager status code: 169

**Message:** internal database access failure

**Explanation:** During an update of a drive status from a pre-6.0 NetBackup server in EMM, a problem occurred.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Run the `tpconfig -d` or `vmquery -a` command to verify that the EMM server is actively running and that it accepts new connections.

Media Manager status code: 171

**Message:** a scratch pool is already defined

**Explanation:** A new scratch pool cannot be defined because another scratch pool already exists.
Recommended Action:
Use the scratch pool already defined, or delete the current scratch pool and create a new scratch pool.

Media Manager status code: 172
Message: pool not defined as a scratch pool
Explanation: You or a NetBackup media management interface have tried to delete (unset) a scratch pool that is not defined as a scratch pool.
Recommended Action: To delete the scratch pool, use the vmpool command.
Make sure that the name of the pool that is specified with the unset_scratch option is the correct name of the scratch pool.

Media Manager status code: 173
Message: invalid scratch pool name
Explanation: You, or a NetBackup media management interface have tried to specify the NetBackup, DataStore, or None pool as a scratch pool. The NetBackup, DataStore, and None pools cannot be specified as scratch pools.
Recommended Action: Create a scratch pool with a different name.

Media Manager status code: 175
Message: unable to open the device test state file
Explanation: The process is not able to open the state file, mostly likely because another process locked it.
Recommended Action:
Try again to open the state file. If you cannot open the state file, you may have to remove the file, which would result in a loss of previous test runs.

Media Manager status code: 176
Message: unable to find any records in the device test database
Explanation: The state file exists, but it is empty. This error indicates that no previous test runs have occurred.
Recommended Action: None required.
Media Manager status code: 177

**Message:** request can only be performed on the Media and Device Management Domain Server

**Explanation:** The host this request was performed on is blocked from being a database host. An administrator blocked the host to restrict which hosts are allowed to be EMM servers.

- Verify that you specified the correct EMM server (the -h option on the command line). If you did not specify the database host, the command line defaults to the local host, while the console uses the currently administered host.

- Contact the administrator in charge of this configuration and verify that the host was intentionally blocked from being a database host. If not, remove the NOT_DATABASE_HOST flag in the host's `vm.conf` file. To do so without having to stop and restart the daemons, use:

  ```
  vmquery -h <hostname> -remove_not_db_host.
  ```

  To add this entry to a host without having to stop and restart the daemons, use:

  ```
  vmquery -h <hostname> -add_not_db_host.
  ```

Media Manager status code: 181

**Message:** not authorized to connect to robotic daemon

**Explanation:** A caller requesting services from a robotic daemon is not authenticated or authorized. Or when two systems try to authenticate one another, a problem occurs.

- See the *NetBackup Security and Encryption Guide* for information on Media Manager security.
  Media Manager security is based on NetBackup authentication and authorization, but has extensions for handling SERVER entries in the Media Manager configuration file.

- Examine the debug log files for a more detailed message on the authentication and authorization problem.
  See “Using debug logs” on page 422.

- Determine whether authorization fails on `vmd`. Examine the debug log files for Media Manager status code 126 occurrences ("not authorized to connect to `vmd".

- Correct the Media Manager security configuration by adjusting the authentication configuration, the AUTHORIZATION_REQUIRED entry, the ENABLE_ROBOT_AUTH entry, and the SERVER entries.
If an authentication problem (rather than a configuration issue) is suspected, do the following:

- Ensure that the authentication libraries exist:
  - **Windows:**
    
    - `install_path\NetBackup\lib\libvopie.dll`
    - `install_path\NetBackup\lib\libvnoauth.dll`
  
  - **UNIX and Linux (except HP-UX):**
    
    - `/usr/openv/lib/libvopie.so`
    - `/usr/openv/lib/libvnoauth.so`
  
  - **UNIX and Linux (HP-UX only):**
    
    - `/usr/openv/lib/libvopie.sl`
    - `/usr/openv/lib/libvnoauth.sl`

- Check the `methods_allow.txt` files on the systems that have problems to ensure that authentication is enabled. The files are in the following locations:
  - **Windows:** `install_path\NetBackup\var\auth`
  - **UNIX and Linux:** `/usr/openv/var/auth`

- On the systems that have the authentication problem, remove the remote host that is not authenticated from the `methods_allow.txt` file and retry the operation.
  
  For example, if Host A and Host B have the problem, remove Host A from the file on Host B, and vice versa.
  
  If the problem still exists, the error is caused by connection problems not related to authentication.
  
  If connections are successful after you remove the host, run `bpauthsync -vopie` on the master server to synchronize the key files on the systems again.
  
  - **On Windows:**
    
    - `install_path\NetBackup\bin\admincmd\bpauthsync -vopie -servers`
  
  - **On UNIX and Linux:**
    
    - `/usr/openv/netbackup/bin/admincmd/bpauthsync -vopie -servers`

  Add the removed names and retry the operation.
**Media Manager status code: 182**

**Message:** device test state file does not exist

**Explanation:** The state file does not exist. The reason may be because no tests have been run yet.

**Recommended Action:** If the state file is lost, any previous test runs are also lost. The recommended action is to start again.

---

**Media Manager status code: 185**

**Message:** the robotic library is full and may still have media in its map

**Explanation:** During a robot inventory update, the user attempted to use the empty_map option. The MAP contained more media than the library had space for. In this case, the inventory update was successful, the empty_map part was only partially successful. Those media still in the MAP are not changed or added in the EMM database.

**Recommended Action:** No action is necessary on the user’s part except to be aware that not all of the media was removed from the MAP and placed into the library.

---

**Media Manager status code: 186**

**Message:** invalid container id

**Explanation:** A NetBackup Vault container ID was used with an invalid character.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  - See “Using debug logs” on page 422.
- Retry the operation with a container ID that does not contain invalid characters.

---

**Media Manager status code: 187**

**Message:** VxSS authentication failed

**Explanation:** The parties on either end of a socket connection cannot mutually authenticate each other.

- Ensure that the Symantec Product Authentication Service is installed and configured.
  - For complete installation instructions, see the *NetBackup Security and Encryption Guide*.
- Check that both parties have a valid certificate by examining the listed expiry date from a `bpnbat -WhoAmI`. For example:
bnpbat -WhoAmI
Name: JDOG
Domain: MYCOMPANY
Issued by: /CN=broker/OU=root@machine1.mycompany.com/O=vx
Expiry Date: Sep 19 12:51:55 2009 GMT
Authentication method: Microsoft Windows
Operation completed successfully.

- Shows an expiry date of September 19th, 2009. After 12:51:55 GMT this credential is no longer valid and a new credential is required.

- If you are running from the NetBackup Administration console, close and reopen the console. The console automatically obtains a credential for the currently logged in identity, if possible. By default these certificates are valid for 24 hours. To set a longer default time, consult the following:
  See the NetBackup Security and Encryption Guide.

- Ensure that the certificates for both sides either use the same broker, are children of the same root broker, or have trusts established between them. More information is available on broker hierarchies and how to establish trust relationships between brokers.
  See the NetBackup Security and Encryption Guide.

- Ensure that connectivity is possible between the physical systems in question. If general sockets cannot connect between the machines (such as ping and telnet), network issues unrelated to NetBackup may be the cause of this problem.

- Ensure that the system has sufficient swap space and the following directories are not full:
  - /home/username
  - /user/openv/netbackup/logs
  - /tmp

Media Manager status code: 188

Message: VxSS Access Denied

Explanation: The user identity that is used to attempt an operation does not have the permissions needed to perform the action.

- If you use the default groups, make certain that the user attempts to perform an operation appropriate for that group. For example, a member of NBU_Operators is unable to modify policy information, a permission reserved for administrator roles.
Ensure that the system has sufficient swap space and the following directories are not full:

- /home/username
- /user/openv/netbackup/logs
- /tmp

If you use your own defined groups and permissions, first determine the object with which the operation is associated. Then add the permissions relative to the action. For example, a user is required to up and down drives but does not currently have permission to do so. Verify that the user belongs to the correct authorization group.

If necessary, verify that the group has Up and Down permissions on the Drive object within the Group Permission tab. If necessary, you can increase the verbosity level of NetBackup to locate what object and what permissions are required for the failing request. The pertinent lines in the debug logs look similar to the following:

```
Name: JMIZZLE
Domain: MYCOMPANY
Expiry: Sep 24 21:45:32 2003 GMT
Issued by: /CN=broker/OU=root@machine1.mycompany.com/O=vx
  AuthType: 1
17:19:37.077 [904.872] <2> VssAzAuthorize: vss_az.cpp.5082:
  Function: VssAzAuthorize. Object
  NBU_RES_Drives
17:19:37.077 [904.872] <2> VssAzAuthorize: vss_az.cpp.5083:
  Function: VssAzAuthorize. Permissions Up
17:19:40.171 [904.872] <2> VssAzAuthorize: vss_az.cpp.5166:
  Function: VssAzAuthorize. 20 Permission denied.
```

In the example, the user JMIZZLE attempts to perform an operation that requires the Up permission on the Drives object. To diagnose the problem, examine the group(s) to which the user belongs to ensure that the appropriate group includes the Up permission. (Up is a member of the Operate permission set for Drives.)

**Media Manager status code: 189**

**Message:** failed to initialize a connection to the Enterprise Media Manager

**Explanation:** A request to initialize a connection with the EMM server failed or was already initialized.
- Verify that `pbx_exchange` and `nbemm` are running.
- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.
- Run the `tpconfig -d` or `vmquery -a` command to verify that the EMM server is actively running and that it accepts new connections.

### Media Manager status code: 190

**Message:** the request sent to the Device Allocator has failed

**Explanation:** A request to reserve or release a drive with the DA (EMM server) failed.

- Verify that `pbx_exchange` and `nbemm` are running.
- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.
- Run the `tpconfig -d` or `vmquery -a` command to verify that the EMM server is actively running and that it accepts new connections.
- For a DA reserve drive request, verify that another host had not already reserved the drive.
- For a DA release drive request, verify the following: that the drive is DA reserved by the host requesting the DA release and has not already been released.

### Media Manager status code: 191

**Message:** invalid EMM argument

**Explanation:** An invalid argument was provided on a call to the EMM server.

**Recommended Action:** Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.

### Media Manager status code: 192

**Message:** unknown EMM error code

**Explanation:** An unknown error was returned from the EMM server.

**Recommended Action:** Examine command output, debug logs, and system logs for a more detailed message on the error.
Media and device management status codes and messages

About media and device management status codes and messages

See “Using debug logs” on page 422.

Media Manager status code: 193

Message: generic EMM SQL error
Explanation: The EMM server received an error from the underlying database.
Recommended Action:
Examine command output, debug logs, and system logs for a more detailed message on the error.
See “Using debug logs” on page 422.

Media Manager status code: 194

Message: EMM DB record not found
Explanation: During a NetBackup upgrade a pre-requisite host was not upgraded in the correct order.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Verify that the proper upgrade order is followed as described in the NetBackup Installation Guide.

Media Manager status code: 195

Message: CORBA communication error
Explanation: While trying to communicate with the EMM server, a problem occurred.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Verify that &CompanyName; Private Branch Exchange (VxPBX) processes new requests.
- Verify that the EMM server processes new requests.

Media Manager status code: 196

Message: EMM database error
Explanation: The calling program does not recognize the error the EMM server returned.
Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.

Verify that the EMM server processes new requests.

**Media Manager status code: 198**

**Message:** pool not defined as a catalog backup pool

**Explanation:** An attempt was made to remove the Catalog Backup attribute from a pool in which it was not set.

**Recommended Action:** Verify that the appropriate pool name was used in this operation.

**Media Manager status code: 199**

**Message:** the media is allocated for use

**Explanation:** A request was made to modify a media that was in use.

Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.

Retry the operation once the media is no longer in use.

**Device configuration status codes**

Device configuration status codes appear in exit status and command output for the `tpconfig` and the `tpautoconf` commands, and in system or debug logs. Programs that call `tpconfig` and `tpautoconf`, such as media and device management user interfaces and the `vmoconfig` command, also present these codes.

**Device configuration status code: 0**

**Message:** Success

**Explanation:** A requested operation was successfully completed.

**Recommended Action:** None.

**Device configuration status code: 1**

**Message:** Cannot execute command, permission denied
**Explanation:** A user or process that did not have root privileges (on UNIX and Linux) or administrator privileges (on Windows) started the process. Or the EMM server name cannot be set.

- If appropriate, give the user or the process administrator privileges (on Windows) or root privileges (on UNIX and Linux) and reissue the device configuration request.

- Establish a common EMM server name as follows:
  - Run `tpautoconf -get_gdbhost` on other hosts.
  - Set the EMM server name with
    
    ```
    tpautoconf -set_gdbhost host_name
    ```
    
    where `host_name` is the host name returned by `tpautoconf -get_gdbhost`.

**Device configuration status code: 2**

**Message:** The `device_mappings` file has invalid license info

The problem concerns one of the following files:

- `/usr/openv/share/device_mappings.txt` (UNIX and Linux) or
- `install_path\VERITAS\NetBackup\share\device_mappings.txt` (Windows).

- The file does not exist.

- The file is for a different version of NetBackup. You can find what version it is for by reading the header in the file.

- The file has a corrupted licensing digest.

**Recommended Action:** Download the latest device mapping file from the following &Company; support website:

`www.symantec.com/business/support/`

**Device configuration status code: 3**

**Message:** Could not get hostname

**Explanation:** An attempt to look up the host name for this host failed.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Verify that the host name is resolvable.
Device configuration status code: 7

**Message:** Invalid SCSI port number for the robot

**Explanation:** A request was made to add or change the SCSI port number for a robot, but the SCSI port number provided was not valid.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Specify the correct SCSI port number for the robot. Perform device discovery by using the Device Configuration wizard, or check the Windows registry as needed to obtain the SCSI port number.

Device configuration status code: 8

**Message:** Invalid SCSI bus number for the robot

**Explanation:** A request was made to add or change the SCSI bus number for a robot, but the SCSI bus number provided was not valid.

**Recommended Action:** Specify the correct SCSI bus number for the robot. Perform device discovery by using the Device Configuration wizard, or check the Windows registry as needed to obtain the SCSI bus number.

Device configuration status code: 9

**Message:** Invalid SCSI target for the robot

**Explanation:** A request was made to add or change the SCSI target for a robot, but the SCSI target provided was not valid.

**Recommended Action:** Specify the correct SCSI target for the robot. Perform device discovery by using the Device Configuration wizard, or check the Windows registry as needed to obtain the SCSI target.

Device configuration status code: 10

**Message:** Invalid SCSI logical unit number for the robot

**Explanation:** A request was made to add or change the SCSI logical unit number for a robot, but the SCSI logical unit number was not valid.

**Recommended Action:** Specify the correct SCSI logical unit number for the robot. Perform device discovery by using the Device Configuration wizard, or check the Windows registry as needed to obtain the SCSI logical unit number.
Device configuration status code: 11

Message: Invalid Usage

Explanation: One of the Media Manager device configuration commands (tpconfig or tpautoconf) was executed with improper options. Or an incompatibility exists between components or versions of the product.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Check the tpconfig or the tpautoconf usage statement for expected usage and compare with the parameters being sent to start the new process.
- Verify that all Media Manager binaries are at a compatible version level.

Device configuration status code: 13

Message: Failed reading drive or robot config file

Explanation: A request was made to list the device configuration, but an error was encountered while reading from the EMM database.

- Examine the daemon debug log and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Verify that nbemm is running. Display the device configuration to determine whether or not the database is corrupt. Restore a saved copy of the databases from catalog backups, or delete them and recreate the device configuration as needed.

Device configuration status code: 14

Message: Invalid drive index

Explanation: A request was made to add, update, or list a drive configuration entry, and the specified drive index was not associated with a configured drive.

- Display the device configuration to obtain the list of valid drives. Avoid making device configuration changes from multiple sources simultaneously.
- If more information is needed, examine the daemon debug log and command or interface output for a more detailed message on the error.
  See “Using debug logs” on page 422.

Device configuration status code: 15

Message: Invalid robot number
**Explanation:** On a request to modify the device configuration, the following occurred: the specified robot number was not within the allowable range, the robot number did not correspond to a currently configured robot, or the robotic database is corrupted.

- Specify a robot number in the range of 0 to 32767.
- Ensure that all device configuration changes or deletions are performed on the devices that are currently part of the device configuration.
- Verify that nbemm is running. Restore a saved copy of the robotic database from catalog backups, or delete it and recreate any needed robotic configuration information.

**Device configuration status code: 16**

**Message:** A SCSI inquiry sent to the device has failed

**Explanation:** On a request to add or update a SCSI robotic library or drive, Media Manager cannot obtain the device’s serial number and inquiry string. Media Manager obtains this information by sending a SCSI Inquiry command to the device. Failure indicates that NetBackup was not able to communicate with the device by means of SCSI.

- Ensure that the device is physically connected.
- Ensure that the operating system is configured to recognize the device and that the operating system can see the device.
- Ensure that no other process uses the device and that the device is not offline.

**Device configuration status code: 17**

**Message:** This robot type does not support multiple media types

**Explanation:** An attempt to add or update a robotic drive failed because the drives in this robotic library are configured with a different drive type. (Some NetBackup robotic library types do not support multiple media types.)

Refer to the *NetBackup Release Notes* or to the *NetBackup Administrator’s Guide, Volume II*, for more information on which NetBackup robotic library types support multimedia.

- Configure all drives for this robotic library with the same drive type.
- If you use NetBackup Server and want a robotic library with multiple media types, contact &CompanyName; to purchase NetBackup Enterprise Server.
Device configuration status code: 18

**Message:** Invalid robot type

**Explanation:** On a request to modify the device configuration, the specified robot type was invalid. Or it did not match the robot type for the robot that is associated with the specified robot number.

- Check the device configuration for configured robots, and specify the correct robot type applicable for the device configuration information being updated.
- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Verify that all Media Manager binaries are at a compatible version level.

Device configuration status code: 19

**Message:** Invalid device path name

**Explanation:** On a request to change the device configuration, the specified device path or device name was not valid.

- To avoid configuring invalid device paths and device names, use the Device Configuration wizard (on supported device discovery platforms). The wizard automatically configures device paths and device names.
- On Windows hosts, check the operating system configuration or registry for device names and refer to the `tpconfig` command in NetBackup online help. Information for UNIX and Linux hosts is available
  See the *NetBackup Device Configuration Guide*.
  Always use no-rewind device files for drives that are attached to UNIX and Linux hosts. Check to ensure that the specified device paths exist as character-special files. Check for detailed errors from the command or the user interface output.

Device configuration status code: 21

**Message:** Robot number is already in use

**Explanation:** On a request to add a robot to the device configuration, the robot number was found to be already in use for a different robot.

**Recommended Action:** Check the device configuration on all device hosts for configured robots, and specify a robot number that is not already in use. Use the following to display all devices in the EMM database:

```
tpconfig -emm_dev_list
```
Device configuration status code: 22

Message: Device path is already in use

Explanation: On a request to add or change robot information in the device configuration, the specified robotic device path is in use for another configured robot.

- To avoid configuring the device paths that are already in use, use the Device Configuration wizard (on supported device discovery platforms). The wizard automatically configures device paths and device names.
- Display the device configuration using `tpconfig -d` or a device configuration interface to see the robotic information that is already configured. Windows hosts have multiple ways to configure robots (changer names or port, bus, target, LUN). Check the operating system configuration or registry for changer names and their associated SCSI paths. Check for detailed errors from the command or the user interface output.

Device configuration status code: 24

Message: Incomplete robot information

Explanation: On a request to change the device configuration, some of the required robot information was not specified.

Recommended Action: Check the command usage and reissue the request with all required robot information specified.

Device configuration status code: 25

Message: Robot drive number in use for this robot

Explanation: On a request to change the device configuration, the specified drive address in the robot is in use by another drive in the device configuration.

Recommended Action: The drive address in the robot is the following: the robot drive number for most robot types, the ACS/LSM/PANEL/DRIVE coordinates for ACS robots, or a vendor drive name for TLH and TLM robots. Two drives cannot have the same drive address in a robot in a given device configuration. If the drive addresses need to be adjusted, delete one of the drives or make use of an unused drive address as a temporary state. For example, a robot has two drives with robot drive numbers 1 and 2 that need to be swapped. Change one drive to use robot drive number 3 temporarily. Then change the other drive to use robot drive number 1 or 2 as appropriate. Finally, change the first drive to the open robot drive address 1 or 2.
Device configuration status code: 27

**Message:** Invalid drive type for the robot

**Explanation:** On a request to configure a drive to be in a robot, the drive type was not valid for the selected robot type.

**Recommended Action:** Check the Robot Attributes tables in the following manual to determine valid media types for a given robot type:

See the *NetBackup Device Configuration Guide*.

Drive types directly correspond to the listed media types. Configure supported devices so that invalid combinations of drive types and robot types are not required.

Device configuration status code: 28

**Message:** Invalid robot drive number for the robot type

**Explanation:** On a request to configure a drive to be in a robot, the robot drive number was not valid for the selected robot type.

**Recommended Action:** The robot drive number (for ACS robots, the set of ACS drive identifiers) is limited to the ranges that are based on the robot type. These limits are based on a supported device list. An invalid robot drive number means that the drive number was not within the acceptable range. Make sure that the robot hardware is supported and that the required patches are installed to support the robotic library. If the robot type is TLH or TLM, do not specify a robot drive number because the drives are addressed with a vendor drive name.

Device configuration status code: 29

**Message:** Drive index is in use by another drive

**Explanation:** On a request to add a drive to the device configuration, the requested drive index was in use on the targeted device host.

- To avoid configuring a drive index that is already in use, use the Device Configuration wizard (on supported device discovery platforms). The wizard automatically configures the drive index.

- If you use a device configuration interface that allows the drive index to be specified, do the following: use `tpconfig -d` to determine the drive indexes already in use on the targeted device host. Then specify a drive index that is not in use.
Device configuration status code: 30

Message: Robot number is in use by another robot

Explanation: On a request to add or update a robotic drive in the device configuration, the following occurred: the robot number and robot type specified were associated with an existing robot of a different robot type.

Recommended Action: Check the device configuration on the targeted device host and identify the configured robots. On the drive configuration request, specify both the robot number and robot type that relate to the robot that contains the drive.

Device configuration status code: 31

Message: Robot number does not exist

Explanation: On a request to add or update a drive or robot in the device configuration, the following occurred: the robot number and robot type specified were not associated with any configured robots on the targeted device host.

Recommended Action: Check the device configuration on the targeted device host and identify the configured robots. Every drive that is configured as a robotic drive must already have its robot configured on that device host. Shared robotic libraries having robotic control on a remote host must have a logical robotic entry that refers to the remote host having robotic control. Add the robot to the device configuration first. Then add the drive. Define it to be in the robot. If the robot was already configured, specify the correct robot number and robot type on the drive or the robot configuration request.

Device configuration status code: 33

Message: Robot type must be controlled locally

Explanation: On a request to add or update a robot in the device configuration, the following occurred: a remote control host was specified for a library type which does not support it.

- Check that you configured the correct robot type.
- Configure the device with local control by using its local device path.

Device configuration status code: 34

Message: Drive name is already in use by another drive

Explanation: On a request to add or update a drive in the device configuration, the requested drive path was in use on the targeted device host.
To avoid configuring any paths that are already in use, use the Device Configuration wizard (on supported device discovery platforms). The wizard automatically configures the drive paths.

Before you make configuration changes, check the existing drive configuration through a device configuration interface. Or run `tpconfig -d` to determine the drive paths that are already in use on the targeted device host. Then specify a drive path that is not already in use.

**Device configuration status code: 35**

**Message:** Drive name does not exist

**Explanation:** On a request to update or delete a drive in the device configuration, the following occurred: no drives having the specified drive name were found on the targeted device host.

**Recommended Action:** Check the device configuration on the targeted device host and identify the configured drives. When you make drive configuration changes or deletions, specify the drive name as it is configured. Take care to use the proper case.

**Device configuration status code: 36**

**Message:** <NONE>

**Explanation:** On a request to make a device configuration change, an error occurred. A detailed message appears in the command or the utility interface output.

- Examine the daemon debug log and command or interface output for a more detailed message on the error.
  - See “Using debug logs” on page 422.
- Retry the device configuration request and examine the logs.

**Device configuration status code: 37**

**Message:** Residence is not licensed for shared drive support

**Explanation:** On a request to add or update a drive in the device configuration, the drive was specified as shared. No support for shared drives exists for that drive type or for the type of robot that is associated with the drive.

**Recommended Action:** Check the Technical Support Web site and product release documentation for supported device configurations.
Device configuration status code: 38

**Message:** Current version does not support remote device host

**Explanation:** On a request to change the EMM server, the specified host is not the local host. The current software is not licensed to allow remote hosts.

**Recommended Action:** Check product documentation for supported device configurations. Obtain an additional software license that allows remote hosts to be configured, or specify only local host names on the configuration request.

Device configuration status code: 39

**Message:** Adding this drive would exceed the maximum allowed

**Explanation:** On a request to add a drive to the device configuration, the following occurred: the licensed limit for the maximum number of drives was reached on the targeted host.

**Recommended Action:** Check product documentation for supported device configurations. Obtain an additional software license that allows more drives to be configured. Or limit the configuration to the number of drives that the current licensing allows.

Device configuration status code: 40

**Message:** Adding this device would exceed the maximum allowed

**Explanation:** On a request to add a robot to the device configuration, the following occurred: the licensed limit for the maximum number of robots was reached on the targeted host.

**Recommended Action:** Check product documentation for supported device configurations. Obtain an additional software license that allows more robots to be configured. Or limit the configuration to the number of robots that the current licensing allows.

Device configuration status code: 41

**Message:** Cannot change terminal mode

**Explanation:** When an attempt was made to change the mode for terminal input between cooked and raw, a system call failed.

**Recommended Action:** Examine the user interface output for the system error that is associated with the failed system call. Then troubleshoot according to operating system vendor recommendations.
Device configuration status code: 42

**Message:** Cannot create miscellaneous working repository

**Explanation:** On a device configuration request, the miscellaneous working directory or folder is not present and cannot be created.

**Recommended Action:** Find out why `/usr/openv/volmgr/misc` (UNIX and Linux) or `install_path\volmgr\misc` (Windows) cannot be created. On Windows, determine which accounts the NetBackup Volume Manager service and device configuration interfaces are running under. Compare them with the security properties of the database folder. On UNIX and Linux, determine whether users or device configuration interface callers are running under a user and group with permissions to create the miscellaneous directory.

Device configuration status code: 44

**Message:** Cannot discover devices. See the Troubleshooting Guide for details.

**Explanation:** Device discovery cannot obtain or verify its lock file or had a problem with the EMM server.

- Examine the daemon debug log and command or interface output for a more detailed message on the system error. See “Using debug logs” on page 422.
- Retry the operation and examine the logs. One of the following may have occurred:
  - Lock file problems: The device discovery process sets a lockfile in the `/usr/openv/volmgr/misc` (UNIX and Linux) or `install_path\Volmgr\misc` (Windows) directory named `tpac.lock`. It sets the lockfile to ensure that only one instance of discovery runs on a particular host. It then checks the lockfile before it updates the configuration.
  - Cannot obtain lockfile.
    The lockfile may be held by another discovery process. In this case the following error is displayed:
    ```
    "another tpautoconf is already running"
    ```
    Use standard OS process tools (`ps` on UNIX and Linux or Task Manager on Windows) to determine if another `tpautoconf` process is running. If not, delete the lockfile and re-run device discovery. If another `tpautoconf` process is running, wait for it to complete before retrying.
  - Failed the lockfile check.
In the case of long device-discovery cycles, the interface may timeout or the user may cancel the process. Part of the timeout or cancellation is to remove the lockfile. This action tells the device discovery process that it should not continue making modifications to the device configuration. If action occurs, run the discovery process again.

**Device configuration status code: 48**

**Message:** RSM is not supported.

**Explanation:** On a request to make a device configuration change, the RSM (Microsoft Removable Storage Manager) robot type was specified, but it is no longer supported.

**Recommended Action:** Use a supported Media Manager robot type.

**Device configuration status code: 49**

**Message:** global device database host name is invalid.

**Explanation:** On a device configuration request, the EMM server name cannot be obtained.

The EMM server name is obtained through an internal request to read the bp.conf file (or Windows registry). This request is likely to fail if the EMMSERVER entry is not set.

**Recommended Action:** Use `tpautoconf -get_gdbhost` on a device host to obtain its EMM server name. Use `tpautoconf -set_gdbhost` to set the EMM server name, as needed.

**Device configuration status code: 51**

**Message:** No compatible device is registered at these SCSI coordinates.

**Explanation:** On a request to add or change robot or drive information in the device configuration, the following occurred: the specified SCSI coordinates did not correspond to a device in the system registry. This status code applies to Windows systems only.

**Recommended Action:** To avoid manually specifying SCSI coordinates (port, bus, target, and LUN), use the Device Configuration wizard. The wizard fully automates (on supported device discovery platforms) device configuration requests. Or use the Media And Device Management interface to browse for devices in the system registry. Check the operating system registry to ensure that devices are present at the specified coordinates when SCSI coordinates are manually configured.
Device configuration status code: 52

**Message:** The device name is not valid, no device responded.

**Explanation:** On a request to add or change robot or drive information in the device configuration, the following occurred: no device was found in the system registry with the specified device name. This error code applies to Windows systems only.

**Recommended Action:** To avoid manually specifying the device name, use the Device configuration wizard. The wizard fully automates (on supported device discovery platforms) device configuration requests. Or use the Media And Device Management interface to browse for devices in the system registry. Check the operating system registry to ensure that devices are present at the specified coordinates when devices are manually configured.

Device configuration status code: 53

**Message:** Shared Storage Option (SSO) is not licensed

**Explanation:** An attempt to add a path to a drive failed. It failed because the SSO license was not installed.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Verify that an active SSO license is installed on the following: all servers that have a path configured to this drive and the server where this operation is performed.

Device configuration status code: 55

**Message:** Invalid NDMP hostname

**Explanation:** An invalid hostname or no hostname was specified.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Use `tpconfig -dnh` to verify that the host has been configured.

- Check the usage of the `tpautoconf -list_snapvault_volumes` command.

Device configuration status code: 56

**Message:** Invalid NDMP username

**Explanation:** An invalid username or no username was specified.
- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Use `tpconfig -dnh` to verify that the host has been configured.

**Device configuration status code: 57**

**Message:** Internal NDMP error

**Explanation:** An error occurs on the NDMP device.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Check the usage of the `set_ndmp_attr -probe` or `tpautoconf -probe` commands.

- An error occurs while trying to get the serial number and inquiry string for a device connected to an NDMP filer. Verify that the device is properly attached to the filer.

**Device configuration status code: 58**

**Message:** NDMP failed to verify host

**Explanation:** An error occurs while using the NDMP verify functionality.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Check the usage of the `tpautoconf -verify` commands.

- Verify that the device is properly attached to the filer.

**Device configuration status code: 59**

**Message:** NDMP is not installed on platform

**Explanation:** The NDMP option is not installed on this server.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- Verify that the NDMP option is properly installed and licensed.

- Verify that NDMP is supported on the platform in question.
Device configuration status code: 60

**Message:**  Invalid NDMP password

**Explanation:** An invalid NDMP password or no password was provided.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Verify that the password is appropriate for the media server and filer pair.
- Verify that the password was provided correctly on the command or in the NDMP Host dialog box.

Device configuration status code: 61

**Message:** NDMP host exists, use change option

**Explanation:** An attempt to add a filer fails because the filer already exists in the EMM database.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Use the `-update` option of `tpconfig` instead of `-add`.

Device configuration status code: 62

**Message:** NDMP host does not exist

**Explanation:** The NDMP host does not exist in the EMM database.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Use the `-add -nh` option on the `tpconfig` command to add the NDMP host.

Device configuration status code: 63

**Message:** NDMP request failed

**Explanation:** An attempt to create an NDMP session failed, or an attempt to send an NDMP message failed.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Verify NAS filer licenses, supported operating system levels, and network connectivity.

**Device configuration status code: 64**

**Message:** Invalid NDMP device

**Explanation:** An invalid NDMP device was specified.

**Recommended Action:** Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 422.

**Device configuration status code: 65**

**Message:** NDMP robot exists, use change option

**Explanation:** The robot currently exists in the EMM database.

**Recommended Action:** Use the NetBackup Administration Console, or the `tpconfig -update -robot` command, to change the robot configuration.

**Device configuration status code: 66**

**Message:** NDMP robot does not exist

**Explanation:** An update request was issued for a non-existent robot.

**Recommended Action:** Use the NetBackup Administration Console, or the `tpconfig -update -robot` command, to add the correct robot.

**Device configuration status code: 67**

**Message:** Unable to connect to NDMP host verify hostname

**Explanation:** A network connection to the NAS host failed.

- Use the `tpautoconf -verify` command to verify the hostname, username, and password.
- Use the `ping` command to verify network access.

**Device configuration status code: 68**

**Message:** Unable to process NDMP message

**Explanation:** An unexpected error occurs while an NDMP message processed.

**Recommended Action:** Examine debug logs and system logs for a more detailed message on the error.
See “Using debug logs” on page 422.

**Device configuration status code: 69**

**Message:** NDMP host not connected

**Explanation:** Unable to process NDMP messages with the NDMP host.

**Recommended Action:** Examine debug logs for more information on the error.

See “Using debug logs” on page 422.

**Device configuration status code: 70**

**Message:** Unable to create NDMP session

**Explanation:** An error occurs while opening an NDMP connection to a NAS filer.

- Examine debug logs for more information on the error.
  
  See “Using debug logs” on page 422.

- Use the `tpautoconf -verify` command to verify the hostname, username, and password.

- Use the `ping` command to verify network access.

**Device configuration status code: 71**

**Message:** NDMP get_host_info failed

**Explanation:** The NAS host fails to correctly process the `ndmp_get_host_info` protocol request.

**Recommended Action:** Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 422.

**Device configuration status code: 72**

**Message:** NDMP get_server_info failed

**Explanation:** The NAS host fails to successfully process the `get_server_info` protocol request.

**Recommended Action:** Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 422.
Device configuration status code: 73

**Message:** Unsupported NDMP version

**Explanation:** NetBackup supports tape devices on NDMP protocol versions V2, V3, and V4. For automatic device configuration, only V3 and V4 are supported.

- Examine debug logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- See your NAS vendor documentation for instructions on how to switch NDMP versions.

Device configuration status code: 74

**Message:** NDMP authorization error, verify username/password

**Explanation:** NetBackup fails to authenticate the username or password on the NAS host.

**Recommended Action:** Use the `tpautoconf -verify` command to verify the username and password.

Device configuration status code: 75

**Message:** NDMP config_get_mover_type failed

**Explanation:** The NAS host fails to successfully process the `config_get_mover_type` protocol request.

**Recommended Action:** Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 422.

Device configuration status code: 76

**Message:** NDMP config_get_connection_type failed

**Explanation:** The NAS host fails to successfully process the `config_get_connection_type` protocol request.

**Recommended Action:** Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 422.

Device configuration status code: 77

**Message:** Unable to connect to the EMM server
Explanation: A request was made to the EMM server, but it either did not reach the EMM server or resulted from a communication failure.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Verify that pbx_exchange and nbemm are running.

- Run the tpconfig -d or vmquery -a command to verify that the EMM server is actively running and that it accepts new connections.

**Device configuration status code: 78**

**Message:** The EMM server failed to process the request

**Explanation:** A request was made to the EMM server, but it either did not reach the EMM server or resulted from a communication failure.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Verify that pbx_exchange and nbemm are running.

- Run the tpconfig -d or vmquery -a command to verify that the EMM server is actively running and that it accepts new connections.

**Device configuration status code: 79**

**Message:** Unable to allocate memory for this process

**Explanation:** A memory allocation request failed.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Verify that adequate memory is available.

**Device configuration status code: 81**

**Message:** This is a drive path operation, use the -drpath option

**Explanation:** A path operation was specified with the tpconfig command without the -drpath option. This error can occur when you try to change a drive’s path using tpconfig -update -drive.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
See “Using debug logs” on page 422.

- Check `tpconfig` usage to ensure that the command is used properly and use `tpconfig -update -drpath` instead.

**Device configuration status code: 82**

**Message:** Add Drive Name Rule request failed

**Explanation:** A request to add a drive name rule failed.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- The rule being added already exists.

- The specified host does not exist in the EMM database. Use the `nbemmcmd` `-addhost` command to add the host to the EMM database.

**Device configuration status code: 83**

**Message:** Update Drive Name Rule request failed

**Explanation:** An update to a drive name rule failed.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- The rule being updated does not exist. Ensure that the drive name rule is entered correctly.

- The specified host does not have a local drive name rule configured. Configure a drive name rule.

**Device configuration status code: 84**

**Message:** Delete Drive Name Rule request failed

**Explanation:** A request to delete a drive name rule failed. You cannot add or delete a global drive name rule.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- A local drive name rule does not exist on the hosts specified.
Device configuration status code: 85
Message: List Drive Name Rule request failed
Explanation: Could not list the drive name rules for a given host or set of hosts.
- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Verify that the hosts are known in the EMM database.

Device configuration status code: 86
Message: Invalid Drive Name Rule
Explanation: A drive name rule was not specified, or contained an invalid character.
- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Observe the rules for drive names:
  - Cannot begin with a dash.
  - Cannot exceed 48 characters.
  - A literal field can only contain alphanumeric characters and plus (+), dash (-), period (.), or underscore (_).
  - An invalid field name was specified; check command usage.

Device configuration status code: 87
Message: System Error
Explanation: An operating system error occurred.
- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Verify that adequate memory is available.
- Verify that Windows networking is properly installed.

Device configuration status code: 88
Message: Invalid host
**Explanation:** An attempt was made to add a device to a host that the EMM database does not recognize.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Use `nbemmcmd -addhost` to add the host to the EMM database.

**Device configuration status code: 89**

**Message:** Drive name rule has exceeded its maximum length of 48 characters

**Explanation:** The specified drive name rule is too long.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Choose a shorter rule.

**Device configuration status code: 90**

**Message:** Another device configuration is already in progress

**Explanation:** An instance of the Device Configuration Wizard or `tpautoconf` is already running.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Retry the operation after the current instance is done.

- A lock on the device configuration cache may have been orphaned. Use the `nbemmcmd` command to clear the lock, then retry the operation.

**Device configuration status code: 91**

**Message:** The drive serial number already exists in the device database.

**Explanation:** An attempt was made to add a drive with a duplicate serial number.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Verify that the added drive has a unique serial number.
Device configuration status code: 92
Message: VxSS access denied
Explanation: A user attempts an operation without adequate permissions
- Verify that the user has the correct permissions to perform this operation.
- Verify that the authentication and authorization security settings are correct, under Host Properties in the NetBackup Administration Console. See the NetBackup Security and Encryption Guide for information on how to use the Symantec Product Authentication and Authorization Service.

Device configuration status code: 93
Message: Database Server is down
Explanation: A request was made to the EMM Server, but the underlying database server does not respond.
- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.
- This error can occur if a cold catalog backup is in progress. Retry the request after this operation has completed.

Device configuration status code: 94
Message: NetApp Disk Storage Unit feature is not licensed
Explanation: The NetApp NearStore disk storage unit is a licensed feature. You must install the NearStore license key before NetBackup can configure NearStore devices.
Recommended Action: Install the appropriate license key.

Device configuration status code: 95
Message: The requested operation is not valid for the specified Disk Type
Explanation: The storage device you configured is not a disk storage device.
Recommended Action: Select an appropriate storage device.

Device configuration status code: 96
Message: The specified Disk Array Host is not configured in NetBackup
**Explanation:** You must first add this disk array host to the NetBackup host configuration before this operation can be performed. To view hosts, see `nbemmcmd -listhosts` in the NetBackup Commands Guide.

- If you try to update an existing host’s credentials, this host no longer exists in NetBackup. It must be added again by using the `tpconfig` or the `nbemmcmd` command.
- The name you entered for the disk array host does not match any of the machine aliases in the NetBackup machine configuration. Use the `nbemmcmd` command to add the fully qualified array host name (or the name entered) to the machine alias list for your disk array.

**Device configuration status code: 97**

**Message:** No valid license key for Disk Array configuration

**Explanation:** Disk array snapshot support is a licensed feature. You must install the Snapshot Client license key before NetBackup can configure disk array credentials.

**Recommended Action:** Install the Snapshot Client license key.

**Device configuration status code: 98**

**Message:** Open Storage feature is not licensed

**Explanation:** Credentials for OpenStorage servers cannot be added without the NetBackup OpenStorage license key.

**Recommended Action:** Install the OpenStorage license key.

**Device configuration status code: 99**

**Message:** Credentials already exist

**Explanation:** Credentials already exist for the host you are trying to add.

**Recommended Action:** Delete the existing credentials and then add the new ones.

**Device configuration status code: 100**

**Message:** NetBackup Snapshot client not licensed

**Explanation:** Credentials for this type of host cannot be added without the NetBackup Snapshot Client license key. Host types that require this license are disk array manager servers and virtual machine servers.

**Recommended Action:** Install the NetBackup Snapshot Client license key.
Device configuration status code: 101

Message: authorization error, verify username/password

Explanation: Authorization failed with the given set of username and password values.

Recommended Action: Verify the values provided and check for typographical errors.

Device management status codes

These status codes appear in exit status and command output for the **ltid**, **tpclean**, **tpreq**, and **tpunmount** commands, and in system or debug logs. Programs that call those commands, such as media and device management user interfaces and the **vmoprcmd** command also presented these codes.

Device management status code: 1

Message: Invalid Drive Type/Density

Explanation: An invalid density was specified for the -d parameter on **tpreq**.

Recommended Action: Check the **tpreq** man page (command description) for the list of valid densities. Submit the mount request again with a valid density.

Device management status code: 2

Message: Drive is currently assigned

Explanation: A request was made for a specified drive, but the drive was assigned.

Recommended Action: Display drive status (by using **vmoprcmd** -d or other means) to see the list of drives and their assignment status. Run the request later or first clear the drive assignment: stop application activity on the drive, unmount the media with **tpunmount**, or reset the drive. If the wrong drive was specified, submit the request again. Specify the correct drive name or index as appropriate for the interface being used.

Device management status code: 3

Message: Error in Sending Operator Message

Explanation: An attempt was made to send an operational message to **ltid** on an already existing internal message queue used for inter-process communication. (**ltid** is the Media Manager device daemon on UNIX and Linux and the NetBackup Device Manager service on Windows.) An error was encountered in the message...
communications. The error probably indicates a lack of system resources for message queues.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- On UNIX and Linux servers, gather output from the `ipcs -a` command to see what resources are currently in use.

Device management status code: 4

**Message:** Error in Receiving Operator Message

**Explanation:** An attempt was made to receive a message from ltid on an already existing internal message queue used for inter-process communication. (ltid is the Media Manager device daemon on UNIX and Linux and the NetBackup Device Manager service on Windows.) An error was encountered in the message communications. The error probably indicates a lack of system resources for message queues.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- On UNIX and Linux servers, gather output from the `ipcs -a` command to see what resources are currently in use. Investigate whether ltid is tied up in communications with devices or other components.

Device management status code: 5

**Message:** Error in Sending Daemon Message

**Explanation:** ltid made an attempt to send an internal process communications message to a robotic daemon or process by using an already existing internal message queue. (ltid is the Media Manager device daemon on UNIX and Linux and the NetBackup Device Manager service on Windows.) An error was encountered in the message communications. The error probably indicates a lack of system resources for message queues.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

- On UNIX and Linux servers, gather output from the `ipcs -a` command to see what resources are currently in use. Investigate whether the robotic daemon
or process on the local device host is tied up in communications with devices or other components.

**Device management status code: 6**

**Message:** Error in Receiving Daemon Message

**Explanation:** `ltid` attempted to receive or process an internal process communications message to a robotic process by using an existing internal message queue. (`ltid` is the Media Manager device daemon on UNIX and Linux and the NetBackup Device Manager service on Windows.) An error was encountered in the message communications. The error probably indicates a lack of system resources for message queues, or mismatched software components.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- On UNIX and Linux servers, gather output from the `ipcs -a` command to see what resources are currently in use. Check the installed software components and verify that they are all at a compatible release version.

**Device management status code: 7**

**Message:** Error in Sending User Message

**Explanation:** `ltid` made an attempt to send a user message to `ltid` on an already existing internal message queue used for inter-process communication. (`ltid` is the Media Manager device daemon on UNIX and Linux and the NetBackup Device Manager service on Windows.) An error was encountered in the message communications. The error probably indicates a lack of system resources for message queues.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- On UNIX and Linux servers, gather output from the `ipcs -a` command to see what resources are currently in use.

**Device management status code: 8**

**Message:** Error in Receiving User Message

**Explanation:** An attempt was made to receive a user message from `ltid` on an already existing internal message queue used for inter-process communication. (`ltid` is the Media Manager device daemon on UNIX and Linux and the NetBackup...
Device Manager service on Windows.) An error was encountered in the message communications. The error probably indicates a lack of system resources for message queues. On Windows, this error can also occur if an internal-system-registered event cannot be opened.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- On UNIX and Linux servers, gather output from the `ipcs -a` command to see what resources are currently in use.

**Device management status code: 10**

**Message:** IPC sequence error

**Explanation:** An internal process communications message sequencing error has occurred.

**Recommended Action:**
Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 422.

**Device management status code: 12**

**Message:** Invalid Operator

**Explanation:** An internal list of operators could not be obtained.

**Recommended Action:** This error is an unexpected internal error. Stop and restart `ltid` (the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows).

**Device management status code: 13**

**Message:** Error in IPC SHMGET call

**Explanation:** A process was unable to get a shared memory identifier associated with a segment of shared memory that `ltid` maintains. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.)

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
On UNIX and Linux servers, gather output from the `ipcs -a` command to see what resources are currently in use.

**Device management status code: 14**

**Message:** Error in IPC SHMAT call

**Explanation:** A process was unable to attach a shared memory segment that *ltid* maintains. (*ltid* is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.)

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  - See “Using debug logs” on page 422.
- On UNIX and Linux servers, gather the output of the `ipcs -a` command to see what resources are currently in use.

**Device management status code: 15**

**Message:** The drive is DOWN

**Explanation:** An attempt was made to mount media on a drive or to reserve a shared drive that was logically configured to the DOWN state.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  - See “Using debug logs” on page 422.
- Check the application log files (such as the bptm log) to see why the drive may have been configured DOWN.
- Check the integrity of the drive, drive path, and media.

**Device management status code: 16**

**Message:** No mount pending for given mount index

**Explanation:** An attempt was made to retrieve information about a pending mount request, but no such pending mount request was found.

**Recommended Action:** Use a device monitor interface or consult application logs to see whether the request was completed or canceled. Requests to retrieve information for pending mount requests are valid only when the mount request is ongoing.

**Device management status code: 17**

**Message:** Drive does not support pending request density
Explanation: A drive was selected that has a drive type which is not compatible with the requested density.

- Allow the drive selection to be determined automatically.
- When you select the drive manually, check the device configuration and the valid density table (available in the tpreq man page or command description). Then specify a drive that is compatible with the requested density.

Device management status code: 19

Message: Only the administrative user can perform the requested operation

Explanation: Either an attempt was made to stop ltid (the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows). Or the tpcl clean command was called, but the user was not root (UNIX and Linux) or the administrator (Windows).

Recommended Action: If appropriate, give the user or the process administrator privileges on Windows or root privileges on UNIX and Linux and retry the operation.

Device management status code: 20

Message: Cannot stop device daemon with tapes assigned

Explanation: An attempt was made to stop ltid, but media is currently mounted and assigned. (ltid is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.)

Recommended Action: Halt all jobs referencing media, unmount all media, and stop all applications from using Media Manager before trying to stop ltid. If unable to unmount media through the application interface, check for the existence and permissions of the .ltisymlinks file in the /usr/openv/volmgr/misc directory or in the install_path\Volmgr\misc folder. Initiate tpunmount filename for each line in the .ltisymlinks file, where filename specifies the contents of a line in that file. For example, on UNIX and Linux, the command may look like the following:

    tpunmount /usr/openv/netbackup/db/media/tpreq/A00001

Device management status code: 21

Message: The drive is not ready or inoperable

Explanation: A drive was selected for a mount request, but the drive is not ready with loaded media.
**Recommended Action:** Wait until the drive is ready before you manually assign a drive to a pending mount request.

**Device management status code: 22**
**Message:** IPC Error: Daemon may not be running
**Explanation:** A request to `ltid` cannot be serviced. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.) `ltid` is probably not running. If `ltid` is still running, its process lock file may have been removed. Also, message queues may not function correctly on the system.

- If `ltid` is not running, start `ltid` and try the operation again. On UNIX and Linux, run `/usr/openv/volmgr/bin/ltid`, and on Windows, start the NetBackup Device Manager service.
- If `ltid` is already running, check for the existence and permissions of the lock file itself and the lock file directory, which are as follows: `/usr/openv/volmgr/misc/.ltipid` (UNIX and Linux) or `install_path\Volmgr\misc\.ltipid` (Windows). Terminate the `ltid` process if it is running. Create the lock directory or folder and adjust the permissions as needed so that `ltid` can obtain the lock.
- On UNIX and Linux, check the `msgget` man page and look for suggestions on how to troubleshoot the system message queues.

**Device management status code: 23**
**Message:** Invalid Drive Number
**Explanation:** A request was made for drive, but no such drive can be found in the active configuration.

**Recommended Action:** Ensure that `ltid` was stopped and restarted after changes were last made to the device configuration. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.) Display the device configuration (by using `tpconfig -d` or other means) to view the list of valid drives. Specify the drive name or index as appropriate for the interface being used.

**Device management status code: 24**
**Message:** Requested drive could not be reserved
Explanation: An attempt was made to reserve a shared drive, but the drive reservation request failed. This status code is related to the internal implementation of the SSO feature. It is not related to SCSI Reserve or Release.

Recommended Action: This condition is expected for any shared drives that are retried automatically. If problems persist, verify the following: the EMM server services requests and it does not list drives as reserved to hosts that currently do not use the drives.

Device management status code: 25

Message: File name does not exist

Explanation: A logical tape file or help file cannot be found. The `tpunmount` command was probably issued with a logical tape file specified that does not exist for this user.

Recommended Action: Check for existence of the logical tape file at the file path specified. The specified file path must match the exact case-sensitive path that was used when the tape mount was requested. Submit the request again with the correct file path. If the condition occurs during operator display of a pending request error message, check to see if the help files are properly installed at the following: `/usr/openv/volmgr/help/robots/robot_type/help_file_name` (UNIX and Linux) or at `install_path\Volmgr\Help\Robots\robot_type\help_file_name` (Windows).

Device management status code: 26

Message: Request terminated because host not validated for volume pool

Explanation: The host where the mount request was initiated is denied access to the media. It is denied due to defined permissions for the volume pool in which the media ID is contained.

- Query the volume pool information for the requested volume pool on the host where the mount request was issued by running `vmpool -listall -b`. Check the system log to obtain the name of the host where the mount request originated. This host name is the one returned by the `system hostname(1)` command.

- Change the volume pool host name security with `vmpool` or another user interface that supports volume pool host attributes. Or change the volume pool that is associated with the volume (if it is not assigned). Or log in to the host that is allowed to use media in the targeted volume pool. Then, submit the mount request again.
Device management status code: 27
Message: Request terminated because media ID is expired
Explanation: A mount request was canceled because the media was requested with write access, and the media has expired.
Recommended Action: Request read-only access to the media on the mount request if a read-only operation is needed. Replace the media or change the expiration date to a future date that is based on site policy. Use the media management interface to view and change the expiration date for the media. Check and correct the system date and time, as needed.

Device management status code: 28
Message: Error in MsgGet
Explanation: tid made an attempt to obtain a message queue identifier that was used for internal message communications. (tid is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.) The request failed due to a system error. The error probably indicates a lack of system resources for message queues, or mismatched software components.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- On UNIX and Linux servers, gather the output of the ipcs -a command to see what resources are currently in use. Check the installed software components and verify that they are all at a compatible release version.

Device management status code: 30
Message: Request terminated because media id will exceed maximum mount count
Explanation: A mount request has been canceled because the media being requested has reached the maximum mount count associated with the media.
Recommended Action: Replace the media or change the maximum mount count to a higher value that is based on site policy. A media management interface can be used to view and change the maximum mounts allowed for the media. Check that the number of mounts for the media is set to a reasonable value given the media’s usage history. Correct it as needed by using vmchange.

Device management status code: 32
Message: Error in getting semaphore
Explanation: \texttt{ltid} made an attempt to obtain a semaphore that was used for arbitrating access to shared memory. (\texttt{ltid} is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows) The request failed due to a system error. The error probably indicates a lack of system resources for semaphores, or mismatched software components.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- On UNIX and Linux servers, gather the output of the \texttt{ipcs -a} command to see what resources are currently in use. Check the installed software components and verify that they are all at a compatible release version.

Device management status code: 33

Message: Error in SEMAPHORE operation

Explanation: A process was unable to perform a semaphore operation (such as lock or unlock) associated with resources maintained by \texttt{ltid}. (\texttt{ltid} is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.)

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- On UNIX and Linux servers, gather the output of the \texttt{ipcs -a} command to see what resources are currently in use.

Device management status code: 35

Message: Request terminated because media is unavailable (in DOWN drive, misplaced, write protected or unmountable)

Explanation: A mount request was canceled because the media being requested is not available. It may be in a DOWN drive or misplaced, write protected, or unmountable. Another possible cause of this message is that you are using a cleaning tape with no cleanings remaining.

Recommended Action: Use robotic inventory or manual means to compare the contents of media in the robotic library with the volume configuration. Then update the configuration as needed. Determine the physical location of the media. Check integrity of the drive, drive path, and media if the media is found in a logically DOWN drive. Verify that the media is not a misconfigured cleaning tape. Move the media into the robotic library and update the volume configuration if the media was not present in the library. Set the cartridge tab to allow write access,
or request the media with read-only access if the write protection was the cause of the error.

If the problem is a cleaning tape with no cleanings remaining, replace the cleaning tape.

**Device management status code: 36**

**Message:** Request terminated by tpunmount call from another process

**Explanation:** A request was made to change the limit for the following: the number of times that a volume can be mounted with write access for one or more volumes in the volume configuration. The value specified was not within the acceptable range. The maximum number of mounts value may also be invalid in the number of mounts and cleanings field of a bar code rule.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Specify a maximum-mounts value within the range of 0 to 2,147,483,647.

**Device management status code: 37**

**Message:** Drive being assigned is either not NDMP or on the wrong NDMP client

**Explanation:** A mount request was canceled because the request was targeted to a drive configured as attached to an NDMP client. The request was manually assigned to a drive other than the requested drive. The assigned drive is either not NDMP or it is an NDMP drive configured to a different client.

**Recommended Action:** Display the device configuration to determine which drives are configured as being attached to specific NDMP clients. Ensure that `ltid` was stopped and restarted after the last configuration changes were made. Reissue the request and assign it to a drive that is attached to the requested NDMP client.

**Device management status code: 38**

**Message:** Character device name for drive is not a character device

**Explanation:** On a tape mount request, the configured tape drive’s no-rewind-on-close device file was neither a character-special device nor of a known type such as NDMP. (NDMP does not need to be a character special file.)

- To avoid configuring invalid device paths and device names, use the Device Configuration wizard (on supported device discovery platforms). The wizard automatically configures paths and device names for tape drives.
Always use no-rewind tape device files or recognized drive name syntax (such as for NDMP) for tape drives. Make sure that the specified device paths exist as character-special files. Check for detailed errors from the command or the user interface output.

See the *NetBackup Device Configuration Guide*.

**Device management status code: 39**

**Message:** Parameter is invalid

**Explanation:** The `tpclean` command was called with invalid arguments, or an internal function encountered a missing reference to data it requires.

- If a cleaning operation was requested, check the `tpclean` usage statement and compare with the parameters that were specified.

- Check the installed software components and verify that they are all at a compatible release version.

**Device management status code: 40**

**Message:** File name already exists

**Explanation:** On a tape mount request, the file name that is associated with the request already exists or is already associated with another mount request.

**Recommended Action:** Submit the request again with a different file name. Specify a file name that does not correspond to an existing file. Or specify a file name that is not in use for another mount request that may be in progress.

**Device management status code: 41**

**Message:** Unknown drive name

**Explanation:** A request was made for a specified drive, but no such drive can be found in the active configuration. This status can occur in the following situations: if the device files are corrupt or missing, if they cannot be opened or read, or if there are no devices configured.

- Ensure that `ltid` was stopped and restarted after changes were last made to the device configuration. (`ltid` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.) Display the device configuration (use `tpconfig -d` or other means) to see the list of valid drives. Specify the drive name or index as appropriate for the interface being used.

- Check integrity of the EMM database. Display the device configuration to do the following:
Determine if the database is corrupt.

- Restore a saved copy of the database file from catalog backups, or remove the devices and recreate the device configuration.

**Device management status code: 42**

**Message:** Incorrect tpreq access mode

**Explanation:** On a tape mount request, the specified access mode was invalid. On Windows hosts, a user without Administrator privileges made a request for NetBackup Device Manager services.

**Recommended Action:** When you use `tpreq`, specify an access mode argument of `r` for read, `w` for write, or use the default (read) access mode. When you make any requests that require NetBackup Device Manager services on Windows, do so under an account with Administrator privileges.

**Device management status code: 44**

**Message:** You do not have permission to create the file

**Explanation:** On a tape mount request, the file name that is associated with the request cannot be created due to directory permissions or folder permissions.

**Recommended Action:** Check for existence of a file at the file path specified. If a file is found, delete the file if it is not needed or submit the request again and use a different file path. If no file exists at that location, check the directory permissions or the folder permissions for the following: read and write access for the user or the application process that issued the mount request.

**Device management status code: 46**

**Message:** Tape needs to be write enabled

**Explanation:** On a tape mount request, the specified access mode was for write access, but the physical media was write-protected.

**Recommended Action:** Change the physical media write-protect setting to allow write access (unlocked), or submit the request again with read-only access. To request read-only access using `tpreq`, specify an access mode argument of `r` for read or use the default (read) access mode.

**Device management status code: 47**

**Message:** Unable to establish scan host for shared drive
**Explanation:** On a request to change a shared drive's status, an attempt to establish a connection to the drive's scan host failed.

- Determine which host serve as the drive's scan host: use `vmprcmd` output or by checking the Device Monitor in the Administration Console.

- Ensure that `vmd` (the NetBackup Volume Manager daemon on UNIX and Linux or NetBackup Volume Manager service on Windows) is running on the scan host. On the scan host, examine debug logs and system logs for any messages that are related to the error.

- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.

- The detailed reason for the canceled request should be available in the daemon debug logs on the scan host. Correct the problem and submit the request again if needed.

**Device management status code: 48**

**Message:** Host is not the scan host for this shared drive

**Explanation:** On a request to assign, reserve, or scan a drive, the targeted device host determined that it was not the scan host for the drive. The request was refused (the caller retries it).

- If problems are encountered as a result of the reported error, check for communication, configuration, and system problems among the associated hosts. To check, use `vmprcmd` output or check the Device Monitor in the Administration Console.

- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.

- Configure scan ability priorities for assigning scan hosts by changing the Media Manager configuration. Configure so that less network connections need to be maintained, and greater system load is placed on hosts with more capability to service the load.

**Device management status code: 49**

**Message:** Tape file path exceeds 255 character maximum

**Explanation:** On a tape mount request, the file name that is associated with the request exceeds 255 characters.
**Recommended Action:** When you request a tape mount, ensure that the file name does not exceed 255 ASCII characters in length. If the mount requests come from an application, request an application change to use a shorter file name. Or install the product in a directory or a folder that does not cause the file name limit to be exceeded.

**Device management status code: 50**
**Message:** No action pending for given mount index
**Explanation:** On a request to obtain the pending action for a mount request, no known pending action was associated with the request.

**Recommended Action:** Use a device monitor interface to display any requests that have pending actions. Perform requests (like assign, deny, display, or resubmit) only on the requests that have pending actions.

**Device management status code: 52**
**Message:** No robot is defined of this type
**Explanation:** On internal communications between a robotic daemon or process and `ltd`, no robots of the expected type were found actively configured. (`ltd` is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.)

**Recommended Action:** Display the running robotic processes to see if processes from a previous configuration are still running. If any are found, terminate them. Check the installed software components and verify that they are all at a compatible release version.

**Device management status code: 53**
**Message:** Request has been queued (Cancel to clear message)
**Explanation:** A mount request or drive-related operation was queued because drive resources were in use.

**Recommended Action:** Wait until the drive resources become available, or cancel pending mount requests as needed.

**Device management status code: 55**
**Message:** Operator denied mount request
**Explanation:** The operator denied a mount request.

**Recommended Action:** This error occurs when an administrator or operator cancels a user or application mount request. The request may have been canceled...
for a number of reasons: missing or faulty media or the need to allow other, higher priority requests to obtain drive resources. Check with the administrator or operator for more information.

**Device management status code: 56**

**Message:** Mount canceled, device daemon is terminating

**Explanation:** Pending mount requests were canceled because the administrator terminated `ltid` (the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows).

**Recommended Action:** Wait for `ltid` to be restarted before you submit the request again. Check with the administrator as needed to determine daemon or service availability.

**Device management status code: 58**

**Message:** The device is not robotic, cannot perform cleaning

**Explanation:** An attempt was made to automatically clean a drive, but the drive is not in a robotic library.

**Recommended Action:** Clean stand-alone drives by inserting a cleaning tape when needed. For non-shared drives, update the cleaning statistics with `tpclean` or another user interface that supports cleaning-related operations.

**Device management status code: 59**

**Message:** No cleaning tape is defined in the device’s robot or 0 cleanings remain.

**Explanation:** An attempt was made to automatically clean a drive, but no usable cleaning media is available. Or the number of cleanings that remains for the cleaning tape is zero.

- Ensure that cleaning media was added to the robotic library for each drive type capable of being cleaned with a separate cleaning cartridge.

- Ensure that a positive number of cleanings is available for the cleaning media in the EMM database for the robotic library. Replace the cleaning tape or increase the number of cleanings for the cleaning media before the count reaches zero.

- Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 422.
Device management status code: 60
Message: Robot daemon and/or robotic hardware is not available
Explanation: A robot was not configured or was operationally unavailable. Specifically, an attempt may have been made to automatically clean a robotic drive, but the robot is not defined or is unavailable. Alternatively, on an attempt to initialize the shared drive lists, a drive was found to be configured as robotic, without the required robot configured.
Recommended Action: Display the device configuration and ensure that the drive and robotic configuration information are consistent. Check the operational status of the robot and robotic software by checking the system log files. If more detail on robot operational status is needed, increase the level of verbosity by adding the VERBOSE option in the `vm.conf` file. Then restart `ltid` (the device daemon /NetBackup Device Manager service).

Device management status code: 61
Message: No media found in device or robot slot, please verify
Explanation: On a request to mount media, no media was found in the targeted location before a designated time period had elapsed.
Recommended Action: Resubmit the request, and mount the media in the targeted drive before the designated time period has elapsed. Check the device configuration to ensure the following: that the correct drive name has been configured and that `ltid`, the device daemon, was restarted after the last device configuration change was made.

Device management status code: 62
Message: Drive not available in library for mount request
Explanation: A mount request has been canceled because no drive is available. All compatible drives may be DOWN, or oversubscribed due to other active mount requests.
Recommended Action: Investigate device availability and scheduling/drive utilization of applications requesting drive resources. Under some conditions, mount requests are canceled so that they can be reissued at a later time when compatible drive resources are available.

Device management status code: 63
Message: Request terminated because mount requests are disabled
Explanation: A mount request was canceled because it cannot be satisfied.
Recommended Action:

Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 422.

The detailed reason for the canceled request should be available in the system log, command output, or from a device monitor interface. Correct the problem and resubmit the request if needed.

Device management status code: 64

Message: Cannot assign a robotically controlled device

Explanation: An attempt was made to manually assign a specific device to satisfy a mount request, and the chosen device was configured in a robotic library.

Recommended Action: Assign the request to a standalone drive, or allow requests for mounts in robotic drives to be automatically assigned.

Device management status code: 65

Message: Invalid volume pool specified

Explanation: On a mount request, the media pool specified was not valid.

Recommended Action: Resubmit the request, specifying a volume pool name that is no more than 20 ASCII characters in length.

Device management status code: 66

Message: Request terminated because of volume pool mismatch

Explanation: The volume pool that is specified on the tpreq command did not match the volume pool in the Media Manager configuration for the media ID.

Recommended Action: Use a media management interface to obtain the volume pool name of the media that is to be mounted. Then resubmit the mount request, specifying the correct pool name.

Device management status code: 69

Message: Request terminated because media is unmountable

Explanation: A mount request has been canceled because the media being requested is not mountable. The same media has been found to be unmountable in at least two different drives.

- Check integrity of the drive, drive path, and media.
■ Verify that the media is not a misconfigured cleaning tape.

Device management status code: 70

Message: Request terminated because media is write protected

Explanation: A mount request has been canceled because the media being requested for write access is not write-enabled.

Recommended Action: Check the physical media cartridge to see whether write-protection has been enabled. If write access to the media is desired, disable write protection for the media.

If read-only access is desired, leave the write-protection enabled. Then make the necessary administrative requests in the requesting application (such as suspending the media) to ensure that the media is requested only for read access.

If the media was requested through the command line interface, see the \texttt{tpreq} man page or command description for specifying the media access mode. The \texttt{tpreq} command is described in the following manuals:

See the \textit{NetBackup Administrator's Guide, Volume II}.

See the \textit{NetBackup Commands} manual.

Device management status code: 71

Message: Request terminated because media is a cleaning tape

Explanation: A mount request has been canceled because the media that was found in the drive is a cleaning tape.

Recommended Action: Check to make sure the Media Manager’s EMM database is up-to-date. If there are cleaning media in the library, assign appropriate cleaning media types to them in the Media Manager EMM database.

Device management status code: 72

Message: EMM library call failed

Explanation: A request that was made to read/write data to EMM failed.

■ Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 422.

■ Verify that \texttt{pbx\_exchange} is running.

■ Run the \texttt{tpconfig -d} or \texttt{vmquery -a} command to verify that the EMM server is actively running and accepting new connections.
Device management status code: 73
Message: Stopping device daemon with tapes assigned
Explanation: An operator requested that ltid shutdown but tapes are still in use.
Recommended Action: None. This message is advisory and no action is required.

Device management status code: 74
Message: Robot operation failed
Explanation: A tape mount via bptm resulted in a failed robotic operation.
■ Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
■ Verify that the robotic hardware is functional.

Device management status code: 75
Message: LTI system error
Explanation: A system error occurred.
■ Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
■ A tpclean operation was attempted and Windows networking was not properly configured.
■ A malloc system call failed when trying to stop ltid.

Device management status code: 76
Message: Robot/LTI protocol error
Explanation: Communication between ltid and the robotic daemons caused a protocol error.
■ Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
■ Verify that ltid, bptm, and the robotic daemons are at a compatible NetBackup level.
Device management status code: 77
Message: VxSS access denied
Explanation: A user tried to run tpclean without adequate permissions.
- Verify that the user is logged in with permissions adequate for this operation.
- Verify that the VxSS settings are correct, under Host Properties in the NetBackup Administration Console.
  See the NetBackup Security and Encryption Guide.

Device management status code: 78
Message: Unable to connect to the EMM server
Explanation: An attempt to retrieve or update information in EMM failed.
- Verify that the correct EMM server name is listed in the NetBackup configuration.
- Verify that the media server that is encountering this error is listed in the NetBackup configuration on the EMM server.
- Verify that EMM is running on the EMM server.
- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.

Device management status code: 79
Message: Can not retrieve Job ID from Job Manager
Explanation: The tpreq, tpclean, or tpunmount command encountered an error while trying to get a job ID from the NetBackup Job Manager.
- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Verify that the NetBackup Job Manager is running on the master server.

Device management status code: 80
Message: Job Manager returned error: see activity monitor
Explanation: The tpunmount command encountered an error while communicating with the NetBackup Job Manager. The details of this issue may be found in the Activity Monitor entry for this job.
Examine command output, debug logs, and system logs for a more detailed message on the error.
See “Using debug logs” on page 422.

- Verify that the NetBackup Job Manager is running on the master server.
- Verify that the arguments provided to the tpunmount command are correct.

**Device management status code: 81**

**Message:** Retry later

**Explanation:** An attempt was made to use resources controlled by EMM. These resources were not available.

**Recommended Action:** Retry the command at a later time.

**Device management status code: 82**

**Message:** No drive available

**Explanation:** An attempt to use a drive was made but that drive was not available.

- Verify that the drive is not DOWN on the intended media server.
- Verify that the media server where the drive is found is ACTIVE.
- Retry the command with a different drive.

**Device management status code: 83**

**Message:** Media does not exist in database

**Explanation:** The requested media ID was not found in the EMM database.

- Verify that the requested media ID was entered correctly.
- Retry with a different media ID.

**Device management status code: 84**

**Message:** No Error on operation, sideband data only

**Explanation:** This is only an informational message.

**Recommended Action:** No action is required by the user.
Robotic status codes

Robotic daemons or processes issue these status codes. They are also issued by programs that call the robotic operations, such as the `vmchange` command and the media and device management user interfaces.

**Robotic status code: 200**

**Message:** STATUS_SUCCESS

**Explanation:** A robotic operation was successfully completed.

**Recommended Action:** None.

**Robotic status code: 201**

**Message:** Unable to open robotic path

The robotic library device could not be opened. The specific case could be one of the following:

- The robot device, path, or library name in the device configuration may not be valid.
- The configured robotic device may not exist.
- The robotic device may be incorrect, such as a UNIX and Linux device file that is not of a character special file format.
- The robotic daemon/process lock file could not be opened or a lock obtained.
- The open operation on the device or through the API interface (such as NDMP) failed.

1. Stop any robot test utilities that may be running, since they have the lock on the robotic device when they are active.
2. Check the configuration of the robot against the recommended configuration as indicated in the documentation for robot configuration.
3. Check the health of the robotic device by using a robot test utility, then close the test utility when finished.
4. Check for the existence and permissions of the lock file itself and the lock file directory, which is `/usr/openv/volmgr/misc/vmd.lock` (UNIX and Linux) or `install_path\Volmgr\misc\vmd.lock` (Windows). Create the directory/folder and adjust the permissions as needed so that the robotic daemon/process can use the lock file. Stop and restart `ltid` (the device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows).
Robotic status code: 202

**Message:** Unable to sense robotic device

An element of the robotic library device could not be sensed. The cause could be any of the following:

- The SCSI commands mode sense, mode select, or read element status (of slot, drive, transport, i/e element) may have failed.
- A network API-controlled library inventory request may have failed.
- The robotic daemon/process could not initialize a robotic database file.
- Check the configuration of the robot against the recommended configuration as indicated in the documentation for robot configuration.
- Check the health of the robotic device by using a robot test utility, then close the test utility when finished.
- Check for the existence and permissions of the temporary robotic database and the temporary database directory/folder, which is `/usr/openv/volmgr/misc/robotic_db` (UNIX and Linux) or `install_path\Volmgr\misc\robotic_db` (Windows). Create the directory/folder and adjust the permissions as needed so that the robotic daemon/process can create it or use it. Stop and restart `ltid` (the device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows).

Robotic status code: 203

**Message:** Timeout waiting for robotic command

**Explanation:** A robotic operation timed out: it did not return with a status before a designated time period elapsed.

- Stop any robot test utilities, since they have the lock on the robotic device when they are active, and can block other requests.
- Check whether excessive hardware retries have delayed the completion of a robotic command.
- Check to see whether the robotic device still functions. Use a robot test utility to send commands to the device to see whether it is responsive. Execute `vmps` to verify that no unexpected Media Manager processes are running. Some processes should remain running, but some processes that do not go away can indicate a more serious problem, such as a hung system call.

Robotic status code: 204

**Message:** Unable to initialize robot
**Explanation:** The robot could not be initialized. This generic status is used for many conditions.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Investigate the system log messages that are related to the specific error leading to the robot initialization failure.

**Robotic status code: 205**
**Message:** Robotic mount failure

**Explanation:** The robot could not mount media.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Investigate the system log messages that are related to the specific error leading to the media mount failure.

**Robotic status code: 206**
**Message:** Robotic dismount failure

**Explanation:** The robot could not dismount media.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Investigate the system log messages that are related to the specific error leading to the media dismount failure.

**Robotic status code: 207**
**Message:** Invalid command code

**Explanation:** A robotic operation was requested with improper options, when it was not supported, or a robotic operation encountered an incompatible device interface. There may be an incompatibility between components or versions of the product.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
Verify that all Media Manager binaries and user interfaces are at a compatible version level.

**Robotic status code: 208**

**Message:** Requested slot is empty

**Explanation:** No media was found in a specified slot. The volume configuration may not be consistent with the physical contents of the robotic library that is associated with the volume.

**Recommended Action:** Install or realign the container/holder for the media if it is misplaced or misaligned. Place media right-side-up in the slot if the media is upside-down. Check to see if the requested slot is reserved to the robotic library for internal use. Physically correct issues within the robotic library, or use a media management interface to correct the volume configuration.

**Robotic status code: 209**

**Message:** Unable to open drive

**Explanation:** The drive could not be opened. The drive configuration may be incorrect and the drive may be logically DOWN. Also, the drive may never have become ready after media was placed in the drive.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 422.
- Check for improperly configured cleaning media or interference with the drive cleaning operation. Check for bad media that may have led to the drive not becoming ready after media was placed within it.
- To avoid configuring incorrect device paths and device names, which is a common cause of drive open problems, do the following: use the Device Configuration wizard (on supported device discovery platforms) so that device paths and device names can be automatically configured. Investigate the system log messages that are related to the specific error leading to the open failure.

**Robotic status code: 210**

**Message:** Unable to SCSI unload drive

**Explanation:** The drive could not be unloaded. The drive configuration may be incorrect and the drive may be logically DOWN. Also, the drive may never have become ready after media was placed in the drive.
Examine command output, debug logs, and system logs for a more detailed message on the error.
See “Using debug logs” on page 422.

Check for improperly configured cleaning media or interference with the drive cleaning operation. Check for bad media that may prevent unloading the drive. To avoid configuring incorrect device paths and device names, which is a common cause of drive unload problems, do the following: use the Device Configuration wizard (on supported device discovery platforms) so that device paths and device names can be automatically configured. Investigate the system log messages that are related to the specific error leading to the unload failure.

**Robotic status code: 211**

**Message:** Process killed by signal

**Explanation:** An unexpected signal or event canceled the robotic operation.

Examine command output, debug logs, and system logs for a more detailed message on the error.
See “Using debug logs” on page 422.

Check vendor or operating system administrative interfaces and logs to see if robotic commands are being canceled.

**Robotic status code: 212**

**Message:** Process killed by parent

**Explanation:** A robotic operation was canceled because of one of the following: it did not return a status before a designated time period elapsed, or communications or hardware errors led to the need to reinitialize the device.

Stop any robot test utilities, since they have the lock on the robotic device when they are active, and can block other requests.

Check to see whether the robotic device still functions.

Check whether excessive hardware or communication problems have delayed the completion of a robotic command.

Use a robot test utility to send commands to the device to see whether it is responsive. Execute `vmps` to verify that no unexpected Media Manager processes are running. Some processes should remain running, but some processes that do not go away can indicate a problem, such as a hung system call.
Robotic status code: 213

Message: Drive does not exist in robot

Explanation: A targeted drive was not found in the robotic library. The drive configuration may be incorrect.

- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.
- Obtain the list of drives using a method that involves a robotic library query, such as a query available from the robot test utility. Compare the list of drives against the device configuration. Ensure that \texttt{ltid} was stopped and restarted after changes were last made to the device configuration. \texttt{ltid} is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.

Robotic status code: 214

Message: Robot number does not exist

Explanation: A targeted robotic library was not found in the active device configuration.

- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.
- Ensure that \texttt{ltid} was stopped and restarted after changes were last made to the device configuration. (\texttt{ltid} is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.) On commands to robotic libraries, specify only robotic libraries that are actively part of the device configuration.

Robotic status code: 215

Message: Requested tape in other or non-configured drive

Explanation: The targeted media was found in a drive differing from the targeted drive.

Requested media can be temporarily unavailable, which is normal. Also, media can remain unavailable until administrator or operator action is taken.

- If the media is needed immediately, examine command output (if available), debug logs, and system logs for messages relating to the targeted media. See “Using debug logs” on page 422.
Check for conflicts between multiple applications using media in the robotic library. Check integrity of the drive and drive paths, so that media is not routinely left in other drives.

**Robotic status code: 216**

**Message:** Door is open on cabinet

**Explanation:** The robotic library door was open.

**Recommended Action:** Close the door of the robotic library and reissue the robotic request. See if the door latch mechanism works by comparing what happens with robot test utility commands when the door is open versus closed.

**Robotic status code: 217**

**Message:** Requested slot already has cartridge

**Explanation:** The requested slot was already held or was associated with a cartridge.

**Recommended Action:** Ensure that the inject/eject request does not target a slot that already contains media. Check for media in drives to ensure that the media’s home slot location is not targeted for use with media to be injected.

**Robotic status code: 218**

**Message:** Cannot move from media access port to slot

**Explanation:** A robotic inject media operation returned a status indicating that an inject failure occurred.

- See whether the robotic library has a media access port (use the robot test utility to validate). Investigate whether the administrator or operator has canceled the inject operation.

- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.

**Robotic status code: 219**

**Message:** Cannot move from slot to media access port

**Explanation:** A robotic eject media operation returned a status indicating that an eject failure occurred.
See whether the robotic library has a media access port (use the robot test utility to validate). Investigate whether the administrator or operator has canceled the eject operation.

Examine command output, debug logs, and system logs for a more detailed message on the error.
See “Using debug logs” on page 422.

Robotic status code: 220
Message: Media access port does not contain media
Explanation: A robotic inject media operation returned a status indicating that the media access port does not contain any cartridges/media. The operator or administrator may not have placed media into the media access port for inject.

Examine command output, debug logs, and system logs for a more detailed message on the error.
See “Using debug logs” on page 422.

Coordinate inject/eject operations between all operators and administrators.

Robotic status code: 221
Message: Media access port already contains media
Explanation: A robotic eject media operation returned a status indicating that the media access port contains one or more cartridges. The operator or administrator may not have removed media from the media access port as part of the latest (or a previous) eject operation.

Examine command output, debug logs, and system logs for a more detailed message on the error.
See “Media Manager status codes” on page 422.

Coordinate inject/eject operations between all operators and administrators.
Ensure that the media access port is empty of media before an eject operation.

Robotic status code: 222
Message: Robotic arm has no addressable holder
Explanation: A holder is gone from an element of the robot and cannot be used.

Examine command output, debug logs, and system logs for a more detailed message on the error.
See “Using debug logs” on page 422.
- Investigate the state of the physical hardware and correct the holder status for storage, drive, and transport elements as needed. Then, resubmit the request.

**Robotic status code: 223**

**Message:** Robot busy, cannot perform operation

**Explanation:** The robot is busy performing another operation, using resources that are needed for the requested operation.

**Recommended Action:** Wait until the robot is done performing current external-based requests (including robot inventory and inject/eject media) before starting new requests. Check vendor or operating system administrative interfaces and logs to see if robotic resources are busy.

**Robotic status code: 224**

**Message:** Control daemon connect or protocol error

**Explanation:** A protocol error occurred between robotic and other components.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Investigate the system log messages that are related to the specific error leading to the media mount failure. Verify that all Media Manager binaries are at a compatible version level.

- Verify that robotic interfaces to vendor and operating system software have compatible versions.

**Robotic status code: 225**

**Message:** Robot hardware or communication error

**Explanation:** A hardware or communications error occurred between robotic and other components.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Investigate the system log messages that are related to the error leading to the media mount failure.
- Verify that all Media Manager binaries are at a compatible version level. Verify that robotic interfaces to vendor and operating system hardware and software have compatible versions.

**Robotic status code: 226**

**Message:** Requested slot contains the wrong tape

**Explanation:** The media in the requested slot is different from the media that is expected in that slot. The volume configuration is not consistent with the physical contents of the robotic library that is associated with the slot associated with the requested volume.

**Recommended Action:** The volume configuration or media placement in the robotic library needs to be adjusted using one of the media management interfaces. Determine whether the barcode changed or the media changed since the last time the EMM database was reconciled for the affected slot. If only the barcode has changed but not the media, issue an update barcode request for each affected volume. If the media has been changed, use a media management interface to run robot inventory update, which updates the EMM database with the media location.

**Robotic status code: 228**

**Message:** Requested slot does not exist in robot

**Explanation:** The slot that is associated with a request is not valid for the robot.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Issue a robot inventory Contents report to determine the valid slot range for the robot. Check the volume configuration to ensure that only valid slots are referenced in volume records, paying particular attention to the starting and ending slot numbers. Update the volume configuration as needed, or request only valid slot ranges for robotic operations.

**Robotic status code: 229**

**Message:** Requested operation is not supported by the robot

**Explanation:** A robotic operation was sent to a robotic component that did not support that operation. Or the options that were requested for the operation were not supported. There may be an incompatibility between components or versions of the product.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
See “Using debug logs” on page 422.

■ Verify that all Media Manager binaries and user interfaces are at a compatible version level.

**Robotic status code: 230**

**Message:** System error occurred during robot operation

**Explanation:** A robotic operation encountered a system error. This status code is used for generic system call failures within robotic daemons/processes.

■ Check for other error messages in the command or interface output to indicate which system call failed. Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 422.

■ Check the system application log for error and warning messages.

■ Verify that the system is not running out of virtual memory. If virtual memory is the problem, shut down unused applications or increase the amount of virtual memory. To increase virtual memory on Windows: display the Control Panel, double-click System, and on the Performance tab, set Virtual Memory to a higher value.

■ Verify that all product binaries are properly installed.

■ Verify that no unexpected Media Manager processes are running by executing `vmps`. Some processes should remain running, but some processes that do not go away could indicate a problem, such as a hung system call.

**Robotic status code: 232**

**Message:** Volume not found in library

**Explanation:** The requested media was not found in the robotic library. The media has been ejected or become inaccessible for some other reason.

■ Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 422.

■ Issue a robot inventory Contents report to obtain the list of media in the robotic library. See whether inventory filters have been enabled in the Media Manager configuration file. Inventory filters affect the contents of the media list returned from the robotic daemon or process. Use a robot test utility or an operating system/vendor administrative interface to verify the status of media, as needed. Update the volume configuration and search for the media if it was not in the robotic library, as needed, and resubmit the request.
Robotic status code: 233

**Message:** Volume is in library, but not in drive domain

**Explanation:** The media was in the robotic library, in a library domain that is inaccessible to the drives that are configured in the robot.

**Recommended Action:** Issue a robot inventory Contents report to obtain the list of media in the robotic library. Check the device configuration and ensure that the drive addresses correspond to the correct domain for the media. Correct the device configuration as needed and restart `ltid` (the device daemon on UNIX and Linux or NetBackup Device Manager service on Windows). Use a robot test utility or a vendor administrative interface to verify the status of media, as needed. Update the volume configuration and physically move the media into the robotic library, as needed, and resubmit the request.

Robotic status code: 234

**Message:** Robot denied access to the resource

**Explanation:** The media was found in the robotic library, but is denied access according to an established security policy.

**Recommended Action:** Issue a robot inventory Contents report to obtain the list of media in the robotic library. Use a vendor administrative interface to verify the status of media, as needed. Delete the media in the volume configuration, or make the volume accessible through a vendor administrative interface, as appropriate. Update the volume configuration, as needed, and resubmit the request.

Robotic status code: 235

**Message:** barcode label is unreadable

**Explanation:** The media was found in the robotic library, but it has an unreadable barcode label.

**Recommended Action:** Use the robot test utility or a vendor administrative interface to verify the status of media. Correct the label or replace the media as appropriate. Update the volume configuration, as needed, and resubmit the request.

Robotic status code: 236

**Message:** Robot has misplaced the media

**Explanation:** The requested media was known according to the vendor software managing the robotic library, but the media has been misplaced.

**Recommended Action:** Use a robot test utility or a vendor administrative interface to verify the status of media. Search for the media inside the robotic library.
Update the volume configuration and search for the media if it was not in the robotic library, as needed, and resubmit the request.

**Robotic status code: 237**

**Message:** Volume is in use

**Explanation:** The media was in use.

**Recommended Action:** Use the robot test utility or a vendor administrative interface to verify the status of media. Determine what applications may be using the media. Dismount the media if it is not being used. Wait for the media to become available, as needed.

**Robotic status code: 238**

**Message:** Requested drive is in an offline domain

**Explanation:** The drive that is targeted for a mount request was in a robotic library domain that is offline.

**Recommended Action:** Bring the robotic library domain (ACS Library Storage Module) back online. Or postpone use of drives in that domain until the domain can be brought back online.

**Robotic status code: 239**

**Message:** Requested volume is in an offline domain

**Explanation:** The volume that is targeted for a mount request was in a robotic library domain that is in the offline or offline pending state.

**Recommended Action:** Bring the robotic library domain (ACS Library Storage Module) back online. Or postpone use of media in that domain until the domain can be brought back online.

**Robotic status code: 240**

**Message:** A memory allocation attempt failed in the robotic daemon

**Explanation:** An attempt by the robotic control daemon to allocate memory has failed. This error may indicate serious memory problems on your media server.

**Recommended Action:** Stop all NetBackup Media Manager daemons. Consult the documentation for your operating system memory management tools to determine what remaining process is leaking memory, and stop that process. Restart the NetBackup Media Manager daemons. Free up memory by terminating unneeded processes that consume a lot of memory. Add more swap space or physical memory if necessary.
Robotic status code: 242

Message: Robot media access port does not exist

Explanation: the requested media access port was not valid for use with the targeted media.

Recommended Action: Use the robot test utility or a vendor administrative interface to verify the media access port address based on the location of the media. Choose a media access port that is valid, or let one be automatically selected, and retry the robotic operation.

Robotic status code: 243

Message: Cannot open/create the media access port status file

Explanation: A robotic daemon/process could not create or open a status file in the database directory/folder.

Recommended Action: Investigate why the robot status file in the directory /usr/openv/volmgr/database (UNIX and Linux) or folder install_path\Volmgr\database (Windows) cannot be created or opened. On Windows, check which account the NetBackup Device Manager service (and thus the robotic process) is running under. Compare it against the security properties of the database folder.

Robotic status code: 244

Message: The eject command was aborted by the user

Explanation: An administrator or operator canceled an eject media request.

Recommended Action: This error happens when an administrator or operator cancels an eject request. The request may have been canceled for a number of reasons: missing or faulty media, to allow the media access port to be used for other requests, or to perform the operation at a later time. Check with the administrator or operator for more information.

Robotic status code: 245

Message: Physical drive is not available

Explanation: A robotic mount operation could not be completed because physical drive resources are not available for the request. This error may result from an environment that is based on virtualized resources, such as one involving the Storagenet 6000 Storage Domain Manager (SN6000).

The SN6000 virtualizes tape drives. Some SN6000 configurations may have more logical drives than the number of physical drives (or equivalent resources) available
for drive requests. Also, the relationship between the number of logical drives and physical drives may change as hardware failures occur. NetBackup scheduling, drive allocation, and drive assignment algorithms can only determine logical drive availability. NetBackup attempts to fully utilize all configured and available logical drives. If the number of required logical drives exceeds the physical drives available, a NetBackup job may be started with insufficient drive resources. Instead of queueing the job in the scheduler, the job runs and encounters the resource issue when it makes an ACS tape mount request.

- Install the Shared Storage Option (SSO) license for mount requests to requeue when physical drive resources are not available.

- The number of drives that can be in use at any one time is limited. Configure backup windows so the different storage units that are tied to the same physical drives are active only at non-overlapping times. Increase the media mount timeout to avoid job failures when the job cannot get a physical drive due to the drives all being busy.

**Robotic status code: 246**

**Message:** Failed to find an available slot to inject to

**Explanation:** An attempt to inject a volume into a full library failed. This error should only occur when the library is full. Full means that all storage elements either contain media or have been assigned media that are currently mounted in a drive. Note that some libraries that support multiple media types restrict which type of media can be assigned to each storage element. In this case, this error might occur even if some of the storage elements in a library were not full. Since the empty storage elements may not match the media type for the media to inject, the library is full for this media type.

**Recommended Action:** Clear the media access port, then re-inventory the robot by doing a volume configuration update.

**Robotic status code: 249**

**Message:** Volume is in home slot

**Explanation:** Volume is currently in its home slot and ready for eject.

**Recommended Action:** None.

**Robotic status code: 250**

**Message:** Media access port is available

**Explanation:** Media access port is available for inject or eject.
Recommended Action: Begin inject or eject operation.

Robotic status code: 251
Message: Media access port is unavailable
Explanation: Media access port is not ready for inject or eject.
Recommended Action: Manually remove any media remaining in the robot’s media access port. If this status persists, check robotic console for errors.

Robotic status code: 252
Message: Media access port is in inject mode
Explanation: Media access port is ready to inject and is not available for eject.
Recommended Action: Complete inject operation.

Robotic status code: 253
Message: Media access port is in eject mode
Explanation: Media access port is ready to eject and is not available for inject.
Recommended Action: Complete eject operation.

Robotic status code: 254
Message: Robot busy, inventory operation in progress
Explanation: The robot is not available because it is performing an inventory, using resources that are needed for the requested operation.
Recommended Action: Wait until the robot is done performing the inventory before starting new requests. Check the vendor or operating system administrative interfaces and logs to see if robotic resources are busy.

Robotic status code: 255
Message: Robot busy, inject operation in progress
Explanation: The robot is not available because it is involved in an inject operation, using resources that are needed for the requested operation.
Recommended Action: Wait until the robot is done performing the inject operation before starting new requests. Check the vendor or operating system administrative interfaces and logs to see if robotic resources are busy.
Robotic status code: 256

**Message:** Robot busy, multiple eject operation in progress

**Explanation:** The robot is unavailable because a multiple eject is in progress, using resources that are needed for the requested operation.

**Recommended Action:** Wait until the robot is done performing the multiple eject operation before starting new requests. Check the vendor or operating system administrative interfaces and logs to see if robotic resources are busy.

Robotic status code: 257

**Message:** Robot busy, multiple inject operation in progress

**Explanation:** The robot is unavailable because a multiple inject is in progress, using resources that are needed for the requested operation.

**Recommended Action:** Wait until the robot is done performing the multiple inject operation before starting new requests. Check the vendor or operating system administrative interfaces and logs to see if robotic resources are busy.

Robotic status code: 258

**Message:** Cleaning/unknown media in drive

**Explanation:** A request to mount a tape failed because cleaning media was found in the drive.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Retry the operation once the drive cleaning has completed.

Robotic status code: 259

**Message:** Not authorized by VxSS

**Explanation:** A request was made to the robot daemons by an unauthorized user.

- Verify that the user has the necessary permissions to perform this operation.

- Verify that the authentication and authorization security settings are correct, under Host Properties in the NetBackup Administration Console. Information is available on using the Symantec Product Authentication and Authorization Service.

  See the *NetBackup Security and Encryption Guide*. 
Robotic status code: 260

Message: Robot busy, robot diagnostics in progress

Explanation: The requested robot is running a robot diagnostic.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Retry the operation when the robot diagnostic cycle is complete.

Robotic status code: 261

Message: EMM error

Explanation: A request that was made to read/write data to EMM failed.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Run the `tpconfig -d` or `vmquery -a` command to verify that the EMM server is actively processing commands.

Robotic status code: 262

Message: Configuration has changed, robot daemons and ltid need restarting

Explanation: A device configuration change has been made that is not reflected in the robotic daemon's run-time cache of the data.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Restart ltid and the robotics on this system or on the robot control host system.

Robotic error codes

These status codes are returned if a robotic daemon/process was started from the command line and an error occurs. For example, if the administrator executes the following:

```
/usr/openv/volmgr/bin/tl8d
```

and no robots are configured, the following may be returned:

```
TL8: No robots are configured
```
These status codes are also logged to the system log. Usually, robotic daemons/processes are not started from the command line, but are started automatically, as needed, when \texttt{ltid} starts.

**Robot Error status code: 1**

**Message:** You must be \texttt{ROOT} to start daemon

**Explanation:** A user other than root started a robotic daemon. This status applies to UNIX and Linux systems only.

**Recommended Action:** Log on as the root user before starting robotic daemons. Allow robotic daemons to be started automatically as needed by \texttt{ltid} (the device daemon).

**Robot Error status code: 2**

**Message:** LTI Daemon may not be running

**Explanation:** On an attempt to start a robotic daemon or process, an attempt to connect to the \texttt{ltid} message queue failed. This error indicates that \texttt{ltid} (the device daemon or NetBackup Device Manager service) may not be running.

- Start \texttt{ltid} so that shared memory can be initialized, allowing the robotic daemon/process to function.
- If problems persist, examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.
- On UNIX and Linux servers, gather the output of the \texttt{ipcs -a} command to see what resources are currently in use.

**Robot Error status code: 3**

**Message:** Error in getting shared memory

**Explanation:** A robotic daemon/process was unable to get a shared memory identifier associated with a segment of shared memory that \texttt{ltid} maintains. (\texttt{ltid} is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.)

- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.
- On UNIX and Linux servers, gather the output of the \texttt{ipcs -a} command to see what resources are currently in use.
Robot Error status code: 4

Message: Error in attaching the shared memory

Explanation: A robotic daemon/process was unable to attach a shared memory segment that \texttt{ltid} maintains. (\texttt{ltid} is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.)

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- On UNIX and Linux servers, gather the output of the \texttt{ipcs -a} command to see what resources are currently in use.

Robot Error status code: 5

Message: Error in getting process Id

Explanation: A robotic daemon/process was unable to obtain its own process identifier due to a system call failure.

Recommended Action: Investigate operating system functionality regarding a process obtaining its own process identifier.

Robot Error status code: 6

Message: No devices are configured on the robot

Explanation: A robotic daemon/process was started, but no drives are configured for the robot.

Recommended Action: Some robotic daemons or processes do not run if no drives are configured for them to manage. Add or reconfigure one or more drives to be in the associated robot. Then, stop and restart \texttt{ltid} (the Media Manager device daemon on UNIX and Linux or NetBackup Device Manager service on Windows).

Robot Error status code: 7

Message: No robots are configured

Explanation: A robotic daemon/process was started, but no robots of the associated robot type are configured.

Recommended Action: Robotic daemons or processes do not run if no robots are configured for the associated robot type. Add or reconfigure robots, then stop and restart \texttt{ltid} (the Media Manager device daemon on UNIX and Linux or NetBackup Device Manager service on Windows).
Robot Error status code: 8

Message: No memory available

Explanation: A robotic daemon/process was unable to allocate memory. This error occurs when insufficient system memory is available. This error could result from the system being overloaded with too many processes and from insufficient physical and virtual memory.

Recommended Action: Free up memory by terminating unneeded processes. Add more swap space or physical memory.

Robot Error status code: 9

Message: Error in SEMAPHORE operation

Explanation: A process was unable to perform a semaphore operation (such as lock or unlock) associated with resources maintained by ltid. (ltid is the Media Manager device daemon on UNIX and Linux or the NetBackup Device Manager service on Windows.)

- Examine command output, debug logs, and system logs for a more detailed message on the error. See “Using debug logs” on page 422.
- On UNIX and Linux servers, gather the output of the ipcs -a command to see what resources are currently in use.

Robot Error status code: 10

Message: Fork failure occurred

Explanation: A robotic daemon or process could not create a child process due to a system error. This error is probably intermittent, based on the availability of resources on the system (applies to UNIX and Linux servers only).

- Restart the device daemon at a later time and investigate system problems that limit the number of processes.
- Examine the system logs for a more detailed message on the error. See “Using debug logs” on page 422.
- Restart the device daemon, then retry the operation and examine the system log file.

Robot Error status code: 11

Message: System error occurred

Explanation: A robotic daemon/process encountered a system error.
**Recommended Action:** Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 422.

**Robot Error status code: 12**

**Message:** Usage error in creating child process

**Explanation:** A robotic daemon/process could not create a child process due to an incompatibility between robotic software components.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

- Verify that all Media Manager binaries are at a compatible version level.

**Robot Error status code: 13**

**Message:** EMM error

**Explanation:** The robotic daemon had a problem communicating with EMM.

- Make sure nbemmm is running and responding to requests.

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  
  See “Using debug logs” on page 422.

**Robot Error status code: 14**

**Message:** You must be administrator to execute

**Explanation:** A robotic process was started under a user account that lacks Administrator privileges (applies to Windows systems only).

**Recommended Action:** Allow robotic daemons to be started automatically as needed by the NetBackup Device Manager service. Ensure that this service starts from a user account with administrator privilege.

**Robot Error status code: 16**

**Message:** Devices located in multiple domains

**Explanation:** A robotic daemon or process encountered an invalid device configuration. In this configuration, a single logical robot controls drives from different domains.
**Recommended Action:** Display the device configuration using `tpconfig -d` or a device configuration interface to see the robotic and the drive information that is already configured. Ensure that the drive addresses do not span physical domains. Drives can only be configured in the same robot if they can be used with media from a single domain. The domain must include a single physical library or multiple libraries that are connected by a cartridge exchange or pass-through mechanism.

**Robot Error status code: 17**

**Message:** Robotic daemon not licensed

**Explanation:** A robotic daemon or process was started without the required, current product license, or a required database file was missing or corrupt.

- Check product documentation for supported device configurations.
- Obtain an additional software license that allows robots of the associated robot type to be configured. Or, limit the configuration to robot types that current licensing allows. Check for the existence and permissions of the `external_robotics.txt` file in the `/usr/openv/share` directory (UNIX and Linux) or in the `install_path\NetBackup\share` folder (Windows).

---

**Media and device management messages**

This topic can be used as a cross reference to the status code descriptions and recommended actions listed previously. Use the information in this topic if you know the error message itself, but don’t have access to the status code number.

Table 6-1 lists the NetBackup error messages alphabetically in the left column and the corresponding status code number in the right column.

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code number</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; NONE &gt;</td>
<td>Device Configuration status code 36</td>
</tr>
<tr>
<td>A memory allocation attempt failed in the robotic daemon</td>
<td>Robotic status code 240</td>
</tr>
<tr>
<td>a scratch pool is already defined</td>
<td>Media Manager status code 171</td>
</tr>
<tr>
<td>A SCSI inquiry sent to the device has failed</td>
<td>Device Configuration status code 16</td>
</tr>
<tr>
<td>ADAMM GUID does not exist in database</td>
<td>Media Manager status code 168</td>
</tr>
<tr>
<td>ADAMM GUID is not unique in the database</td>
<td>Media Manager status code 167</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code number</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>Add Drive Name Rule request failed</td>
<td>Device Configuration status code 82</td>
</tr>
<tr>
<td>Adding this device would exceed the maximum allowed</td>
<td>Device Configuration status code 40</td>
</tr>
<tr>
<td>Adding this drive would exceed the maximum allowed</td>
<td>Device Configuration status code 39</td>
</tr>
<tr>
<td>another daemon already exists</td>
<td>Media Manager status code 89</td>
</tr>
<tr>
<td>Another device configuration is already in progress</td>
<td>Device Configuration status code 90</td>
</tr>
<tr>
<td>barcode does not exist in database</td>
<td>Media Manager status code 78</td>
</tr>
<tr>
<td>barcode label is unreadable</td>
<td>Robotic status code 235</td>
</tr>
<tr>
<td>barcode not unique in database</td>
<td>Media Manager status code 36</td>
</tr>
<tr>
<td>barcode tag is not unique in rule database</td>
<td>Media Manager status code 122</td>
</tr>
<tr>
<td>cannot allocate requested memory</td>
<td>Media Manager status code 18</td>
</tr>
<tr>
<td>Cannot assign a robotically controlled device</td>
<td>Device management status code 64</td>
</tr>
<tr>
<td>Cannot assign due to media ID mismatch</td>
<td>Device management status code 57</td>
</tr>
<tr>
<td>cannot auto-eject this robot type</td>
<td>Media Manager status code 51</td>
</tr>
<tr>
<td>cannot auto-inject this robot type</td>
<td>Media Manager status code 52</td>
</tr>
<tr>
<td>Cannot change terminal mode</td>
<td>Device Configuration status code 41</td>
</tr>
<tr>
<td>cannot connect to robotic software daemon</td>
<td>Media Manager status code 42</td>
</tr>
<tr>
<td>cannot connect to vmd [on host host name]</td>
<td>Media Manager status code 70</td>
</tr>
<tr>
<td>Cannot create miscellaneous working repository</td>
<td>Device Configuration status code 42</td>
</tr>
<tr>
<td>cannot delete assigned volume</td>
<td>Media Manager status code 92</td>
</tr>
<tr>
<td>cannot delete one of the default volume pools</td>
<td>Media Manager status code 118</td>
</tr>
<tr>
<td>Cannot discover devices. See the Troubleshooting Guide for details.</td>
<td>Device Configuration status code 44</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code number</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Cannot execute command, permission denied</td>
<td>Device Configuration status code 1</td>
</tr>
<tr>
<td>cannot get host name</td>
<td>Media Manager status code 76</td>
</tr>
<tr>
<td>Cannot move from media access port to slot</td>
<td>Robotic status code 218</td>
</tr>
<tr>
<td>Cannot move from slot to media access port</td>
<td>Robotic status code 219</td>
</tr>
<tr>
<td>cannot obtain daemon lockfile</td>
<td>Media Manager status code 21</td>
</tr>
<tr>
<td>Cannot open/create the media access port status file</td>
<td>Robotic status code 243</td>
</tr>
<tr>
<td>cannot perform operation on this host</td>
<td>Media Manager status code 60</td>
</tr>
<tr>
<td>Can not retrieve Job ID from Job Manager</td>
<td>Device management status code 79</td>
</tr>
<tr>
<td>Cannot stop device daemon with tapes assigned</td>
<td>Device management status code 20</td>
</tr>
<tr>
<td>cannot update database due to existing errors</td>
<td>Media Manager status code 80</td>
</tr>
<tr>
<td>child process killed by signal</td>
<td>Media Manager status code 63</td>
</tr>
<tr>
<td>Cleaning/unknown media in drive</td>
<td>Robotic status code 258</td>
</tr>
<tr>
<td>Configuration has changed, robot daemons and ltid need restarting</td>
<td>Robotic status code 262</td>
</tr>
<tr>
<td>Control daemon connect or protocol error</td>
<td>Robotic status code 224</td>
</tr>
<tr>
<td>CORBA communication error</td>
<td>Media Manager status code 195</td>
</tr>
<tr>
<td>Could not get hostname</td>
<td>Device Configuration status code 3</td>
</tr>
<tr>
<td>Credentials already exist</td>
<td>Device configuration status code 99</td>
</tr>
<tr>
<td>Current version does not support remote device host</td>
<td>Device Configuration status code 38</td>
</tr>
<tr>
<td>current version does not support this configuration</td>
<td>Media Manager status code 149</td>
</tr>
<tr>
<td>daemon cannot obtain socket</td>
<td>Media Manager status code 58</td>
</tr>
<tr>
<td>daemon failed accepting connection</td>
<td>Media Manager status code 59</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code number</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>daemon resources are busy</td>
<td>Media Manager status code 5</td>
</tr>
<tr>
<td>daemon terminated</td>
<td>Media Manager status code 7</td>
</tr>
<tr>
<td>database open operation failed</td>
<td>Media Manager status code 26</td>
</tr>
<tr>
<td>database read operation read too few bytes</td>
<td>Media Manager status code 28</td>
</tr>
<tr>
<td>database read record operation failed</td>
<td>Media Manager status code 27</td>
</tr>
<tr>
<td>database server is down</td>
<td>Media Manager status code 23 and Device Configuration status code 93</td>
</tr>
<tr>
<td>database write record operation failed</td>
<td>Media Manager status code 32</td>
</tr>
<tr>
<td>Delete Drive Name Rule request failed</td>
<td>Device Configuration status code 84</td>
</tr>
<tr>
<td>device entry is not unique in global device database</td>
<td>Media Manager status code 153</td>
</tr>
<tr>
<td>device management error</td>
<td>Media Manager status code 83</td>
</tr>
<tr>
<td>Device path is already in use</td>
<td>Device Configuration status code 22</td>
</tr>
<tr>
<td>device test state file does not exist</td>
<td>Media Manager status code 182</td>
</tr>
<tr>
<td>Devices located in multiple domains</td>
<td>Robot Error status code 16</td>
</tr>
<tr>
<td>Disk Optimization feature is not licensed</td>
<td>Device Configuration status code 94</td>
</tr>
<tr>
<td>Door is open on cabinet</td>
<td>Robotic status code 216</td>
</tr>
<tr>
<td>Drive being assigned is either not NDMP or on the wrong NDMP client</td>
<td>Device management status code 37</td>
</tr>
<tr>
<td>Drive does not exist in robot</td>
<td>Robotic status code 213</td>
</tr>
<tr>
<td>Drive does not support pending request density</td>
<td>Device management status code 17</td>
</tr>
<tr>
<td>Drive index is in use by another drive</td>
<td>Device Configuration status code 29</td>
</tr>
<tr>
<td>Drive is currently assigned</td>
<td>Device management status code 2</td>
</tr>
<tr>
<td>Drive name does not exist</td>
<td>Device Configuration status code 35</td>
</tr>
<tr>
<td>Drive name is already in use by another drive</td>
<td>Device Configuration status code 34</td>
</tr>
</tbody>
</table>
### Table 6-1: Media and device management messages and status codes (continued)

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive name rule has exceeded its maximum length of 48 characters</td>
<td>Device Configuration status code 89</td>
</tr>
<tr>
<td>Drive not available in library for mount request</td>
<td>Device management status code 62</td>
</tr>
<tr>
<td>Duplicate device path names</td>
<td>Device Configuration status code 20</td>
</tr>
<tr>
<td>EMM database error</td>
<td>Media Manager status code 196</td>
</tr>
<tr>
<td>EMM DB record not found</td>
<td>Media Manager status code 194</td>
</tr>
<tr>
<td>EMM error</td>
<td>Robotic status code 261 and Robot Error status code 13</td>
</tr>
<tr>
<td>EMM library call failed</td>
<td>Device management status code 72</td>
</tr>
<tr>
<td>error auto-generating volume group</td>
<td>Media Manager status code 57</td>
</tr>
<tr>
<td>Error in attaching the shared memory</td>
<td>Robot Error status code 4</td>
</tr>
<tr>
<td>Error in getting process Id</td>
<td>Robot Error status code 5</td>
</tr>
<tr>
<td>Error in getting semaphore</td>
<td>Device management status code 32</td>
</tr>
<tr>
<td>Error in getting shared memory</td>
<td>Robot Error status code 3</td>
</tr>
<tr>
<td>Error in IPC SHMAT call</td>
<td>Device management status code 14</td>
</tr>
<tr>
<td>Error in IPC SHMGET call</td>
<td>Device management status code 13</td>
</tr>
<tr>
<td>Error in MsgGet</td>
<td>Device management status code 28</td>
</tr>
<tr>
<td>Error in Receiving Daemon Message</td>
<td>Device management status code 6</td>
</tr>
<tr>
<td>Error in Receiving Operator Message</td>
<td>Device management status code 4</td>
</tr>
<tr>
<td>Error in Receiving User Message</td>
<td>Device management status code 8</td>
</tr>
<tr>
<td>Error in SEMAPHORE operation</td>
<td>Device management status code 33</td>
</tr>
<tr>
<td>Error in SEMAPHORE operation</td>
<td>Robot Error status code 9</td>
</tr>
<tr>
<td>Error in Sending Daemon Message</td>
<td>Device management status code 5</td>
</tr>
<tr>
<td>Error in Sending Operator Message</td>
<td>Device management status code 3</td>
</tr>
<tr>
<td>Error in Sending User Message</td>
<td>Device management status code 7</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code number</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Evaluation period expired. Go to <a href="http://www.symantec.com">www.symantec.com</a> to order this product.</td>
<td>Media Manager status code 165</td>
</tr>
<tr>
<td>failed appending to pool database</td>
<td>Media Manager status code 104</td>
</tr>
<tr>
<td>failed appending to rule database</td>
<td>Media Manager status code 121</td>
</tr>
<tr>
<td>failed changing terminal characteristics</td>
<td>Media Manager status code 45</td>
</tr>
<tr>
<td>failed initiating child process</td>
<td>Media Manager status code 88</td>
</tr>
<tr>
<td>failed making the database directory</td>
<td>Media Manager status code 25</td>
</tr>
<tr>
<td>failed opening tmp output file</td>
<td>Media Manager status code 86</td>
</tr>
<tr>
<td>Failed reading drive or robot config file</td>
<td>Device Configuration status code 13</td>
</tr>
<tr>
<td>failed receiving from robotic software daemon</td>
<td>Media Manager status code 44</td>
</tr>
<tr>
<td>failed receiving from vmd</td>
<td>Media Manager status code 72</td>
</tr>
<tr>
<td>failed redirecting input to pipe</td>
<td>Media Manager status code 62</td>
</tr>
<tr>
<td>failed redirecting tmp output file</td>
<td>Media Manager status code 87</td>
</tr>
<tr>
<td>failed sending request to vmd</td>
<td>Media Manager status code 69</td>
</tr>
<tr>
<td>failed sending to robotic software daemon</td>
<td>Media Manager status code 43</td>
</tr>
<tr>
<td>failed sending to vmd</td>
<td>Media Manager status code 71</td>
</tr>
<tr>
<td>Failed to find an available slot to inject to</td>
<td>Robotic status code 246</td>
</tr>
<tr>
<td>failed to initialize a connection to the Enterprise Media Manager</td>
<td>Media Manager status code 189</td>
</tr>
<tr>
<td>File name already exists</td>
<td>Device management status code 40</td>
</tr>
<tr>
<td>File name does not exist</td>
<td>Device management status code 25</td>
</tr>
<tr>
<td>Fork failure occurred</td>
<td>Robot Error status code 10</td>
</tr>
<tr>
<td>generic EMM SQL error</td>
<td>Media Manager status code 193</td>
</tr>
<tr>
<td>global device database append operation failed</td>
<td>Media Manager status code 155</td>
</tr>
</tbody>
</table>
### Table 6-1

**Media and device management messages and status codes (continued)**

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code number</th>
</tr>
</thead>
<tbody>
<tr>
<td>global device database host name is invalid</td>
<td>Device Configuration status code 49</td>
</tr>
<tr>
<td>global device database record not found</td>
<td>Media Manager status code 152</td>
</tr>
<tr>
<td>Host is not the scan host for this shared drive</td>
<td>Device management status code 48</td>
</tr>
<tr>
<td>incompatible database version</td>
<td>Media Manager status code 146</td>
</tr>
<tr>
<td>Incomplete robot information</td>
<td>Device Configuration status code 24</td>
</tr>
<tr>
<td>Incorrect tpreq access mode</td>
<td>Device management status code 42</td>
</tr>
<tr>
<td>internal database access failure</td>
<td>Media Manager status code 169</td>
</tr>
<tr>
<td>Internal NDMP error</td>
<td>Device Configuration status code 57</td>
</tr>
<tr>
<td>invalid barcode</td>
<td>Media Manager status code 10</td>
</tr>
<tr>
<td>invalid change type</td>
<td>Media Manager status code 75</td>
</tr>
<tr>
<td>invalid change-entry request</td>
<td>Media Manager status code 50</td>
</tr>
<tr>
<td>Invalid command code</td>
<td>Robotic status code 207</td>
</tr>
<tr>
<td>invalid command usage.</td>
<td>Media Manager status code 4</td>
</tr>
<tr>
<td>invalid container id.</td>
<td>Media Manager status code 186</td>
</tr>
<tr>
<td>invalid database host.</td>
<td>Media Manager status code 19</td>
</tr>
<tr>
<td>invalid database version header</td>
<td>Media Manager status code 56</td>
</tr>
<tr>
<td>invalid description</td>
<td>Media Manager status code 11</td>
</tr>
<tr>
<td>Invalid device path name</td>
<td>Device Configuration status code 19</td>
</tr>
<tr>
<td>Invalid drive index</td>
<td>Device Configuration status code 14</td>
</tr>
<tr>
<td>invalid drive name</td>
<td>Media Manager status code 129</td>
</tr>
<tr>
<td>Invalid Drive Name Rule</td>
<td>Device Configuration status code 86</td>
</tr>
<tr>
<td>Invalid Drive Number</td>
<td>Device management status code 23</td>
</tr>
<tr>
<td>Invalid drive type for the robot</td>
<td>Device Configuration status code 27</td>
</tr>
<tr>
<td>Invalid Drive Type/Density</td>
<td>Device management status code 1</td>
</tr>
</tbody>
</table>
### Table 6-1

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code number</th>
</tr>
</thead>
<tbody>
<tr>
<td>invalid EMM argument</td>
<td>Media Manager status code 191</td>
</tr>
<tr>
<td>invalid expiration date</td>
<td>Media Manager status code 113</td>
</tr>
<tr>
<td>Invalid host</td>
<td>Device Configuration status code 88</td>
</tr>
<tr>
<td>invalid host name</td>
<td>Media Manager status code 136</td>
</tr>
<tr>
<td>invalid maximum mounts</td>
<td>Media Manager status code 114</td>
</tr>
<tr>
<td>invalid media generation rule</td>
<td>Media Manager status code 140</td>
</tr>
<tr>
<td>invalid media ID for naming mode</td>
<td>Media Manager status code 41</td>
</tr>
<tr>
<td>invalid media ID</td>
<td>Media Manager status code 8</td>
</tr>
<tr>
<td>invalid media type</td>
<td>Media Manager status code 9</td>
</tr>
<tr>
<td>Invalid NDMP device</td>
<td>Device Configuration status code 64</td>
</tr>
<tr>
<td>Invalid NDMP hostname</td>
<td>Device Configuration status code 55</td>
</tr>
<tr>
<td>Invalid NDMP password</td>
<td>Device Configuration status code 60</td>
</tr>
<tr>
<td>invalid number of cleanings</td>
<td>Media Manager status code 74</td>
</tr>
<tr>
<td>invalid number of mounts</td>
<td>Media Manager status code 141</td>
</tr>
<tr>
<td>invalid offsite location</td>
<td>Media Manager status code 142</td>
</tr>
<tr>
<td>invalid offsite return date</td>
<td>Media Manager status code 144</td>
</tr>
<tr>
<td>invalid offsite sent date</td>
<td>Media Manager status code 143</td>
</tr>
<tr>
<td>invalid offsite session id</td>
<td>Media Manager status code 148</td>
</tr>
<tr>
<td>invalid offsite slot</td>
<td>Media Manager status code 147</td>
</tr>
<tr>
<td>Invalid Operator</td>
<td>Device management status code 12</td>
</tr>
<tr>
<td>invalid pool database entry</td>
<td>Media Manager status code 102</td>
</tr>
<tr>
<td>invalid protocol request</td>
<td>Media Manager status code 6</td>
</tr>
<tr>
<td>invalid query type</td>
<td>Media Manager status code 73</td>
</tr>
<tr>
<td>invalid robot coord1</td>
<td>Media Manager status code 16</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code number</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>invalid robot coord2</td>
<td>Media Manager status code 17</td>
</tr>
<tr>
<td>Invalid robot drive number for the robot type</td>
<td>Device Configuration status code 28</td>
</tr>
<tr>
<td>invalid robot host</td>
<td>Media Manager status code 14</td>
</tr>
<tr>
<td>Invalid robot number</td>
<td>Device Configuration status code 15</td>
</tr>
<tr>
<td>invalid robot number</td>
<td>Media Manager status code 13</td>
</tr>
<tr>
<td>Invalid robot type</td>
<td>Device Configuration status code 18</td>
</tr>
<tr>
<td>invalid robot type</td>
<td>Media Manager status code 12</td>
</tr>
<tr>
<td>invalid rule database entry</td>
<td>Media Manager status code 119</td>
</tr>
<tr>
<td>invalid scratch pool name</td>
<td>Media Manager status code 173</td>
</tr>
<tr>
<td>Invalid SCSI bus number for the robot</td>
<td>Device Configuration status code 8</td>
</tr>
<tr>
<td>Invalid SCSI logical unit number for the robot</td>
<td>Device Configuration status code 10</td>
</tr>
<tr>
<td>Invalid SCSI port number for the robot</td>
<td>Device Configuration status code 7</td>
</tr>
<tr>
<td>Invalid SCSI target for the robot</td>
<td>Device Configuration status code 9</td>
</tr>
<tr>
<td>Invalid Usage</td>
<td>Device Configuration status code 11</td>
</tr>
<tr>
<td>invalid volgroup</td>
<td>Media Manager status code 15</td>
</tr>
<tr>
<td>invalid volume move mode</td>
<td>Media Manager status code 53</td>
</tr>
<tr>
<td>Invalid volume pool specified</td>
<td>Device management status code 65</td>
</tr>
<tr>
<td>invalid volume pool</td>
<td>Media Manager status code 90</td>
</tr>
<tr>
<td>IPC Error: Daemon may not be running</td>
<td>Device management status code 22</td>
</tr>
<tr>
<td>IPC sequence error</td>
<td>Device management status code 10</td>
</tr>
<tr>
<td>Job Manager returned error: see activity monitor</td>
<td>Device management status code 80</td>
</tr>
<tr>
<td>List Drive Name Rule request failed</td>
<td>Device Configuration status code 85</td>
</tr>
<tr>
<td>LTI Daemon may not be running</td>
<td>Robot Error status code 2</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code number</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>LTI system error</td>
<td>Device management status code 75</td>
</tr>
<tr>
<td>Media access port already contains media</td>
<td>Robotic status code 221</td>
</tr>
<tr>
<td>Media access port does not contain media</td>
<td>Robotic status code 220</td>
</tr>
<tr>
<td>Media access port is available</td>
<td>Robotic status code 250</td>
</tr>
<tr>
<td>Media access port is in eject mode</td>
<td>Robotic status code 253</td>
</tr>
<tr>
<td>Media access port is in inject mode</td>
<td>Robotic status code 252</td>
</tr>
<tr>
<td>Media access port is unavailable</td>
<td>Robotic status code 251</td>
</tr>
<tr>
<td>media access port not available</td>
<td>Media Manager status code 166</td>
</tr>
<tr>
<td>Media does not exist in database</td>
<td>Device management status code 83</td>
</tr>
<tr>
<td>media generation rule already exists</td>
<td>Media Manager status code 138</td>
</tr>
<tr>
<td>media generation rule does not exist</td>
<td>Media Manager status code 139</td>
</tr>
<tr>
<td>media ID is not the specified media type</td>
<td>Media Manager status code 95</td>
</tr>
<tr>
<td>media ID not unique in database</td>
<td>Media Manager status code 34</td>
</tr>
<tr>
<td>media type and volume group mismatch</td>
<td>Media Manager status code 101</td>
</tr>
<tr>
<td>Mount canceled, device daemon is terminating</td>
<td>Device management status code 56</td>
</tr>
<tr>
<td>NDMP authorization error, verify username/password</td>
<td>Device Configuration status code 74</td>
</tr>
<tr>
<td>NDMP config_get_connection_type failed</td>
<td>Device Configuration status code 76</td>
</tr>
<tr>
<td>NDMP config_get_mover_type failed</td>
<td>Device Configuration status code 75</td>
</tr>
<tr>
<td>NDMP failed to verify host</td>
<td>Device Configuration status code 58</td>
</tr>
<tr>
<td>NDMP get_host_info failed</td>
<td>Device Configuration status code 71</td>
</tr>
<tr>
<td>NDMP get_server_info failed</td>
<td>Device Configuration status code 72</td>
</tr>
<tr>
<td>NDMP host does not exist</td>
<td>Device Configuration status code 62</td>
</tr>
<tr>
<td>NDMP host exists, use change option</td>
<td>Device Configuration status code 61</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code number</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>NDMP host not connected</td>
<td>Device Configuration status code 69</td>
</tr>
<tr>
<td>NDMP is not installed on platform</td>
<td>Device Configuration status code 59</td>
</tr>
<tr>
<td>NDMP request failed</td>
<td>Device Configuration status code 63</td>
</tr>
<tr>
<td>NDMP robot does not exist</td>
<td>Device Configuration status code 66</td>
</tr>
<tr>
<td>NDMP robot exists, use change option</td>
<td>Device Configuration status code 65</td>
</tr>
<tr>
<td>NetApp Disk Storage Unit feature is not licensed</td>
<td>Device configuration status code 94</td>
</tr>
<tr>
<td>NetBackup Snapshot client not licensed</td>
<td>Device configuration status code 100</td>
</tr>
<tr>
<td>network protocol error</td>
<td>Media Manager status code 39</td>
</tr>
<tr>
<td>No action pending for given mount index</td>
<td>Device management status code 50</td>
</tr>
<tr>
<td>no child process to wait for</td>
<td>Media Manager status code 64</td>
</tr>
<tr>
<td>No cleaning tape is defined in the device's robot or 0 cleanings remaining</td>
<td>Device management status code 59</td>
</tr>
<tr>
<td>No compatible device is registered at these SCSI coordinates</td>
<td>Device Configuration status code 51</td>
</tr>
<tr>
<td>No devices are configured on the robot</td>
<td>Robot Error status code 6</td>
</tr>
<tr>
<td>No drive available</td>
<td>Device management status code 82</td>
</tr>
<tr>
<td>no entries changed</td>
<td>Media Manager status code 47</td>
</tr>
<tr>
<td>no entries deleted</td>
<td>Media Manager status code 48</td>
</tr>
<tr>
<td>no entries inserted</td>
<td>Media Manager status code 49</td>
</tr>
<tr>
<td>No Error on operation, sideband data only</td>
<td>Device management status code 84</td>
</tr>
<tr>
<td>No media found in device or robot slot, please verify</td>
<td>Device management status code 61</td>
</tr>
<tr>
<td>No memory available</td>
<td>Robot Error status code 8</td>
</tr>
<tr>
<td>No mount pending for given mount index</td>
<td>Device management status code 16</td>
</tr>
<tr>
<td>no pools in the pool list</td>
<td>Media Manager status code 112</td>
</tr>
</tbody>
</table>
Table 6-1  Media and device management messages and status codes

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robot daemon and/or robotic hardware is not available</td>
<td>Device management status code 60</td>
</tr>
<tr>
<td>No robot is defined of this type</td>
<td>Device management status code 52</td>
</tr>
<tr>
<td>No robots are configured</td>
<td>Robot Error status code 7</td>
</tr>
<tr>
<td>No valid license key for Disk Array configuration</td>
<td>Device Configuration status code 97</td>
</tr>
<tr>
<td>&lt;NONE&gt;</td>
<td>Device Configuration status code 36</td>
</tr>
<tr>
<td>Not authorized by VxSS</td>
<td>Robotic status code 259</td>
</tr>
<tr>
<td>not authorized to connect to vmd</td>
<td>Media Manager status code 126</td>
</tr>
<tr>
<td>Only the administrative user can perform the requested operation</td>
<td>Device management status code 19</td>
</tr>
<tr>
<td>Open Storage feature is not licensed</td>
<td>Device configuration status code 98</td>
</tr>
<tr>
<td>operation not allowed on cleaning cartridge</td>
<td>Media Manager status code 117</td>
</tr>
<tr>
<td>Operator denied mount request</td>
<td>Device management status code 55</td>
</tr>
<tr>
<td>oprd request is not supported on the remote host</td>
<td>Media Manager status code 137</td>
</tr>
<tr>
<td>oprd returned abnormal status</td>
<td>Media Manager status code 96</td>
</tr>
<tr>
<td>Parameter is invalid</td>
<td>Device management status code 39</td>
</tr>
<tr>
<td>Physical drive is not available</td>
<td>Robotic status code 245</td>
</tr>
<tr>
<td>pool does not exist in pool database</td>
<td>Media Manager status code 109</td>
</tr>
<tr>
<td>poolname is not unique in pool database</td>
<td>Media Manager status code 105</td>
</tr>
<tr>
<td>pool not defined as a catalog backup pool</td>
<td>Media Management status code 198</td>
</tr>
<tr>
<td>pool not defined as a scratch pool</td>
<td>Media Manager status code 172</td>
</tr>
<tr>
<td>pool type change is not allowed for &lt;CatalogBackup&gt; pool</td>
<td>Media Manager status code 22</td>
</tr>
<tr>
<td>Process killed by parent</td>
<td>Robotic status code 212</td>
</tr>
</tbody>
</table>
Table 6-1  Media and device management messages and status codes (continued)

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process killed by signal</td>
<td>Robotic status code 211</td>
</tr>
<tr>
<td>protocol error</td>
<td>Media Manager status code 20</td>
</tr>
<tr>
<td>registering this host would exceed the maximum allowed</td>
<td>Media Manager status code 150</td>
</tr>
<tr>
<td>request can only be performed on the Media and Device management Domain Server</td>
<td>Media Manager status code 177</td>
</tr>
<tr>
<td>request completed</td>
<td>Media Manager status code 1</td>
</tr>
<tr>
<td>Request has been queued (Cancel to clear message)</td>
<td>Device management status code 53</td>
</tr>
<tr>
<td>Request terminated because host not validated for volume pool</td>
<td>Device management status code 26</td>
</tr>
<tr>
<td>Request terminated because media id is expired</td>
<td>Device management status code 27</td>
</tr>
<tr>
<td>Request terminated because <em>media id</em> will exceed maximum mount count</td>
<td>Device management status code 30</td>
</tr>
<tr>
<td>Request terminated because media is a cleaning tape</td>
<td>Device management status code 71</td>
</tr>
<tr>
<td>Request terminated because media is unavailable (in DOWN drive, misplaced,</td>
<td>Device management status code 35</td>
</tr>
<tr>
<td>write protected or unmountable)</td>
<td></td>
</tr>
<tr>
<td>Request terminated because media is unmountable</td>
<td>Device management status code 69</td>
</tr>
<tr>
<td>Request terminated because media is write protected</td>
<td>Device management status code 70</td>
</tr>
<tr>
<td>Request terminated because mount requests are disabled</td>
<td>Device management status code 63</td>
</tr>
<tr>
<td>Request terminated because of volume pool mismatch</td>
<td>Device management status code 66</td>
</tr>
<tr>
<td>Request terminated by tpunmount call from another process</td>
<td>Device management status code 36</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code number</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>Requested drive could not be reserved</td>
<td>Device management status code 24</td>
</tr>
<tr>
<td>requested drive is already reserved by host</td>
<td>Media Manager status code 145</td>
</tr>
<tr>
<td>requested drive is already reserved</td>
<td>Media Manager status code 130</td>
</tr>
<tr>
<td>Requested drive is in an offline domain</td>
<td>Robotic status code 238</td>
</tr>
<tr>
<td>requested drive is not currently registered</td>
<td>Media Manager status code 132</td>
</tr>
<tr>
<td>requested drive is not currently reserved</td>
<td>Media Manager status code 134</td>
</tr>
<tr>
<td>requested drive is not registered for host</td>
<td>Media Manager status code 131</td>
</tr>
<tr>
<td>requested drive is not reserved by host</td>
<td>Media Manager status code 133</td>
</tr>
<tr>
<td>requested host is not currently registered</td>
<td>Media Manager status code 135</td>
</tr>
<tr>
<td>Requested operation is not supported by the robot</td>
<td>Robotic status code 229</td>
</tr>
<tr>
<td>Requested slot already has cartridge</td>
<td>Robotic status code 217</td>
</tr>
<tr>
<td>Requested slot contains the wrong tape</td>
<td>Robotic status code 226</td>
</tr>
<tr>
<td>Requested slot does not exist in robot</td>
<td>Robotic status code 228</td>
</tr>
<tr>
<td>Requested slot is empty</td>
<td>Robotic status code 208</td>
</tr>
<tr>
<td>Requested tape in other or non-configured drive</td>
<td>Robotic status code 215</td>
</tr>
<tr>
<td>Requested volume is in an offline domain</td>
<td>Robotic status code 239</td>
</tr>
<tr>
<td>Residence is not licensed for multihosted drive support</td>
<td>Device Configuration status code 37</td>
</tr>
<tr>
<td>Retry later</td>
<td>Device management status code 81</td>
</tr>
<tr>
<td>Robot busy, cannot perform operation</td>
<td>Robotic status code 223</td>
</tr>
<tr>
<td>Robot busy, inject operation in progress</td>
<td>Robotic status code 255</td>
</tr>
<tr>
<td>Robot busy, inventory operation in progress</td>
<td>Robotic status code 254</td>
</tr>
<tr>
<td>Robot busy, multiple eject operation in progress</td>
<td>Robotic status code 256</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code number</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Robot busy, multiple inject operation in progress</td>
<td>Robotic status code 257</td>
</tr>
<tr>
<td>Robot busy, robot diagnostics in progress</td>
<td>Robotic status code 260</td>
</tr>
<tr>
<td>Robot denied access to the resource</td>
<td>Robotic status code 234</td>
</tr>
<tr>
<td>Robot drive number in use for this robot</td>
<td>Device Configuration status code 25</td>
</tr>
<tr>
<td>Robot hardware or communication error</td>
<td>Robotic status code 225</td>
</tr>
<tr>
<td>Robot has misplaced the media</td>
<td>Robotic status code 236</td>
</tr>
<tr>
<td>robot host and volume group mismatch</td>
<td>Media Manager status code 82</td>
</tr>
<tr>
<td>Robot/LTI protocol error</td>
<td>Device management status code 76</td>
</tr>
<tr>
<td>Robot media access port does not exist</td>
<td>Robotic status code 242</td>
</tr>
<tr>
<td>robot number and robot host mismatch</td>
<td>Media Manager status code 61</td>
</tr>
<tr>
<td>robot number and robot type mismatch</td>
<td>Media Manager status code 54</td>
</tr>
<tr>
<td>robot number and volume group mismatch</td>
<td>Media Manager status code 55</td>
</tr>
<tr>
<td>Robot number does not exist</td>
<td>Device Configuration status code 31</td>
</tr>
<tr>
<td>Robot number does not exist.</td>
<td>Robotic status code 214</td>
</tr>
<tr>
<td>Robot number is already in use</td>
<td>Device Configuration status code 21</td>
</tr>
<tr>
<td>Robot number is in use by another robot</td>
<td>Device Configuration status code 30</td>
</tr>
<tr>
<td>Robot operation failed</td>
<td>Device management status code 74</td>
</tr>
<tr>
<td>robot type and volume group mismatch</td>
<td>Media Manager status code 81</td>
</tr>
<tr>
<td>Robot type must be controlled locally</td>
<td>Device Configuration status code 33</td>
</tr>
<tr>
<td>Robotic arm has no addressable holder</td>
<td>Robotic status code 222</td>
</tr>
<tr>
<td>Robotic daemon not licensed</td>
<td>Robot Error status code 17</td>
</tr>
<tr>
<td>Robotic dismount failure</td>
<td>Robotic status code 206</td>
</tr>
<tr>
<td>Robotic mount failure</td>
<td>Robotic status code 205</td>
</tr>
<tr>
<td>robotic volume position is already in use</td>
<td>Media Manager status code 37</td>
</tr>
</tbody>
</table>
### Table 6-1

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code number</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSM is not supported</td>
<td>Device Configuration status code 48</td>
</tr>
<tr>
<td>rule does not exist in rule database</td>
<td>Media Manager status code 97</td>
</tr>
<tr>
<td>Shared Storage Option (SSO) is not licensed</td>
<td>Device Configuration status code 53</td>
</tr>
<tr>
<td>specified robot is unknown to vmd</td>
<td>Media Manager status code 79</td>
</tr>
<tr>
<td>STATUS_SUCCESS</td>
<td>Robotic status code 200</td>
</tr>
<tr>
<td>Stopping device daemon with tapes assigned</td>
<td>Device management status code 73</td>
</tr>
<tr>
<td>Success</td>
<td>Device Configuration status code 0</td>
</tr>
<tr>
<td>System Error</td>
<td>Device Configuration status code 87 and Media Manager status code 2</td>
</tr>
<tr>
<td>System error occurred</td>
<td>Robot Error status code 11</td>
</tr>
<tr>
<td>System error occurred during robot operation</td>
<td>Robotic status code 230</td>
</tr>
<tr>
<td>Tape file path exceeds 255 character maximum</td>
<td>Device management status code 49</td>
</tr>
<tr>
<td>Tape needs to be write enabled</td>
<td>Device management status code 46</td>
</tr>
<tr>
<td>The device is not robotic, cannot perform cleaning</td>
<td>Device management status code 58</td>
</tr>
<tr>
<td>The device_mappings file has invalid license info</td>
<td>Device Configuration status code 2</td>
</tr>
<tr>
<td>The device name is not valid, no device responded</td>
<td>Device Configuration status code 52</td>
</tr>
<tr>
<td>The drive is DOWN</td>
<td>Device management status code 15</td>
</tr>
<tr>
<td>The drive is not ready or inoperable</td>
<td>Device management status code 21</td>
</tr>
<tr>
<td>The drive serial number already exists in the device database</td>
<td>Device Configuration status code 91</td>
</tr>
<tr>
<td>The eject command was aborted by the user</td>
<td>Robotic status code 244</td>
</tr>
<tr>
<td>The EMM server failed to process the request</td>
<td>Device Configuration status code 78</td>
</tr>
<tr>
<td>Error message</td>
<td>Status code number</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>the global device database device name is invalid</td>
<td>Media Manager status code 162</td>
</tr>
<tr>
<td>the global device database device type is invalid</td>
<td>Media Manager status code 160</td>
</tr>
<tr>
<td>the media is allocated for use</td>
<td>Media Management status code 199</td>
</tr>
<tr>
<td>the operation requested has failed</td>
<td>Media Manager status code 163</td>
</tr>
<tr>
<td>the query with time failed because a limit was reached</td>
<td>Media Manager status code 184</td>
</tr>
<tr>
<td>The requested operation is not valid for the specified Disk Type</td>
<td>Device Configuration status code 95</td>
</tr>
<tr>
<td>the request sent to the Device Allocator has failed</td>
<td>Media Manager status code 190</td>
</tr>
<tr>
<td>the robotic daemon returned an invalid volume GUID</td>
<td>Media Manager status code 164</td>
</tr>
<tr>
<td>the robotic library is full and may still have media in its map</td>
<td>Media Manager status code 185</td>
</tr>
<tr>
<td>The specified Disk Array Host is not configured in NetBackup</td>
<td>Device Configuration status code 96</td>
</tr>
<tr>
<td>the specified pool is not empty</td>
<td>Media Manager status code 111</td>
</tr>
<tr>
<td>This is a drive path operation, use the -drpath option</td>
<td>Device Configuration status code 81</td>
</tr>
<tr>
<td>this machine is not the database host</td>
<td>Media Manager status code 84</td>
</tr>
<tr>
<td>This robot type does not support multiple media types</td>
<td>Device Configuration status code 17</td>
</tr>
<tr>
<td>Timeout waiting for robotic command</td>
<td>Robotic status code 203</td>
</tr>
<tr>
<td>too many volumes in volume group</td>
<td>Media Manager status code 68</td>
</tr>
<tr>
<td>Unable to allocate memory for this process</td>
<td>Device configuration status code 79</td>
</tr>
<tr>
<td>Unable to connect to NDMP host verify hostname</td>
<td>Device configuration status code 67</td>
</tr>
</tbody>
</table>
### Table 6-1  
**Media and device management messages and status codes (continued)**

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unable to connect to the EMM server</td>
<td>Device configuration status code 77 and Device management status code 78</td>
</tr>
<tr>
<td>Unable to create NDMP session</td>
<td>Device configuration status code 70</td>
</tr>
<tr>
<td>unable to find any records in the device test database</td>
<td>Media Manager status code 176</td>
</tr>
<tr>
<td>unable to generate a unique media id</td>
<td>Media Manager status code 127</td>
</tr>
<tr>
<td>Unable to initialize robot</td>
<td>Robotic status code 204</td>
</tr>
<tr>
<td>Unable to open drive</td>
<td>Robotic status code 209</td>
</tr>
<tr>
<td>Unable to open robotic path</td>
<td>Robotic status code 201</td>
</tr>
<tr>
<td>unable to open the device test state file</td>
<td>Media Manager status code 175</td>
</tr>
<tr>
<td>Unable to process NDMP message</td>
<td>Device configuration status code 68</td>
</tr>
<tr>
<td>Unable to SCSI unload drive</td>
<td>Robotic status code 210</td>
</tr>
<tr>
<td>unable to send exit status</td>
<td>Media Manager status code 67</td>
</tr>
<tr>
<td>Unable to sense robotic device</td>
<td>Robotic status code 202</td>
</tr>
<tr>
<td>unexpected data from robotic software daemon</td>
<td>Media Manager status code 46</td>
</tr>
<tr>
<td>unexpected data received</td>
<td>Media Manager status code 40</td>
</tr>
<tr>
<td>Unknown drive name</td>
<td>Device management status code 41</td>
</tr>
<tr>
<td>unknown EMM error code</td>
<td>Media Manager status code 192</td>
</tr>
<tr>
<td>Unsupported NDMP version</td>
<td>Device configuration status code 73</td>
</tr>
<tr>
<td>Update Drive Name Rule request failed</td>
<td>Device configuration status code 83</td>
</tr>
<tr>
<td>Usage error in creating child process</td>
<td>Robot Error status code 12</td>
</tr>
<tr>
<td>user id was not superuser</td>
<td>Media Manager status code 3</td>
</tr>
<tr>
<td>volume daemon fork failed</td>
<td>Media Manager status code 85</td>
</tr>
<tr>
<td>volume does not exist in database</td>
<td>Media Manager status code 35</td>
</tr>
<tr>
<td>volume group does not exist</td>
<td>Media Manager status code 65</td>
</tr>
</tbody>
</table>
Table 6-1  Media and device management messages and status codes (continued)

<table>
<thead>
<tr>
<th>Error message</th>
<th>Status code number</th>
</tr>
</thead>
<tbody>
<tr>
<td>volume has exceeded maximum mounts</td>
<td>Media Manager status code 116</td>
</tr>
<tr>
<td>volume has passed expiration date</td>
<td>Media Manager status code 115</td>
</tr>
<tr>
<td>volume is already assigned</td>
<td>Media Manager status code 93</td>
</tr>
<tr>
<td>Volume is in home slot</td>
<td>Robotic status code 249</td>
</tr>
<tr>
<td>Volume is in library, but not in drive domain</td>
<td>Robotic status code 233</td>
</tr>
<tr>
<td>Volume is in use</td>
<td>Robotic status code 237</td>
</tr>
<tr>
<td>volume is not in specified pool</td>
<td>Media Manager status code 94</td>
</tr>
<tr>
<td>Volume not found in library</td>
<td>Robotic status code 232</td>
</tr>
<tr>
<td>VxSS Access Denied</td>
<td>Media Manager status code 188, Device management status code 77, and Device configuration status code 92</td>
</tr>
<tr>
<td>VxSS authentication failed.</td>
<td>Media Manager status code 187</td>
</tr>
<tr>
<td>You do not have permission to create the file</td>
<td>Device management status code 44</td>
</tr>
<tr>
<td>You must be administrator to execute</td>
<td>Robot Error status code 14</td>
</tr>
<tr>
<td>You must be ROOT to start daemon</td>
<td>Robot Error status code 1</td>
</tr>
</tbody>
</table>
This chapter includes the following topics:

- About disaster recovery
- Recommended backup practices
- Disk recovery procedures for UNIX and Linux
- Disk recovery procedures for Windows
- Catalog recovery from an online backup
- Clustered NBU server recovery for UNIX and Linux
- Clustered NBU server recovery for Windows

### About disaster recovery

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, &CompanyName; recommends that you contact technical support.

This topic provides information about NetBackup installation and (if necessary), catalog recovery after a system disk failure. &CompanyName; assumes that you recover to the original system disk or one configured exactly like it.
Warning: NetBackup may not function properly if you reinstall NetBackup and recover its catalogs on a system disk to a different partition or one that is partitioned differently due to internal configuration information. Instead, configure a replacement disk with partitioning identical to the failed disk, then reinstall NetBackup on the same partition on which it was originally installed.

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 describes a set of recommended backup practices.

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. The first concern is to include all files with that records that are critical to users and the organization. You also need to 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.

You should 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 Bare Metal Restore System Administrator's Guide.
Critical policies

When configuring a policy for online catalog backup, you can 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**, you should 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

&Company; recommends saving the disaster recovery files 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 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, if the system that performs the recovery does not include NetBackup servers with identical names to those where the backups were made, the automated recovery may not succeed.
Online catalog disaster recovery information email

You should 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 providing a customized mail script. More details are available.

See Reference Topics of the *NetBackup Administrator's Guide, Volume II.*

Identifying the correct catalog backup

A complete catalog should be recovered from the most recent series of backups. If not, the potential for inconsistency between the catalog and the actual state or contents of storage media could exist.

The following are two examples of the need for recovering from the most recent series of backups:

- Tape media images have all expired after the catalog backup that the recovery was done from and the tape designated for and possibly re-used.
- Disk-based media whose images expired after the catalog backup that the recovery was done from and the images were deleted from the disk.

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. You should also set up backup schedules for the master 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.
Disk recovery procedures for UNIX and Linux

The following section describes the procedures for three different types of disk recovery for UNIX and Linux:

- Master server disk recovery procedures
- Media server disk recovery procedures
- Client disk recovery procedures

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

The procedure in this section explains how to recover data if the system disk fails on a UNIX or Linux NetBackup master server.

The following two scenarios are covered:

- Root file system is intact. The operating system, NetBackup software and some (if not all) other files are assumed to be lost.
- 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 caused by overwriting files that the operating system uses during the restore.

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 backup and recovery procedures.

See the 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, then restoring NetBackup, and finally restoring all other files.

To recover

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:** &CompanyName; 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*.
   - Using the NetBackup Device Configuration Wizard to discover and configure the recovery device in NetBackup.
     See the *NetBackup Administrator's Guide, Volume I*.
   - Using the NetBackup command `tpautoconf` to discover and configure the recovery device in NetBackup.
See the NetBackup Command Guide.

Updating the device mapping files.

See the NetBackup Administrator’s Guide, Volume II.

6 If you must restore from policy 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.
- Using the NetBackup Volume Configuration Wizard to inventory the media contents of a robotic device.
- Using 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.

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.

/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 general steps to this procedure are: 1) load the operating system on an alternate boot disk, 2) install NetBackup on that disk, 3) recover NetBackup catalogs to that disk, 4) restore the root partition and the latest backed up files to the recovery disk, and 5) copy the NetBackup catalogs from the alternate disk to the recovery disk.
This 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 caused by overwriting 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. Create on the alternate disk the partition and directory where NetBackup and 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 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 any changes to the default catalog directories would be reflected in the NetBackup catalog backups, recreate those directories before the catalog recovery.

   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 \texttt{tpautoconf} to discover and configure
the recovery device in NetBackup.
See the NetBackup Command manual.

Update the device mapping files.
See the NetBackup Administrator’s Guide, Volume II.

If you must restore from policy 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 \texttt{robtest} or vendor-specific robotic
  control software to load media into the required recovery device or devices.
- Using the NetBackup Volume Configuration Wizard to inventory the media
  contents of a robotic device.
- Using the vendor-specific robotic control software to load the media into
  the required recovery device(s).

Recover the NetBackup catalogs to the alternate disk.
See “Catalog recovery from an online backup” on page 589.
The catalogs can be recovered only to the same directory structure from
which they were backed up (alternate path recovery is not allowed).

Start the NetBackup Backup, Archive, and Restore interface (or the \texttt{bp}
command) and restore the latest backed up version of all files to the disk you
are recovering.

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.

\textbf{Warning:} Do not restore files to the \texttt{/usr/openv/var}, \texttt{/usr/openv/db/data},
or \texttt{/usr/openv/volmgr/database} directories (or relocated locations) or
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.

If your configuration includes an Enterprise Media Manager (EMM) server that is separate from the master server, start NetBackup on the EMM server before starting NetBackup on the master server.

/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.

Recovering the NetBackup media server disk for UNIX and Linux

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 client disk” on page 578.

---

**Note:** A separate computer that functions as a NetBackup 6.0 or later media server is available only on NetBackup Enterprise Server. For NetBackup Server installations, the master server and the media server are installed on the same system and have the same host name. Therefore, recovering the master server disk also recovers the media server.

---

Recovering the client disk

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 Administrator's Guide*. 
If you installed and configured NetBackup Intelligent Disaster Recovery (IDR) on the client system, use the recovery procedures in the *NetBackup Administrator’s Guide, Volume II* instead of the following instructions:

**To recover the system disk on a client workstation**

1. Reload the operating system as you normally would for a client workstation of that type.
   
   If the root file system is lost, the best approach may be to reload the operating system on an alternate boot disk and start from this disk. After restoring the system, restore root to its original partition. This operation lets you recover the root partition without risking a crash due to overwriting files that the operating system uses during the restore. The procedure is similar to the procedure that is used for the master server, except that recovering the NetBackup catalogs is not necessary.
   
   See “*Recovering the master server disk for Windows*” on page 580.

2. Reinstall NetBackup client software and patches.

3. Use the NetBackup Backup, Archive, and Restore interface to select and restore files.

### Disk recovery procedures for Windows

The following section describes the procedures for three different types of disk recovery for Windows:

- Master server disk recovery procedures
- Media server disk recovery procedures
- Client disk recovery procedures

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.
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.
- 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.

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 you are recovering. 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 any changes to the default catalog directories would be reflected in the NetBackup catalog backups, recreate those directories before the catalog recovery. 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*.

- Using the NetBackup command `tpautoconf` to discover and configure the recovery device in NetBackup.
  See the *NetBackup Commands* manual.

- Updating the device mapping files.
  See the *NetBackup Administrator's Guide, Volume II*.

8 If the recovery scenario involves restoring policy or catalog backups, the appropriate recovery device(s) must be configured.

Configuring the media may involve the following tasks:

- 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 “Catalog recovery from an online backup” on page 589.
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 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 any changes to the default catalog directories would be reflected in the NetBackup catalog backups, recreate those directories before the catalog recovery. 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*.

- Using the NetBackup Device Configuration Wizard to discover and configure the recovery device in NetBackup. See the *NetBackup Administrator's Guide, Volume I*.

- Using the NetBackup command `tpautoconf` to discover and configure the recovery device in NetBackup. See the *NetBackup Commands* manual.

- Updating the device mapping files. See the *NetBackup Administrator's Guide, Volume II*.

9 If you must restore from policy 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.

- Using the NetBackup Volume Configuration Wizard to inventory the media contents of a robotic device.

- Using the vendor-specific robotic control software to load the media into the required recovery devices.

10 Recover the NetBackup catalogs. See “Catalog recovery from an online backup” on page 589.
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
```

If your configuration includes an Enterprise Media Manager (EMM) server that is separate from the master server, start NetBackup on the EMM server first.

---

**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 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.
Recovering the NetBackup media server disk for Windows

A separate computer that functions as a NetBackup 6.0 or later media server is available only on NetBackup Enterprise Server. For NetBackup Server installations, the master server and the media server are installed on the same system and have the same host name. Therefore, recovering the master server disk also recovers the media server.

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 the client disk” on page 578.

Recovering the 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.

---

**Note:** If you installed and configured NetBackup Intelligent Disaster Recovery (IDR) on the client system, refer to the NetBackup Administrator’s Guide, Volume II, for recovery procedures instead of the instructions in this procedure.

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 to be identical 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 is being restored. Reinstall the same type and version of software that was previously used.
- NetBackup client software to install on the client that is 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 all 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 `bpinetd` 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.
Catalog recovery from an online backup

This topic explains how to recover a catalog that was backed up using the online, hot catalog backup method that is described in the following manual:

See the NetBackup Administrator’s Guide, Volume I.

This procedure can be stand-alone or part of a larger disk recovery procedure. See one of the following topics:

See “Disk recovery procedures for UNIX and Linux” on page 573.

See “Disk recovery procedures for Windows” on page 579.

---

Note: When any online catalog backup recovery try that involves media completes, NetBackup changes the state of the media that contains the catalog backup to frozen. 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.

See “Unfreezing online catalog recovery media” on page 622.

---

Note: You must have root (administrative) privileges to perform these procedures.

You can recover the catalog from an online, hot backup in either of two ways:

- Recovering the entire catalog from an online backup
  This procedure is the recommended method for recovering the entire catalog and recovers the NetBackup relational database as well as NetBackup policy files, backup image files, and configuration files.

- Recovering the catalog image file
  This method recovers only the NetBackup policy files, backup image files, and configuration files. Use this method if the NetBackup relational database is valid but NetBackup policy, backup image, or configuration files are lost. The NetBackup relational database can also be recovered separately using the `bprecover -nbdb` command.

---

Recovering the entire catalog from an online backup

The entire catalog can be recovered by using the Catalog Recovery Wizard or the text-based `bprecover -wizard` command.
Warning: Do not run any client backups before you recover the NetBackup catalog.

The Catalog Recovery Wizard screens that appear when performing these procedures are very similar for UNIX, Linux, and Windows platforms. Only the Windows screens are shown in text in the following procedures.

Recovering the entire catalog using the Catalog Recovery Wizard

This procedure shows you how to recover the entire catalog using the Catalog Recovery Wizard. You must have root (administrative) privileges.

Note: The Catalog Recovery wizard does not work after performing a change server operation. You must be logged on locally to the master server that is being recovered.

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.

To recover the entire catalog

1. Your configuration may include an Enterprise Media Manager (EMM) server that is separate from the master server. If so, start NetBackup on the EMM server before starting NetBackup on the master server.

2. Start NetBackup by entering the following:
   - On UNIX and Linux:
     ```
     /usr/openv/netbackup/bin/bp.start_all
     ```
   - On Windows:
     ```
     install_path\NetBackup\bin\bpup
     ```

   The NetBackup Administration Console appears.

3. If the necessary devices are not already configured, configure them in NetBackup.

4. Make available to NetBackup the media that contains the catalog backup.
5 Click **Recover the Catalogs** on the NetBackup Administration Console to start the Catalog Recovery Wizard.

The **Welcome** screen appears.
6 Click **Next** on the Welcome screen to display the **Catalog Disaster Recovery File** screen.

This wizard relies on the disaster recovery information that is generated during the online catalog backup. Part of the online catalog backup configuration that is included indicates where the disaster recovery information file was to be stored and-or sent.

In most cases, you specify the most recent disaster recovery information file available, unless some form of corruption has occurred and you want to restore to an earlier state of the catalog. If the most recent catalog backup was an incremental, use the disaster recovery file from the incremental backup. (There is no need to first restore the full backup that is followed by the incremental.)

Indicate where the disaster recovery file is stored by entering the fully qualified path to the disaster recovery file.

More information is available on the email that is sent and the attached disaster recovery file.

See “**Recovering the catalog without the disaster recovery file**” on page 613.
The wizard waits while NetBackup searches for the necessary media sources, then informs you if the necessary backup ID of the disaster recovery image is located.

Or, if the media is not located, the wizard lists which media is needed to update the database.

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 screen depends on whether the recovery is from a full backup or an incremental backup.

If an online catalog backup policy includes both full and incremental backups, the disaster recovery email may indicate either a full or an incremental backup for recovery. An incremental backup recovery completely recovers the entire catalog because it references information from the last full backup. You don’t need to first recover the last full catalog backup, then subsequent incremental backups.
8 When the required media sources are all found, click **Next** to display the **Disaster Recovery Method** screen. The **Recover entire NetBackup catalog** radio option is selected.

![Disaster Recovery Method](image)

9 With the **Recover entire NetBackup catalog** radio option selected, 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.
10 The wizard displays the recovery progress.

![NetBackup Catalog Recovery Wizard](image)

If the recovery is not successful, consult the log file messages for an indication of the problem.

11 The final screen announces that the full recovery is complete. Each image file is restored to the proper image directory, and the NetBackup relational databases (NBDB and optionally BMRDB) have been restored and recovered.

If this step is part of a server recovery procedure, complete the remaining steps in the appropriate Server Disk Recovery procedure.

12 NetBackup does not run scheduled backup jobs until NetBackup is stopped and restarted. Before you restart NetBackup, protect the media that contains any backups that were successfully performed after the catalog backup that was used to recover the catalog.

This 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
You can manually submit backup jobs before you stop and restart NetBackup. Be aware that if you have not protected the media containing the backups done after the catalog backup, the media may be overwritten.

Stop and restart NetBackup on all the servers.

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

If a remote EMM server is being used, start NetBackup on it before you start NetBackup on the master server.

If you have recovered from removable media, that media is now frozen.

To unfreeze, see the following:
See “Unfreezing online catalog recovery media” on page 622.

Recovering the entire catalog using bprecover -wizard

The bprecover -wizard command is an alternate way to recover an entire catalog that is backed up using the online catalog backup method. This method does not require the NetBackup Administration Console. You must have root (administrative) privileges to perform this procedure.

Note: You must be logged on locally to the master server that is being recovered.

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.

The steps are the same as those in the following topic:
See “Recovering the entire catalog using the Catalog Recovery Wizard” on page 590.
To recover the entire catalog using `bprecover -wizard`

1. Start NetBackup by entering the following:
   
   If your configuration includes an Enterprise Media Manager (EMM) server that is separate from the master server, start NetBackup on the EMM server before starting NetBackup on the master server.
   
   On UNIX and Linux:
   
   `/usr/openv/netbackup/bin/bp.start_all`
   
   On Windows:
   
   `install_path\NetBackup\bin\bpup`

2. Run 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)

3. Enter Y to continue. The following prompt appears:
   
   Please specify the full pathname to the catalog disaster recovery file:

4. Enter the fully qualified pathname to the Backup ID file. For example:
   
   `C:\DR_INFO\HotCatBack_1120078077_FULL`
   
   The following is displayed:
   
   All media resources were located
   
   Do you want to recover the entire NetBackup catalog? (Y/N)
5 Enter Y to continue. The following is displayed:

Catalog recovery is in progress. Please wait...
Database server restarted, and completed successful recovery of NBDB on <EMM Server>
Catalog recovery has completed.
Please review the log file C:\Program Files\VERITAS\NetBackup\Logs\user_ops\Administrator\logs\Recover1120078220.log for more information.

The image file is restored to the proper image directory and the NetBackup relational databases (NBDB and optionally BMRDB) are restored and recovered.

6 NetBackup does not run scheduled backup jobs until NetBackup is stopped and restarted. Before you restart NetBackup, protect the media that contains backups that were successfully performed after the catalog backup that was used to recover the catalog.

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

7 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

If a remote EMM server is being used, start NetBackup on it before you start NetBackup on the master server.

Recovering the catalog image file

Consider performing this recovery procedure only in the following scenarios:

■ The NetBackup relational database is valid, but NetBackup policy, backup image, or configuration files are lost.
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.

The catalog backup images contain information about all the data that has been backed up. This information constitutes the largest part of the NetBackup catalog.

If the backup images are intact but the NetBackup relational database files are not, you can still recover these files. See “Recovering relational database files from an online catalog backup” on page 608.

The wizard restores whatever catalog images and configuration files are in the backup set identified by the disaster recovery file. If the disaster recovery file is from a full backup, all catalog images and configuration files are restored.

For an incremental backup, the wizard restores only catalog images and configuration the files that were changed since the previous backup. However, all catalog backup image files back to the last full catalog backup are automatically included in an incremental catalog backup. This operation allows for the complete restoration of all backup images by the Backup, Archive, and Restore user interface.

For a catalog that was backed up using the online method of NetBackup catalog image and configuration files, recovery in either of the following ways:

- Use the Catalog Recovery Wizard
- Use the `bprecover -wizard` command

During a manual recovery, the wizard recovers only NetBackup policy files, NetBackup backup image files, and other NetBackup configuration files. It does not recover the NBDB (includes EMM) or BMR databases.

If the backup from which you recover is an incremental catalog backup and no catalog backup images exist in the catalog, the following occurs: only the NetBackup policy, backup image, and configuration files that are backed up in that incremental backup are restored. However, all of the catalog backup images up to the last full catalog backup are restored. So you can restore the rest of the policy, images, and configuration files from the Backup, Archive and Restore interface. If catalog backup images already exist, all files that were included in the related set of catalog backups are restored. The NBDB (includes EMM) and BMR (if applicable) databases must then be recovered by running the following:

```
bprecover -r -nbdb
```

Table 7-1 is a list of the files that you recover in a manual recovery (an asterisk indicates multiple files within that folder).
The following is a list of NetBackup relational database (SQL Anywhere) files that are not recovered in a manual recovery.

- NBDB.db
- NBDB.log
- EMM_DATA.db
- EMM_INDEX.db
- BMRDB.db
- BMRDB.log
- BMR_DATA.db
- BMR_INDEX.db
- vxdbms.conf
- DARS_DATA.db
- DARS_INDEX.db
- DBM_DATA.db
- DBM_INDEX.db

- `install_path\NetBackupDB\conf\server.conf` (Windows only)
- `install_path\NETBACKUP\DB\conf\databases.conf` (Windows only)

You can recover these files.

See “Recovering relational database files from an online catalog backup” on page 608.

### Recovering the catalog image files using the Catalog Recovery Wizard

You must have root (administrative) privileges to perform this procedure.
Note: The Catalog Recovery wizard does not work after performing a change server operation. You must be logged on locally to the master server that is being recovered.

To recover the catalog image files

1  Start NetBackup by entering the following:
   If your configuration includes an EMM server that is separate from the master server, do the following: start NetBackup on the EMM server before starting NetBackup on the master server.
   On UNIX and Linux:
   /usr/openv/netbackup/bin/bp.start_all
   On Windows:
   install_path\NetBackup\bin\bpup

2  Click Recover the Catalogs in the NetBackup Administration Console to start the Catalog Recovery Wizard.

Warning: Do not run any client backups before you recover the NetBackup catalog.
This wizard relies on the disaster recovery information that was generated during the online, hot catalog backup. Part of configuring the catalog backup included the indication of where the disaster recovery information was to be stored and sent.

Indicate where the disaster recovery file is stored by entering the fully qualified path to the disaster recovery file.

For example:

/net/lex/Cat_DR/CatBk_1119304246_INCR

Specify the most recent disaster recovery file available, unless there is a reason to restore from an earlier state.

Note whether the disaster recovery file is based on a full (*)_FULL) or an incremental (*)_INCR) catalog backup.

More information is available on the email that is sent and the attached disaster recovery file.

See “Recovering the catalog without the disaster recovery file” on page 613.
4 The wizard waits while NetBackup searches for the necessary media sources, then tells you if the necessary backup ID of the DR image was located. If the media is not located, the wizard lists which media is needed to update the database.

Follow the wizard instructions to insert the indicated media and run an inventory to update the NetBackup database.

5 Click Next to display the Disaster Recovery Method dialog. Select the Recover only NetBackup catalog image and configuration files radio option and click Next.
6. 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.
The final screen indicates that the catalog backup images have been recovered.

You can now recover the NetBackup database if necessary.

NetBackup does not run scheduled backup jobs until NetBackup is stopped and restarted. Before you restart NetBackup, protect the media that contains backups that were successfully performed after the catalog backup that was used to recover the catalog.

Media protection may 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

9 Stop and restart NetBackup on all the servers.
   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

   If a remote EMM server is being used, start NetBackup on it before you start NetBackup on the master server.

Recovering the catalog image file using bprecover -wizard

You must have root (administrative) privileges to perform this procedure.

To recover the catalog image file using bprecover -wizard

1 Start NetBackup by entering the following:
   If your configuration includes an EMM server separate from the master server, start NetBackup on the EMM server before starting NetBackup on the master server.
   On UNIX and Linux:
   /usr/openv/netbackup/bin/bp.start_all

   On Windows:
   install_path\NetBackup\bin\bpup

2 Run 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)
3 Enter Y to continue. The following prompt appears:

Please specify the full pathname to the catalog disaster recovery file:

4 Enter the pathname to the Backup ID file. For example:

C:\DR_INFO\HotCatBack_1120078077_FULL

The following is displayed:

All media resources were located
Do you want to recover the entire NetBackup catalog? (Y/N)

5 Enter N to continue. The following is displayed:

Catalog recovery is in progress. Please wait...
This portion of the catalog recovery has completed.

Because this operation is a partial recovery, any remaining portions of the catalog must be restored using Backup, Archive, and Restore.

Please review the following log file for more information

C:\Program Files\VERITAS\NetBackup\Logs\user_ops\Administrator\logs\Recover1123008613.log

You can now recover the NetBackup database if necessary.

6 NetBackup does not run scheduled backup jobs until NetBackup is stopped and restarted. Before you restart NetBackup, protect the media that contains backups that were successfully performed after the catalog backup that was used to recover the catalog.

This media protection may 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

7  Stop and restart NetBackup on all the servers.

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

If a remote EMM server is being used, start NetBackup on it before you start NetBackup on the master server.

Recovering relational database files from an online catalog backup

If the NetBackup (NBDB) or Bare Metal Restore (BMRDB) relational database files need to be recovered, perform this procedure.

The full procedure is necessary only if the NBDB database has been corrupted. A temporary database must be created to restore from the catalog backup. If the NBDB database is available and the SQL Anywhere server is running, then do the following: perform only steps 11 and 12 to replace the existing database with the copy from the catalog backup.

**Note:** If your configuration includes a remote EMM server, perform steps 1 through 7 on the EMM server.
To recover relational database files from an online catalog backup

1. If NetBackup is running, stop it.
   - On UNIX and Linux:
     
     /usr/openv/netbackup/bin/bp.kill_all
   
   - On Windows:
     
     install_path\NetBackup\bin\bpdown

2. Move the following set of existing database files from their current location to a temporary directory.
   - NBDB:
     
     nbdb.db, nbdb.log, emm_index.db, emm_data.db
   
   - BMRDB:
     
     bmrdb.db, bmrdb.log

3. Change databases.conf so SQL Anywhere does not try to automatically start them when the server is started.
   - On UNIX and Linux:
     
     /usr/openv/db/bin/nbdb_admin -auto_start NONE
   
   - On Windows:
     
     install_path\NetBackup\bin\nbdb_admin -auto_start NONE

4. Start the SQL Anywhere server.
   - UNIX and Linux:
     
     /usr/openv/netbackup/bin/nbdbms_start_stop start
   
   - Windows:
     
     install_path\NetBackup\bin\bpup -e SQLANYs_VERITAS_NB
5 Re-create an empty database.
   UNIX and Linux:

   /usr/openv/db/bin/create_nbdb -drop

   Windows:

   install_path\NetBackup\bin\create_nbdb -drop

   If the database has been moved or the environment is clustered, add -staging staging_dir to the end of the create_nbdb command line.

   If the database has been moved or the environment is clustered, and space constraints or other issues force you to create this temporary database in the final location, use the following command:

   UNIX and Linux:

   /usr/openv/db/bin/create_nbdb -drop -data <data_dir> -index <index_dir> -tlog <tlog_dir> -staging <staging_dir>

   Windows:

   install_path\NetBackup\bin\create_nbdb -drop -data <data_dir> -index <index_dir> -tlog <tlog_dir> -staging <staging_dir>

   Where the <data_dir>, <index_dir>, <tlog_dir>, and <staging_dir> values are defined in the vxdbms.conf file as VXDBMS_NB_DATA, VXDBMS_NB_INDEX, VXDBMS_NB_TLOG, and VXDBMS_NB_STAGING.

6 Stop and restart NetBackup.
   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 tpext:
   UNIX and Linux:
   /usr/openv/volmgr/bin/tpext
   Windows:
   install_path\Volmgr\bin\tpext

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. The default location is the following:
   UNIX and Linux:
   /usr/openv/db/data
   Windows:
   install_path\NetBackupDB\data

9 Start the device manager:
   UNIX and Linux:
   /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 or add the media for stand-alone drives.
For online catalog recovery, run the following command on the master server:

**UNIX and Linux:**

```
/usr/openv/netbackup/bin/admincmd/bprecover -r -nbdb
```

**Windows:** start the device manager service.

```
install_path\NetBackup\bin\admincmd\bprecover -r -nbdb
```

Stop and restart NetBackup.

**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
```

If a remote EMM server is being used, start NetBackup on it before you start NetBackup on the master server.

### Recovering NetBackup access management components from a hot backup

If you have configured NetBackup Access Control (NBAC), the online, hot catalog backup automatically backs up your authentication 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.

**To recover the NetBackup catalog from an online catalog backup when NetBackup Access Control is configured**

1. Follow the normal NetBackup catalog recovery procedures. Ensure that NetBackup Access Management Control is installed but disabled before you run the actual catalog recovery wizard or `bprecover` command. You must have root privileges to execute the recovery.

2. Turn off the authentication and authorization services (Windows) or daemons (UNIX and Linux).
3 Recover the NetBackup catalog from the online catalog backup using the recovery wizard or bprecover command. Authentication and authorization data is not copied back to the hosts from which it was backed up. Instead, it is copied to a staging area for use in step 4.

4 Run "bprecover -r -vxss -p <policy name>" and supply the name of the online catalog backup policy. This action recovers authentication and authorization data from the staging area to the hosts from which it was backed up.

5 Start up the authentication and authorization services (Windows) or daemons (UNIX and Linux).

6 Configure NetBackup to use NetBackup Access Management Control by setting up the proper Access Control host properties for master server(s), media server(s), and client(s).

7 Restart NetBackup.

Recovering the catalog using a copy of an online catalog backup

The online, hot catalog backup can create multiple copies of the catalog backup in either of two ways: by specifying multiple copies when the backup is originally done or by duplicating the catalog backup later.

To recover the catalog from a copy, see the following:
See “Recovering the catalog without the disaster recovery file” on page 613.

Recovering the 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 from an online catalog backup when you no longer have the Disaster Recovery file

1 The email identifies the media that contains the Disaster Recovery file, as well as the media that was used to back up critical policies. Ensure that this media is available.

2 Follow the normal catalog recovery steps up until the point where the NetBackup 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 media_id -drfile_dest fully_qualified_directory_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 the directory is available from the NetBackup master server.
Continue with the normal catalog recovery procedure by running the NetBackup 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 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.

The following is an example of a Disaster Recovery email:

```
Server
    ant

Date
    Tue Aug 9 11:41:48 2009

Policy
    CatalogBackup

Catalog Backup Status
    the requested operation was successfully completed (status 0).

To ensure that the NetBackup catalog data is protected through Tue Aug 9 11:41:48 2009, retain a copy of the attached file, and the media or files listed below:

**Catalog Recovery Media**

<table>
<thead>
<tr>
<th>Media Server</th>
<th>Disk image path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* ant</td>
<td>/storage/DiskUnit1/ant_1123605764_C1_TIR</td>
</tr>
<tr>
<td>* ant</td>
<td>/storage/DiskUnit1/ant_1123605764_C1_F1</td>
</tr>
<tr>
<td>* ant</td>
<td>/storage/DiskUnit1/ant_1123605713_C1_F1</td>
</tr>
</tbody>
</table>

DR file written to
```
/storage/DR/CatalogBackup_1123605764_FULL
```
Catalog Recovery Procedure for the Loss of an Entire Catalog

Symantec recommends creating a detailed disaster recovery plan 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 help 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:

1. Install NetBackup.
2. Configure the devices necessary to read the media listed above.
3. Inventory the media.
4. Run:
   \texttt{bpimport \{-create\_db\_info \{-server\ \name\\} \{-id\ \id\}}
   \texttt{/storage/DiskUnit1}
5. Go to the following directory to find the DR image file
   \texttt{CatalogBackup\_1123605764\_FULL:}
   \texttt{/usr/openv/netbackup/db/images/ant/1123000000/tmp}
6. Delete the other files in the directory.
7. Open \texttt{CatalogBackup\_1123605764\_FULL} file and find the
   \texttt{BACKUP\_ID}
   \texttt{(for\ \example:\ \texttt{ant\\_1123605764}).}
8. Run:
   \texttt{bpimport \{-server\ \name\\} \{-backupid\ \id\}}
9. Run:
   \texttt{bprestore \{-T\ \-w \{-L\ \progress\_log\\} \{-C\ \ant\ \-t\ \35\ \-p\}}
   \texttt{CatalogBackup \{-X\ \-s\ \1123605764\ \-e\ \1123605764\ /}}
10. Run the BAR user interface to restore the remaining image
    database
    \texttt{if\ \the\ \DR\ \image\ \is\ \a\ \result\ \of\ \an\ \incremental\ \backup.}
11. To recover the NetBackup relational database, run:
    \texttt{bprecov \{-r\ \-nbdb\}}
12. Stop and Start NetBackup
13. Configure the devices if any device has changed since the
    last
    \texttt{backup.}
14. To make sure the volume information is updated, inventory
    the media
    \texttt{to\ update\ the\ NetBackup\ database.}

### Recovering the user-directed online catalog from the CLI

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.

\textbf{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 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 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 filename and six zeroes attached.
   - media – the media where the catalog backup that is specified by the DR file is located. Found in the DR 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. Run a Phase II import on the media that is specified by the DR file to recover the catalog .f file from the hot catalog backup.

```
bpimport -server master_server -backupid backup_id
```

8. If your catalog backup was an 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
```
and 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 scheduled jobs that may overwrite 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 an 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.

- Select the "NBU-Catalog" policy type (from the Specify NetBackup Machines and Policy Type menu).
- Specify the Master Server as the source client for the restore.

Unfreezing online catalog recovery media

This procedure shows how to unfreeze your online catalog recovery media.

To unfreeze the online catalog recovery media, do the following:

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 done.
   - Identify the associated catalog backup parent image file by viewing the PARENT_IMAGE_ID value.
   - Identify the media that the catalog backup was written to by viewing the second to last field in the DR_MEDIA_REC line(s).
   - Save the catalog backup parent image file identified in step a.
   - Relocate or remove all other image files that relates to the catalog backup policy.

2. If the NetBackup configuration includes a remote EMM server, on the master server, go to the image database for the remote EMM server. Relocate or remove any images that relates to the catalog backup policy.

3. 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`

4. On the master server, run the following command:

   `bpimport`

5. 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`
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.

Refer to "Configuring NetBackup" in the *NetBackup High Availability Guide*.

**Warning:** Before attempting any of the recovery procedures in this topic, contact technical support.

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 "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 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 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.

Refer to the *NetBackup High Availability Guide*.

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 connected to that robot, and correct if necessary.

Refer to the "Media" section of 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 shared disk on a UNIX or Linux cluster

The following procedure is applicable in situations where the configured cluster nodes remain available but the NetBackup catalog, the database files, or both on the shared disk have been corrupted or lost.

The following conditions must be true to 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 UNIX or Linux cluster

1. Clear the faulted NetBackup resource group, disable monitoring and bring the shared disk and virtual name resources up on a functioning node.

2. Manually create the following directories on the shared disk:
   - `<shared disk path>/netbackup/db`
   - `<shared disk path>/db/data`
   - `<shared disk path>/var/global`
   - `<shared disk path>/volmgr/misc/robotic_db`

3. If this is an emm server, enter the following to bring up the database server and emm, then run tpext to initialize the emm db:
   ```
   # SHARED_DISK=<top-level shared disk mount point>
   # dataDir=${SHARED_DISK}/db/data
   # /usr/openv/netbackup/bin/nbdbms_start_stop start
   /usr/openv/db/bin/create_nbdb
   -data ${dataDir} \
   -index ${dataDir} \
   -tlog ${dataDir} \
   -mlog ${dataDir} \
   -staging ${dataDir}/staging \
   -drop
   # /usr/openv/volmgr/bin/tpext -loadEMM
   ```

4. Configure required devices and media and recover the NetBackup catalogs. See “Recovering the master server when root is intact” on page 574.

5. Manually shut down and restart NetBackup on the active node.

6. Re-enable monitoring of the NetBackup resource group.

7. Verify that the NetBackup server can now be brought online on all configured nodes.

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 the 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 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 when root is intact” on page 574.

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*.

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 "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.

See "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 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 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 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 the shared disk and virtual name resources up 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 583.

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 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 the 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 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 583.

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.
Disaster recovery

Clustered NBU server recovery for Windows
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
- Restore processes
- 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. This section explains the operation of NetBackup during . 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.

Note that this appendix does not describe the NetBackup products for backing up relational databases (such as NetBackup for ORACLE). The guides for those products have information regarding their operation.
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, see the following topic:

Information is available on SAN client and Fibre Transport startup processes.

See the NetBackup Shared Storage 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 is similar to a service; NLM stands for NetWare Loadable Module.

Note that all NetBackup processes 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 variations and describes the synthetic backup process. A description is included about how NetBackup operates when backing up its catalogs.

Job scheduling

The scheduler process bpsched consists of the following services:

- The nbpem service (Policy Execution Manager) does the following: 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) accepts requests from nbpem to run backup jobs, or to run media jobs from commands such as bplabel and tpreq. nbjm acquires resources for each job, such as storage unit, drives, media, and client and policy resources, and executes the job.

The nbrb service (Resource Broker) allocates resources in response to requests from nbjm. nbrb acquires physical resources from nbemm (the Enterprise Media Manager service). It also manages logical resources such as multiplex groups, maximum jobs per client, and maximum jobs per policy. nbrb is also responsible for initiating drive unloads and manages pending request queues.

EMM server and master server

The NetBackup master server and the Enterprise Media Manager (EMM) server can be on the same physical host or on different hosts.

The master server is responsible for running jobs as configured in NetBackup policies. The nbpem and nbjm services run only on the master server.

The EMM server allocates resources for one or more master servers. The EMM server is the repository for all device configuration information. The nbemm service and the nbrb service run only on the EMM server. The nbemm service centralizes resource selection and maintains devices, media, and storage units in a relational database.

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 (you cannot archive raw partitions). 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. nbpem 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 command with the –i option. This action causes bprd to contact nbpem, which then processes the policy, client, and schedule that are selected by the administrator.

- 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` commands 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 `nb pem`, which checks the policy configurations for schedules. By default, `nb pem` 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.

See the *NetBackup Administrator’s Guide, Volume II*.

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 66.

*Figure A-1* illustrates the various operations that comprise the backup process.
Table A-1 shows the sequence of operation of a backup process.

<table>
<thead>
<tr>
<th>Agent</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start-up script</td>
<td>Launches <code>bprd</code> on the master server and <code>ltid</code> on the master server and all media servers. All other daemons and programs are started as necessary including <code>nbpem</code>, <code>nbjm</code>, <code>nbrb</code>, and <code>nbemm</code>.</td>
</tr>
</tbody>
</table>
### Table A-1
Backup to tape or disk sequence of operation (continued)

<table>
<thead>
<tr>
<th>Agent</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy execution manager service (nb pem)</td>
<td>Gets the policy list from bpdbm.</td>
</tr>
<tr>
<td></td>
<td>Creates a policy-client task for all policy-client combinations specified in the policy list.</td>
</tr>
<tr>
<td></td>
<td>Computes the due time for each policy-client task (policy priority is honored for internal processing).</td>
</tr>
<tr>
<td></td>
<td>Submits to nbjm all jobs as policy-client tasks become due.</td>
</tr>
<tr>
<td></td>
<td>When a job finishes, it recomputes the due time of that policy-client task.</td>
</tr>
<tr>
<td>Job manager service (nb jm)</td>
<td>Issues a single request (with a request ID) to nbrb, for all resources that are required by a job.</td>
</tr>
<tr>
<td></td>
<td>nbrb gets the storage unit, tape drive, and media id information from nbemm and allocates client and policy resources.</td>
</tr>
<tr>
<td></td>
<td>nbrb returns to nbjm an allocation sequence that contains one allocation for each resource (each allocation contains a unique ID).</td>
</tr>
<tr>
<td></td>
<td>nbrb also returns allocation data for the specific resource type.</td>
</tr>
<tr>
<td></td>
<td>nbrb also returns the request ID along with the allocations so that nbjm can correlate the response with the right request (and job).</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>nbjm starts the backup by using the client daemon bpcd to start the backup and restore manager bpbrm.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Backup and restore manager (bpbrm)</td>
<td>Starts bptm.</td>
</tr>
<tr>
<td></td>
<td>Starts the actual backup (or archive) by using the client daemon bpcd to start the backup program and archive program bpkar on the client.</td>
</tr>
</tbody>
</table>
Table A-1  Backup to tape or disk sequence of operation (continued)

<table>
<thead>
<tr>
<th>Agent</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup and archive manager (bpbkar)</td>
<td>Sends the information about files within the image to <code>bpbrm</code>, which directs the file information to the NetBackup file database. The information is sent by means of <code>bpdbm</code> on the master server. Transmits the backup image to <code>bptm</code> depending on one of the following: whether the media server backs up itself (<code>bptm</code> and <code>bpbkar</code> are on the same host) or back ups a client that resides on a different host. If the media server backs up itself, <code>bpbkar</code> 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 <code>bptm</code> 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 <em>NetBackup Backup Planning and Performance Tuning Guide</em>.</td>
</tr>
</tbody>
</table>
Table A-1  Backup to tape or disk sequence of operation (continued)

<table>
<thead>
<tr>
<th>Agent</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup manager for tape (bptm) or disk</td>
<td>The bptm process or bpdm process on the server takes the image from shared memory and directs it to the storage media.</td>
</tr>
<tr>
<td>(bpdm)</td>
<td>If the storage media is tape, bptm requests information for the first media and drive to use, by exchanging information with nbjm.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>nbemm calls nbrmms on the media server that was chosen to mount the volume.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>For BasicDisk, bpdm writes the images to the path that is configured in the disk storage unit. The system disk manager controls the actual writing of data.</td>
</tr>
<tr>
<td></td>
<td>In the case of an archive, bpbrrm deletes the files from the client disk after the files are successfully backed up.</td>
</tr>
<tr>
<td>job manager service (nbjm)</td>
<td>Receives the completion status of the job from bpbrrm.</td>
</tr>
<tr>
<td></td>
<td>Releases the resources to nbrb and returns the status to nbpem.</td>
</tr>
</tbody>
</table>

Backup with multiple data streams

For multiplexed backups, the process is essentially the same. 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 are the same as shown in Figure A-1.
Figure A-2 shows multiplexed images from two clients.

**Figure A-2**  Multiplexed backups example (two streams)

**NetBackup server**

- **nbemm**
  - Mount request
  - Mount
  - File info

- **bptm** (parent)
  - Tape request
  - File info
  - Tape
  - Backup Image

- **bprm** (child)
  - File info
  - Backup Image
  - Tape

- **bpbkar**
  - File info
  - Backup Image
  - Client disk

**UNIX client**

- **bpcd**
  - File info
  - Client disk

**Notes:**

* For details on these components, see the Media and Device Management Functional Description later in this chapter.

** If the server is backing up itself (server and client on same host), there is no bptm child: bpbkar sends the data directly to shared memory.

---

**Snapshot backup and Windows open file backups**

Figure A-3 shows the overall snapshot backup process. PBX (not shown in the diagram) must be running for NetBackup to operate.
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 $\texttt{bprd}$ 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 685.
- *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 on snapshot backups involving Snapshot Client, refer to the following:
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 EMM database with the information. (FSM runs in the same process as EMM.) 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-4** shows the server and client components that are unique to SAN client backup over Fibre Channel.
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). nbrb returns information on the use of shared memory for SAN Client.

nbjm starts the backup by means of the client daemon bpcd, which starts the backup and restore manager bpbrm.

bpbrm starts bptm. bptm 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). 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 bpbkar by means of bpcd. bpbkar 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, and writes the data to the shared buffer.
- When the buffer is full or the job is done, sets buffer flag.

The FT Client process nbftclnt waits for the shared memory buffer flag to be set. nbftclnt then transfers the image data to the FT Server (nbftsrvr) shared memory buffer, and clears the buffer flag.

nbftsrvr waits for data from nbftclnt; 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-5 shows the Windows client processes.

In this figure, the following items applies:

- **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-5  Backup and archive - Windows clients
Backups and archives - NetWare clients

NetBackup supports the same types of operations on NetWare clients as it does on UNIX clients, with the following exceptions:

■ Raw partition backups are not supported.
■ NetBackup for NetWare does not support archiving.

Figure A-6 shows the NetWare client processes.

In this figure, the following item applies:

■ For NetWare nontarget operations, the Windows-based user interface program is called NBNWNT. For NetWare target operations, the user interface program is called BP.NLM on the Netware console. The bpbbackup, bpararchive, and bplist functions are merged into the user interface programs on the clients.

■ The NetBackup NetWare client daemon is called BPCD. The bpbkar functions are merged into BPCD.

The server processes are the same as described for UNIX.
Figure A-6  Backup and archive -- NetWare 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
A 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 contain 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 typically initiates a synthetic backup. nbpem submits a request to nbjm to start the synthetic backup job. nbjm starts bpsynth. bpsynth 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:

**Phase 1 - Prepare catalog information and extents**

In phase 1, bpsynth makes a synthetic backup request to the database manager, bpdbm. bpdbm 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. Bpdbm 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 must usually be copied from each component image onto the new synthetic image.

**Figure A-7** shows how phase 1 operates.
**Phase 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 or NearStore, no resource reservation is done.

**Phase 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. bpsynth 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. **Figure A-8** illustrates how phase 3 operates.

**Figure A-8** Synthetic backup -- copy data phase

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.

**Phase 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 the following:

- That True Image Restore (TIR) with move detection be selected for each component image.
- That the component images are synthetic images.

**NetBackup online, hot catalog backup**

Online, hot catalog backup. This type of 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. The catalog backup is performed online, meaning that the catalog is not turned off. More details are available.

See “Hot catalog backup process” on page 650.

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.

**Hot catalog backup process**

Figure A-9 shows the hot catalog backup that is followed by the backup process itself.
A hot catalog backup consists of the following jobs that run on the master server:

- A parent job that is started manually by the administrator or by a catalog backup policy schedule.
- A child job that backs up the NetBackup relational database files.
- A child job that copies the NetBackup database files on pre-6.0 media servers, if any.
- A child job that backs up the NetBackup database files (all files in `/usr/openv/netbackup/db`).

A hot catalog backup process is as follows (in the order presented):

- A manual backup or a catalog backup policy initiates the backup.
nbem submits a parent job to nbjm; nbjm sends a request to bpdbm.

bpdbm handles the backup of the relational database files, in two steps:

- 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.
- 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.

NetBackup backs up the database files that are in /usr/openv/netbackup/db and important NetBackup files to the master server.

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

**Note:** If the EMM server is on its own host (separate from the master server), consult this log on the EMM server: /usr/openv/netbackup/logs/admin (UNIX), or install_path\NetBackup\logs\admin (Windows).

For messages pertaining only to the relational database files, see the progress log file in the following directory:

- /usr/openv/netbackup/logs/user_ops/dbext/logs (UNIX)
- install_path\NetBackup\logs\user_ops\dbext\logs (Windows)

## Restore processes

NetBackup restore operations, like backups, can vary according to client type. The following explains the variations.

### Restoring UNIX and Linux clients

Before starting a restore, a user browses the file catalog to list the files available in the backup images. The desired files can then be selected from the list.

The browsing is done through the `bplist` program on the client. The `bplist` program can be started directly from the command line and the NetBackup user interface programs can use it.

`bplist` obtains the file list by sending a query to the request daemon, `bprd`, on the master server (see Figure A-10).
The request daemon, in turn, queries `bpdbm` for the information and transmits it to `bplist` on the client.

**Figure A-10** List operation - UNIX and Linux client

Refer to one of the following topics as you read through the restore process.

See Figure A-11 on page 655.

See Figure A-12 on page 656.

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.
The `bptm` process identifies which media (disk or tape) 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).

For tape, `bptm` asks `ltid` to mount the tape in the drive. For disk (such as AdvancedDisk or OpenStorage), `nbrb` tells `nbemm` to issue the mount by means of `nbrmms`, after `nbemm` allocates the resources.

For restore from non-shared disk (BasicDisk, PureDisk, NearStore, SnapVault), `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.

When the allocation is granted to it, `bptm` starts retrieving data. `bptm` stores the image block-by-block in shared memory.

`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.

PBX must be running for NetBackup to operate (PBX is not shown in the next diagram).

See “Resolving PBX problems” on page 66.

Figure A-11 shows how to restore from tape in the UNIX and Linux environments:
Figure A-11  Restore from tape (UNIX and Linux)

***Figure A-12*** shows how to restore from disk in the UNIX and Linux environments:
Figure A-12  Restore from disk (UNIX and Linux)

Master server

UNIX client

Master or media server

Disk volume

Backup Image

Mount request

Mount

Note:
* If the server is restoring its own data (server and client on same host), there is no bptm child: tar reads the data directly from shared memory.

Restoring SAN client (UNIX or Windows)

Figure A-13 shows the server and client components that are used in a restore of a SAN client over Fibre Channel.
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 \texttt{bprd} starts the backup and restore manager on the master server. If the disk unit or tape unit connects to a media server, \texttt{bprd} starts the backup and restore manager on the media server.

\textbf{bpbrm} starts \texttt{bptm} and provides \texttt{bptm} with the backup ID and the \texttt{shmfat} (shared memory) flag.

\textbf{bptm} does the following:

- Requests SAN Client information from \texttt{nbjm}.
- Sends a restore request to the FT server process (\texttt{nbftsrvr}).
- Sends a restore request to the FT Client process on the client (\texttt{nbftclnt}). 
  \texttt{nbftclnt} opens a fibre channel connection to \texttt{nbftsrvr} on the media server, allocates shared memory, and writes shared memory information to the backup ID file.

\textbf{bpbrm} starts \texttt{tar} by means of \texttt{bpcd} and provides \texttt{tar} with the backup ID, socket information, and the \texttt{shmfat} (shared memory) flag.

\textbf{bptm} does the following:

- Reads the image from the storage device.
- Creates a \texttt{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).

\textbf{tar} does the following:

- Sends the status and control information to \texttt{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 \texttt{shmfat} (shared memory) flag is provided, \texttt{tar} considers the data to be already filtered.

The FT Server process \texttt{nbftsrvr} waits for the shared memory buffer flag to be set. \texttt{nbftsrvr} then transfers the image data to the FT Client (\texttt{nbftclnt}) shared memory buffer, and clears the buffer flag.

The FT Client (\texttt{nbftclnt}) waits for the data from \texttt{nbftsrvr} and writes the data to the shared memory buffer on the client. \texttt{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.

**Restoring Windows clients**

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-14** shows the client processes involved in these operations.
Restoring NetWare clients

NetBackup supports the same types of restore operations on NetWare clients as it does on UNIX clients. Figure A-15 shows the client processes involved in these operations. In this figure, the following applies:

- The NetWare nontarget user interface program is called NBNWNT. The NetWare target user interface program is BP on the Netware console. The bprestore function and the bplist function are merged into the user interface programs on the clients.
- The NetBackup NetWare client daemon is called BPCD. The NetBackup tar functions are merged into BPCD.
- mtfrd functionality (used to restore Backup Exec images) has been merged into BPCD. The server processes involved in import and restore operations for Backup Exec images are the same as those involved for NetBackup restores.

The server processes are the same as described for UNIX.

**Figure A-15** shows the restore operation for a NetWare client

**Figure A-15**  
**Restore - NetWare client**

---

**Server**

For details on the server processes, see *Backups and Archives – UNIX Clients* earlier in this chapter.

**NetWare client**

NetBackup user interface

NBNWNT (NetWare nontarget)

bprd  
Request

bptm  
Backup Image

BPCD (NetWare)

Client disk
Restoring catalog backups

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 569.

Figure A-16 illustrates the catalog restore and recovery process.

**Figure A-16**  Catalog restore and recovery

See “Restore from tape (UNIX)” or “Restore from disk”, depending on the catalog backup policy.
A restore of the NetBackup database and relational database files from a hot catalog backup consists of the following steps (in the order presented):

- The NetBackup database files are restored by means of the standard NetBackup restore procedure.
- The relational database files are restored by means of the standard NetBackup restore procedure. The database files are restored to /usr/openv/db/staging (UNIX and Linux), or to \install\path\NetBackupDB\staging (Windows).
- After the files are restored to the staging directory, the relational database is recovered. Each transaction log in the staging area is applied in order, one by one.
- The relational database files are moved from the staging directory to a location determined by the following: the bp.conf file VXDBMS_NB_DATA setting on UNIX or Linux and by the corresponding registry key on Windows. The default location is /usr/openv/db/data on UNIX and Linux, 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.


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 and Linux), or \install\path\NetBackup\logs\admin (Windows).
- For messages that are related to the first two bulleted items, consult the tar, bpbm, 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 and Linux), or \install\path\NetBackup\logs\user_ops\root\logs (Windows).

**NetBackup directories and files**

Figure A-17 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-17* lists the items that are described in tables on the following pages.

**Table A-2** describes the /usr/openv/ files and directories.
<table>
<thead>
<tr>
<th>File or directory in /usr/openv/</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>bin/</td>
<td>Contains miscellaneous executable binaries including the vnetd daemon and utilities for legacy enhanced authentication.</td>
</tr>
<tr>
<td>db/</td>
<td>Contains the NetBackup Relational Database Manager (SQL Anywhere) and database data file.</td>
</tr>
<tr>
<td>java/</td>
<td>Contains the NetBackup-Java Administration Console and the Backup, Archive and Restore user interface.</td>
</tr>
<tr>
<td>lib/</td>
<td>Contains shared libraries that are required for NetBackup operation.</td>
</tr>
<tr>
<td>logs/</td>
<td>Contains all logs that are written by unified logging. You do not have to create subdirectories for these logs.</td>
</tr>
<tr>
<td>man/</td>
<td>Contains man pages for NetBackup commands.</td>
</tr>
<tr>
<td>msg/</td>
<td>Contains the message files and a configuration file for all installed languages of NetBackup.</td>
</tr>
<tr>
<td>NB-Java.tar.Z</td>
<td>A tar file that contains the NetBackup-Java interfaces.</td>
</tr>
<tr>
<td>netbackup/</td>
<td>See Table A-3 on page 666.</td>
</tr>
<tr>
<td>resources/</td>
<td>Contains the NetBackup message catalogs that are used by unified logging (VxUL).</td>
</tr>
<tr>
<td>share/</td>
<td>Contains static configuration files. These files are normally unchanged between NetBackup releases.</td>
</tr>
<tr>
<td>tmp/sqlany</td>
<td>Contains the NetBackup Relational Database Manager (SQL Anywhere) installation trace files, and the log files regarding to database start and stop.</td>
</tr>
<tr>
<td>var/</td>
<td>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.</td>
</tr>
<tr>
<td>volmgr/</td>
<td>Contains the media and device management directories and files. See “NetBackup directory structure - UNIX” on page 664.</td>
</tr>
</tbody>
</table>
Contents of `/usr/openv/netbackup`

Table A-3 describes the `/usr/openv/netbackup` files and directories.

Table A-3  Directories and files in `/usr/openv/netbackup/` - servers and UNIX clients

<table>
<thead>
<tr>
<th>File or Directory in <code>/usr/openv/netbackup/</code></th>
<th>Contents</th>
</tr>
</thead>
</table>
| `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, Vol 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. Do not install this directory on a media server. |
| `db/`                                       | NetBackup catalogs.  
  See Table A-5 on page 681. |
| `dbext/`                                     | For NetBackup database agent software, contains the version file, compressed tar file, and `install_dbext` script. |
| `help/`                                     | Help files that are used by NetBackup programs. These files are in ASCII format. |
Table A-3  Directories and files in /usr/openv/netbackup/ - servers and UNIX clients (continued)

<table>
<thead>
<tr>
<th>File or Directory in /usr/openv/netbackup/</th>
<th>Contents</th>
</tr>
</thead>
</table>
| logs/                                    | Legacy debug logs for NetBackup processes. You must create the necessary subdirectories in order for these log files to be written.  
See “Legacy NetBackup logging” on page 101.  
See Table A-4 on page 668. for an explanation of the processes that produce the logs. |
| nblog.conf                               | Specifies the settings for unified logging.  
**Note:** Do not edit this file manually: use the vxlogcfg command instead.  
See “Configuring and using unified logging” on page 93. |
| nblog.conf.template                      | Specifies the settings for unified logging.  
**Note:** Do not edit this file manually: use the vxlogcfg command instead.  
See “Configuring and using unified logging” on page 93. |
| 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-4 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 “Legacy NetBackup logging” on page 101.
### Table A-4: NetBackup daemons and programs

<table>
<thead>
<tr>
<th>Program/Daemon</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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.  
                  The debug logs for bpbackup, bparchive, bprestore, and bplist also have information about bp activities. |
| **BP.NLM**     | On NetWare target clients, BP.NLM is the NetWare Loadable Module that starts the client-user interface.  
                  Started By: LOAD BP command.  
                  Stopped By: Choosing Quit Utility from the main menu.  
| **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. |
<table>
<thead>
<tr>
<th>Program/Daemon</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
| bpbkar        | On UNIX clients the Backup/Archive Manager generates the backup images.  
    Started By: bpbkar 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. |
<table>
<thead>
<tr>
<th>Program/Daemon</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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. |
| **BPCD.NLM**  | On NetWare clients, **BPCD.NLM** is the executable file that starts the NetBackup client daemon. 
**Started By:** When you enter `BPSTART.NCF` at the NetWare Server console. Or, add `BPSTART.NCF` to your `autoexec.ncf` file. 
**Stopped By:** UNLOAD BP command 
**Debug Log:** BPCD legacy log directory on the client. |
| **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. |
<table>
<thead>
<tr>
<th>Program/Daemon</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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 backup or restore, 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. |
| **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. |
<table>
<thead>
<tr>
<th>Program/Daemon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bpjava-msvc</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Started By: inetd during startup of the NetBackup Java interfaces.</td>
</tr>
<tr>
<td></td>
<td>Stopped By: When authentication is complete.</td>
</tr>
<tr>
<td></td>
<td>Debug Log: bpjava-msvc legacy log directory on the server.</td>
</tr>
<tr>
<td>bpjava-usvc</td>
<td>NetBackup-Java user server application program. This program services all requests from the NetBackup-Java user and administration interfaces.</td>
</tr>
<tr>
<td></td>
<td>Started By: bpjava-msvc upon successful login through the Login dialog box that is presented when a NetBackup-Java interface is started.</td>
</tr>
<tr>
<td></td>
<td>Stopped By: When the interface program is terminated.</td>
</tr>
<tr>
<td></td>
<td>Debug Log: bpjava-usvc legacy log directory.</td>
</tr>
<tr>
<td>bplist</td>
<td>On UNIX clients, this program communicates with bprd on the master server when a user browses the database during a restore operation.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Stopped By: Completion of operation</td>
</tr>
<tr>
<td></td>
<td>Debug Log: bplist legacy log directory on the client.</td>
</tr>
</tbody>
</table>
Table A-4  NetBackup daemons and programs (continued)

<table>
<thead>
<tr>
<th>Program/Daemon</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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: Initiate Request Daemon option on the Special Actions menu in bpadm (also the `/usr/openv/netbackup/bin/initbprd` command).  
Stopped By: Terminate Request Daemon option on the Special Actions menu in bpadm.  
Debug Log: `bprd` legacy log directory on the server. |
| 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. |
| BPSVR.NLM | On NetWare nontarget clients, `BPSVR.NLM` is the program that allows the system that has the client-user interface to communicate with the Netware server that is the NetBackup client.  
Started By: Enter `bpstart.ncf`.  
Stopped By: Enter `bpstop.ncf`.  
Debug Log: `SYS:VERITAS\NBUCLT\NetBack\logs\bpsrv` directory on the client. |
| BPSYS.EXE | On Windows clients, `BPSYS.EXE` is the NetBackup System Registry Replacement utility.  
Started By: NetBackup as required.  
Stopped By: Completion of operation.  
Debug Log: `BPSYS` legacy log directory on the client. |
<table>
<thead>
<tr>
<th>Program/Daemon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bptm</strong></td>
<td>On master and media servers, <em>bptm</em> 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, <em>bpbrm</em> starts an instance of <em>bptm</em> on the server that has the storage unit. Stopped By: Completion of operation. Debug Log: <em>bptm</em> legacy log directory on the server.</td>
</tr>
<tr>
<td><strong>jbpSA</strong></td>
<td>A Java-based program for performing backups, archives, and restores of UNIX clients. Started By: On UNIX, the <code>/usr/openv/netbackup/bin/jbpSA</code> command. Debug Log: None, although the logs for the <em>bpbackup</em>, <em>bparchive</em>, <em>bplist</em>, and <em>bprestore</em> commands on the client can be useful. Also, check the <em>bpjava-msvc</em> and <em>bpjava-usvc</em> logs.</td>
</tr>
<tr>
<td><strong>jnbSA</strong></td>
<td>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 <code>/usr/openv/netbackup/bin/jnbSA</code> command. On a NetBackup-Java Windows Display console, the NetBackup - Java on <em>host</em> menu item on the Programs/NetBackup menu. Stopped By: Exit option in <em>jnbSA</em>. Debug Log: None, although the logs for <em>bpjava-msvc</em> and <em>bpjava-usvc</em> can be helpful.</td>
</tr>
<tr>
<td>Program/Daemon</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **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/nbemmm
-terminate  
  **Debug Log:** On the server, /usr/openv/logs (UNIX) or install_path\logs (Windows).  
  See “Unified logging” on page 83. |
| **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\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 nbftcint 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\logs (Windows).  
  See “Unified logging” on page 83. |
<table>
<thead>
<tr>
<th>Program/Daemon</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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/logs (Windows).  
See “Unified logging” on page 83. |
| 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/logs (Windows).  
See “Unified logging” on page 83. |
| 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/logs (Windows).  
See “Unified logging” on page 83. |
| NBNWNT.EXE    | For NetWare nontarget clients, NBNWNT.EXE is the executable file that starts the client-user interface on Windows systems.  
Started By: From the Windows Start menu, under Programs/NetBackup.  
Stopped By: Exiting the client-user interface.  
Debug Log: none. |
### Table A-4  NetBackup daemons and programs (continued)

<table>
<thead>
<tr>
<th>Program/Daemon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nbpem</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Started By: Started when NetBackup starts.</td>
</tr>
<tr>
<td></td>
<td>Stopped By: /usr/openv/netbackup/bin/nbpem -terminate</td>
</tr>
<tr>
<td></td>
<td>Debug Log: On the server, /usr/openv/logs (UNIX) or install_path\logs (Windows).</td>
</tr>
<tr>
<td></td>
<td>See “Unified logging” on page 83.</td>
</tr>
<tr>
<td>nbproxy</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Started By: the process that uses nbproxy as a proxy.</td>
</tr>
<tr>
<td></td>
<td>Stopped By: stops the process that uses nbproxy.</td>
</tr>
<tr>
<td></td>
<td>Debug Log: nbproxy legacy log directory on the server.</td>
</tr>
<tr>
<td>nrbbr</td>
<td>On the server that is defined as the EMM server, the nrbbr service accepts resource requests from nbjm, acquires physical resources from nbemm, and manages logical resources.</td>
</tr>
<tr>
<td></td>
<td>Started By: Started when NetBackup starts.</td>
</tr>
<tr>
<td></td>
<td>Stopped By: /usr/openv/netbackup/bin/nrbbr -terminate</td>
</tr>
<tr>
<td></td>
<td>Debug Log: On the server, /usr/openv/logs (UNIX) or install_path\logs (Windows).</td>
</tr>
<tr>
<td></td>
<td>See “Unified logging” on page 83.</td>
</tr>
<tr>
<td>ndmpagent</td>
<td>Controls backup and restore operations on a NAS server. ndmpagent 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.</td>
</tr>
<tr>
<td></td>
<td>Started By: bpbrm.</td>
</tr>
<tr>
<td></td>
<td>Stopped By: Completion of backup or restore.</td>
</tr>
<tr>
<td></td>
<td>Debug Log: On the server, /usr/openv/logs (UNIX) or install_path\logs (Windows).</td>
</tr>
<tr>
<td></td>
<td>See “Unified logging” on page 83.</td>
</tr>
</tbody>
</table>
### Table A-4  NetBackup daemons and programs (continued)

<table>
<thead>
<tr>
<th>Program/Daemon</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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\logs (Windows)`. For more information about OID 226 and 272, see the following topic:  
See “Server processes that use unified logging” on page 86. |
| NBWIN.EXE      | For Windows clients, NBWIN.EXE is the executable file that starts the client-user interface on Windows systems.  
Started By: From the Windows Start menu, under Programs/NetBackup.  
Stopped By: Exiting the client-user interface.  
Debug Log: NBWIN legacy log directory on the client. |
| 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, nbrmms 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\logs (Windows)`.  
See “Unified logging” on page 83. |
<table>
<thead>
<tr>
<th>Program/Daemon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pbx_exchange</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Started By: Started when NetBackup starts, or by /opt/VRTSpbx/bin/vxpbx_exchanged start</td>
</tr>
<tr>
<td></td>
<td>Stopped By: Stopped when NetBackup stops, or by /opt/VRTSpbx/bin/vxpbx_exchanged stop</td>
</tr>
<tr>
<td></td>
<td>Debug Log: On the server, /opt/VRTSpbx/log (UNIX) or install_path\VxPBX\log (Windows). See “PBX logging” on page 68.</td>
</tr>
<tr>
<td>ql2300_stub</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Stopped By: Device driver that is stopped by nbfdrv64 on Linux and nbftsrv_config on Solaris.</td>
</tr>
<tr>
<td></td>
<td>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).</td>
</tr>
<tr>
<td>tar</td>
<td>On UNIX clients, the Tape ARchive program is a special version of tar provided with NetBackup and used to restore images.</td>
</tr>
<tr>
<td></td>
<td>Started By: For each restore, bpbrm starts an instance of tar on the client.</td>
</tr>
<tr>
<td></td>
<td>Stopped By: Completion of restore operation.</td>
</tr>
<tr>
<td></td>
<td>Debug Log: tar legacy log directory on the client.</td>
</tr>
</tbody>
</table>
Table A-4  NetBackup daemons and programs (continued)

<table>
<thead>
<tr>
<th>Program/Daemon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAR32</td>
<td>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.</td>
</tr>
<tr>
<td>windrvr6</td>
<td>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).</td>
</tr>
</tbody>
</table>

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.

Note also that 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-5 describes the NetBackup catalogs.
Table A-5  NetBackup catalogs

<table>
<thead>
<tr>
<th>Database</th>
<th>Contents</th>
</tr>
</thead>
</table>
| 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.  |
| 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.  |
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). `ltid` automatically starts other daemons and programs as necessary. The daemons should be running after initial startup.

See Figure B-1 on page 685.

In the case of robotic daemons, such as `tl8d` and `tlhd`, the associated robot must also be configured for the daemon to run. There are also additional ways to start and stop daemons.

See Table B-1 on page 692.

TL8, TLH, and TLD require following types of daemons:
Each host with a robotic drive attached must have a robotic daemon. These daemons provide the interface between ldid and the robot or, if different drives within a robot can attach to different hosts, the robotic daemon communicates with a robotic-control daemon (see below).

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 and then communicates these requests to the robot.

You must know the hosts involved in order to start all the daemons for a robot.
Media and device management process

When the media and device management daemons are running, NetBackup, Storage Migrator (UNIX only), Storage Migrator for Microsoft Exchange (Windows only), or users can request data storage or retrieval. The request is initially handled by the scheduling services.

See “Backup and archive processes” on page 632.
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 687.

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 then insert the media in the robot and use the appropriate Device Monitor command to resubmit the request so the mount request can occur.

A mount request is also issued if the media is for a nonrobotic (standalone) drive and the drive does not contain 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. More information is available on NetBackup media selection for nonrobotic drives.

See the *NetBackup Administrator’s Guide, Volume II*.

---

**Note:** On UNIX systems, when a tape is being mounted, 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 and/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.
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 (stand-alone or in a robotic library) to be dynamically shared between multiple NetBackup media servers or SAN media servers.

See the *NetBackup Shared Storage Guide*.

The following shows the shared storage option management process in the order presented:

- NetBackup, Storage Migrator, or users can initiate backups. nbjm 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. See “How NetBackup reserves drives” in 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.
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 mounting
the tape. A request for media that is in a robot that can read barcodes begins in
the same manner as other requests.

See Figure B-4 on page 691.

ltid 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).
Media and device management components

This topic shows the file and directory structure and the programs and daemons associated with the media and device management.

Figure B-5 shows the file and directory structure for media 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>
<thead>
<tr>
<th>File or directory</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>bin</td>
<td>Commands, scripts, programs, daemons, and files required for media and device management. There are three subdirectories under bin. driver: Contains SCSI drivers used on various platforms to control robotics. format: Disk format information for optical platters on Solaris (SPARC only) platforms. goodies: Contains vmconf script and scan utility.</td>
</tr>
<tr>
<td>debug</td>
<td>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.</td>
</tr>
<tr>
<td>help</td>
<td>Help files used by media and device management programs. These files are in ASCII format.</td>
</tr>
<tr>
<td>misc</td>
<td>Lock files and temporary files required by various components of media and device management.</td>
</tr>
</tbody>
</table>
**Table B-1**  Media and device management directories and files *(continued)*

<table>
<thead>
<tr>
<th>File or directory</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>vm.conf</td>
<td>Media and device management configuration options.</td>
</tr>
</tbody>
</table>

**Table B-2** describes the media 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

<table>
<thead>
<tr>
<th>Program or daemon</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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*. |
| acsssi            | Available only on UNIX.  
  See the *NetBackup Device Configuration Guide*. |
### Table B-2: Media and device management daemons and programs (continued)

<table>
<thead>
<tr>
<th>Program or daemon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>avrd</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Started By:</strong> Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/avrd command).</td>
</tr>
<tr>
<td></td>
<td><strong>Stopped By:</strong> Stopping ltid, (or on UNIX, independently by finding the PID (process id) and then using the kill command).</td>
</tr>
<tr>
<td></td>
<td><strong>Debug Log:</strong> All errors are logged in the system log. Debug information is included by adding VERBOISE to the vm.conf file. On UNIX, debug information is also included by aborting avrd and starting the daemon with the -v option.</td>
</tr>
<tr>
<td>ltid</td>
<td>The device demon (UNIX) or NetBackup Device Manager service (Windows) controls the reservation and assignment of tapes and optical disks.</td>
</tr>
<tr>
<td></td>
<td><strong>Started By:</strong> /usr/openv/volmgr/bin/ltid command on UNIX or Stop/Restart Device Manager Service command in Media and Device Management window on Windows.</td>
</tr>
<tr>
<td></td>
<td><strong>Stopped By:</strong> /usr/openv/volmgr/bin/stopltid command on UNIX or Stop/Restart Device Manager Service command in the Media and Device Management window on Windows.</td>
</tr>
<tr>
<td></td>
<td><strong>Debug Log:</strong> 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 VERBOISE to the vm.conf file.</td>
</tr>
<tr>
<td>oddld</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Started By:</strong> Starting ltid or independently by using the /usr/openv/volmgr/bin/odld command.</td>
</tr>
<tr>
<td></td>
<td><strong>Stopped By:</strong> Stopping ltid or independently by finding the PID (process id) and then using the kill command.</td>
</tr>
<tr>
<td></td>
<td><strong>Debug Log:</strong> 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 VERBOISE to the vm.conf file.</td>
</tr>
<tr>
<td>Program or daemon</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 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). |
| 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). |
<table>
<thead>
<tr>
<th>Program or daemon</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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). |
| 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). |
### Table B-2  Media and device management daemons and programs (continued)

<table>
<thead>
<tr>
<th>Program or daemon</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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>
<thead>
<tr>
<th>Program or daemon</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
<table>
<thead>
<tr>
<th>Program or daemon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tpconfig</td>
<td>The Tape Library Multimedia daemon is the interface between ltid and a TLM robot that is in a ADIC Distributed AML Server (DAS). This daemon communicates with the TLM robotics through a network API interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Started By:</strong> Starting ltid or independently by using the <code>/usr/openv/volmgr/bin/tlmd</code> command.</td>
</tr>
<tr>
<td></td>
<td><strong>Stopped By:</strong> Stopping ltid or independently by finding the PID (process id) and then using the <code>kill</code> command.</td>
</tr>
<tr>
<td></td>
<td><strong>Debug Log:</strong> Errors are logged in the system log and robots debug log. Debug information is included if the daemon is started with the <code>-v</code> option (either by itself or through ltid). The <code>-v</code> option is available only on UNIX. Also, add the <code>VERBOSE</code> option to the <code>vm.conf</code> file.</td>
</tr>
<tr>
<td>tshd</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Started By:</strong> Starting ltid (or on UNIX, independently by using the <code>/usr/openv/volmgr/bin/tshd</code> command).</td>
</tr>
<tr>
<td></td>
<td><strong>Started By:</strong> <code>tpconfig</code> command.</td>
</tr>
<tr>
<td></td>
<td><strong>Stopped By:</strong> Quit option from within the utility on UNIX. On Windows, <code>tpconfig</code> is only a command-line interface that runs to completion (no quit option).</td>
</tr>
<tr>
<td></td>
<td><strong>Debug Log:</strong> <code>tpcommand</code> debug logs.</td>
</tr>
<tr>
<td>vmd</td>
<td>The Volume Manager daemon (NetBackup Volume Manager service on Windows) allows remote administration and control of Media and Device Management. vmd provides a proxy to EMM for pre-6.0 NetBackup servers.</td>
</tr>
<tr>
<td></td>
<td><strong>Started By:</strong> Starting ltid (or on UNIX, independently by using the Initiate Media Manager Volume Daemon option in <code>vmadm</code>)</td>
</tr>
<tr>
<td></td>
<td><strong>Stopped By:</strong> Terminate Media Manager Volume Daemon option in <code>vmadm</code>).</td>
</tr>
<tr>
<td></td>
<td><strong>Debug Log:</strong> System log and also a debug log if the daemon or reqlib debug directories exist</td>
</tr>
<tr>
<td>Program or daemon</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **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) |
Networks and hostnames

This appendix includes the following topics:

- Background for troubleshooting

Background for troubleshooting

In a configuration with multiple networks and clients with more than one hostname, NetBackup administrators must configure the policy entries carefully. They must consider the network configuration (physical, hostnames 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 is defined by the system’s routing tables. 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 peername of its connection to the server.

The peername is derived from the IP address of the connection. This means that the address must translate into a host name (using the gethostbyaddr() network
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 peername by querying the `bpdbm` process on UNIX systems. On Windows systems, you must query the NetBackup Database Manager service.

The `bpdbm` process compares the peername 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 hostnames and 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 hostname 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 had changed its hostname but its new hostname 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:

- Peername 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 peername 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.

- Client backup and archive images that already exist as recorded in the images directory on the master server. On a UNIX or Linux 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 and Linux)
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 hostnames. 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 is obtained by the client’s `gethostname()` function and sent to the server in the request.
- `client_as_known_by_server` is the name to substitute for `hostname_from_client` when responding to requests. This name must be the name 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:
When the master server receives a request for a configured client name (numeric key 0), the name danr is always replaced by the name danr.eng.aaa.com. 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.
Robotic test utilities

This appendix includes the following topics:

■ About robotic test utilities
■ Robotic tests on UNIX
■ Robotic tests on Windows

About 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:

  \texttt{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 \texttt{robtest} and must execute the command that applies to the robot you are testing (see following list).

<table>
<thead>
<tr>
<th>Robot</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACS</td>
<td>\texttt{install_path\Volmgr\bin\acstest -r ACSLS_HOST}</td>
</tr>
<tr>
<td>TL4</td>
<td>\texttt{install_path\Volmgr\bin\tl4test -r roboticpath}</td>
</tr>
<tr>
<td>TL8</td>
<td>\texttt{install_path\Volmgr\bin\tl8test -r roboticpath}</td>
</tr>
<tr>
<td>TLD</td>
<td>\texttt{install_path\Volmgr\bin\tlldtest -r roboticpath}</td>
</tr>
<tr>
<td>TLH</td>
<td>\texttt{install_path\Volmgr\bin\tlhtest -r robotic_library_name}</td>
</tr>
<tr>
<td>TLM</td>
<td>\texttt{install_path\Volmgr\bin\tlmtest -r DAS_Hostname}</td>
</tr>
</tbody>
</table>

More information on ACS, TLH, and TLM robotic control is available. See the \textit{NetBackup Device Configuration Guide}.

In the previous list of commands, \texttt{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 \texttt{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:

\texttt{install\_path <-p port \ -b bus \ -t target \ -l lan \ | -r roboticpath>}

where: \texttt{roboticpath} is the changer name (e.g., Changer0).
backup (continued)
   synthetic processes 647
   UNIX clients 633
Backup Status report 82
Bare Metal Restore 570, 573, 586
base NetBackup license key 178
bin
   Media and Device Management 692
   UNIX client 665–666
BP 660
bp
   description 668
   log 117
   UNIX client log 114
bp.conf
   file 634
   UNIX client/server 666
   SERVER entries 72
bp.kill_all 69, 71, 176
BP.NLM 646, 668
bp.start_all 71, 176
bpadm
   description 668
bparchive
   description 668
   log 114, 117
bpbackup
   description 669
   log 114, 117
bpbackup log 117
BPBACKUP_POLICY 634
BPBACKUP_SCHED 634
bpbackupdb and catalog backup 208
bpbkar
   description 669
   log 114, 117
bpbkar and VxFS_Checkpoint 242
bpbkar log 117
BPBKAR32 645, 669
bpbrm 641
   description 669
bpbrm log 102
bpsched
   see also nbpem 677
bpsrv
   log 118
bpsrv log 118
BPSVR.NLM 673
bpsynth 648
BPSYS.EXE 673
bptm
   description 674
bptm log 103
bptpcinfo 77
bpup command 71, 176, 582, 585
bundling
   NBCC output 147
   nbsu output 138

C

cache
   partition 171
catalog backup 650
checkpoint
   removing 242
class database file 681
client
   NetBackup
      configured name 702
dbms. See UNIX clients. See Windows
   and NetWare clients
   installation problems 28
   multiple hostnames 701
   peername 702
   software location. See UNIX clients
testing configuration 34, 37
Client Backups report 82
Client Properties dialog 61
client, NetBackup
   Windows disk recovery 586
clone (mirror
   removing) 244–245
CommandCentral Storage 74
communications problems
   PC clients 45
   UNIX clients 40
compression
   for NBCC 147
   for nbsu 138
compression device 33
config file 681
configuration database 681
configuration device file does not exist 32
configuration problems 28

D
demons
  robotic 683
  robotic control 683
database backup (see catalog backup) 650
database extension 631
DAYS_TO_KEEP_LOGS 105
DAYS_TO_KEEP_LOGS vm.conf setting 108
db directory
  NetBackup 665–666
debug level 116, 120, 126
debug logs 83, 125
  analysis utilities 129
  NetBackup 692
  vmd 105, 692
debug.properties file 125
debugging
  NBCC 147
  nbsu 140
define the problem 13
device configuration problems 30
Device Configuration Wizard 581
directory structure
  Media and Device Management 691
disk full 61
disk recovery
  Windows client 586
disk space
  for logs files 99
drive
  type not determined 32
  drive_mount_notify script 686
  driveUnmount_notify script 686
driver directory 692
duplex mode and performance 71
error codes (see status codes) 154
error database 681
evaluation license key 178
Event viewer logging option 120
eventlog 121
  file entries 121
exception errors in Java admin interface 123
expired license key 178

F
failure_history file 681
fibre channel 642
file database 681
file list
  symbolic link 240
file pathname (max length) 155
files
  archive process 632
  backup process 632
  restore process 652
format directory 692
frozen image
  source
    for symbolic link 240
fsckptadm command 243
FSM 642
FT Service Manager 642
full disk 61
full duplex mode 71
functional overview
  introduction 631
  Media and Device Management
    device management 685
    directories and files 691
    volume management 685
NetBackup
  backup and archive 632
  restores 652
  startup 632

G
Global Logging Level 110
Global logging level 90–91
goodies
directory 666
goodies directory 692
### H
- Half duplex and poor performance 71
- Help files
  - Media and Device Management 692
  - UNIX client 666
- Host name entries
  - Checking 48
- Host Properties 60
- Host.xlate file 704
- HostID
  - Unified logging 85

### I
- IDR 579, 586
- ifconfig
  - For checking NIC duplex mode 72
- Images database 681
- Images on Media report 82
- inetd 27
- Information E-mail 572
- Installation
  - Linux 27
- Installation problems 27
- Intelligent Disaster Recovery (IDR) 579, 586
- ipconfig
  - For checking NIC duplex mode 72

### J
- Java interface
  - Debug logging 125
  - Troubleshooting background 123
- jbpSA
  - Overview 674
- Job ID search in unified logs 94
- Jobs
  - Queued for long periods 61
- Jobs database 681

### K
- Keep logs For setting 93
- Keep Logs setting 107
- Key value 254

### L
- Legacy logging (continued)
  - Controlling size of 107
  - Directories 102
  - File name format 109
  - Locations 101
  - PC clients 116
  - Rotation of 107
- Levels for logging 90
- Libsfr.so file 159
- License key 178
- License problems 31–32
- Links (in file list) 240
- Linux 27
- Local system account 239
- Log (bppfi) 247
- Log analysis utilities
  - Debug logs 129
  - How to run 131
  - Installation 130
  - Limitations 131
  - Output format 130
- Log level
  - Windows and NetWare clients 116, 120
- Logging
  - Changing location of 84
  - Levels 90
  - See legacy logging 101
  - Setting level for clients 116
  - Setting level on PC clients 120
  - Synthetic backup 111
  - VxUL (see unified logging) 83
- Logs
  - Activity
    - See debug 83
  - Debug
    - Enabling detailed 125
    - Introduction 83
  - Event viewer logging option 120
  - File retention 93
  - Overview [Logs]
    - AAA 79
  - PC client activity
    - BP 117
    - Bparchive 117
    - Bpbackup 117
    - Bpbkar 117
    - Bpcd 117
    - Bpxcon 117
    - Bpinetd 117
    - Bplist 118
  - PC client logs 113
  - Configuring rotation 109
Index | 715

logs (continued)

PC client activity (continued)

bpmount 118
bprestore 118
bpspsrv 118
tar 118
user_ops 119

reports

NetBackup 81

server activity

acssi 105
admin 102
bpbrm 102
bpcl 102
bpdbjobs 102
bpdm 102
bpdm 102
bpjava-susvc 103
bpdrd 103
bpsynth 103
bptm 103–104
daemon 105
ltid 105
nbj 86
nbpem 86
nrb 86
reqlib 106
robots 106
tpcmd 106

setting retention period 105, 107

system 83

UNIX client activity

bp 114
bparchive 114
bpbackup 114
bpkkar 114
bpcl 114
bpdm 114
bpjava-msvc 103
bplist 114
bpmount 114
bprestore 114
obbackup_tape 115
tar 115
user_ops 115
user progress 83
logs directory

UNIX client/server 667

ltid 111

ltid, description 694

M

master server

test procedure 34, 37

maximum pathname length 155

MaxLogFileSizeKB 96, 98–99, 109

media database 681

Media Log Entries report 82

media server

test procedure 37

message

finding message text from status code 153

messages

NetBackup 397

messages (see status codes) 154

mirror (VxVM snapshot) 241

mirror snapshot (removing) 244–245

misc file 692

mklogdir.bat 102

moving log locations 84

multiple data streams option 172

multiplexed backups 638

multiplexing 170

N

name format

legacy logging 109

NB_dbsrv daemon 62

nbaudit 675

NBCC

archiving and compression 147

does the following 141

introduction 141

location of 142

nbcc-info.txt file 148

Notes on running 147

output 146

progress display 142

Server aliases file 145

troubleshooting 147

when to use 142

nbcc-info.txt file 148

nbdb_move 580

nbdmm 24, 633, 675

nbdrv64 675

nbftclnt 113, 116, 642, 644, 658, 676

and bp.conf 73
nbftsrvr 642, 644, 658, 676
nbjm 25, 86, 633, 641, 648, 676–677
NBNWNT 646, 660
NBNWNT.EXE 676
nb pem 25, 86, 632–633, 641, 648, 677
nb proxy 677
nrb 24, 62, 86, 633, 677
nbrmms 678
nbtserv 678
nsu
  and status codes 139
  archiving and compression 138
  bundling 138
  creating xml output file 139
  introduction 135
  location of 135
  nbsu_info.txt file 141
  output files 137
  progress display 136
  troubleshooting 140
  when to use 135
nbsu_info.txt file 141
NBWIN 645, 659
NBWIN.EXE 678
ndmpagent
  overview 677
NearStore 649
NetBackup
  if unresponsive 61
  product ID 85
NetBackup Administration Console
  debug logging 125
  errors 123
NetBackup Client Service 239
  start and stop 26
NetBackup consistency check
  see NBCC 141
NetBackup Database Manager service
  start and stop 26
NetBackup Device Manager service
  start and stop 26
NetBackup Enterprise Media Manager service
  start and stop 26
NetBackup Job Manager service
  start and stop 26
NetBackup Policy Execution Manager service
  start and stop 26
NetBackup Request Manager service
  start and stop 26
NetBackup Resource Broker service
  start and stop 26
NetBackup Status Collection daemon. See vmscd
NetBackup Support Utility
  see nbsu 135
NetBackup Volume Manager service
  start and stop 26
network connections
  multiple 701
network daemon (vnetd) 104
network interface cards 71
network problems
  PC clients 45
  UNIX clients 40
NIC cards and full duplex 71
Novell
  values affecting restore 173, 175
NumberOfFiles 99
NumberOfLogFile 98, 109

O
obackup_tape log 115
odld, description 694
odlttest 708
off-host backup 77
OpenStorage 257, 573, 579
operating system errors 124
originator IDs
  list of 86
originatorID
  unified logging 85

P
pass-thru not supported 32
patch
  troubleshooting 159
patches (installing during recovery) 588
pathname length 155
PBX
  Auth User 68
  logging 68
  Secure Mode 68–69
  starting 67
  starting/stopping 70
  troubleshooting 66
pbx_exchange 67, 679
pbxcfg 67
preliminary troubleshooting procedure 23
Private Branch Exchange (PBX) 66
problems report 82
procedures
recovery
  Windows client disk 586
troubleshooting
  communications problems 40
  host names and services 48
  installation and configuration 27
  introduction 21
  master server and clients 34
  media server and clients 37
  preliminary 23
processes (see functional overview) 631
product ID for NetBackup 85
productID
  unified logging 85
progress logs
  user 83

Q
ql2300_stub 679
query string 126
queued jobs 61

R
raw partitions
  backup process 632
  restore process 652
recording information 15
recovery procedures
  Windows client disk 586
RedHat 27
relational database 62
removing a snapshot checkpoint 242
removing a snapshot clone 244–245
reports
  NetBackup 81
  reqlib directory 107
restore
  problem with sparse file 184
restore process 652
  NetWare client 660
  Windows 2000 client 659
restoring
  NAS_Snapshot 239
retention
  of logs 93
robot
  drive number unknown 31
  type not determined 31
  unknown 31
robot drive selection 686
robotic control daemons 684
robotic daemons 684
robotic test utility 707
  acptest 709
  odltest 708
  tl4test 708–709
  tl8test 708–709
  tldtest 708–709
  tlhtest 709
  tshtest 708
robtest 707–708
robust file logging 96
RolloverMode 98
rotation
  legacy logging 107
  of logs 92
  unified logging 85

S
SAN Client 642
SAN client
  and bp.conf 73
SANPoint Control 74
Secure Mode
  for PBX 68
serialization problems 30
server
  installation problems 27
  NetBackup debug logs 101
  test procedure for master 34, 37
  test procedure for media server 37
SERVER entries
  bp.conf 72
services entries
  checking 48
SharedDisk 74, 573, 579
slow performance and NIC cards 71
snaplist command 242
snapoff command 242
snapshot
  backup process overview 640
  cache partition 171
  mirror (VxVM) 241
  removing 244–245
snapshot  (continued)
  stale 242
Snapshot Client
  pathname length 155
software version
  determining
    Macintosh clients 172
    NetWare non-target clients 172
    NetWare target clients 172
    UNIX client/server 667
    UNIX servers 172
    Windows clients 172
    Windows servers 172
sparse files (restore problem) 184
stale snapshots 242
starting NetBackup processes 71, 176
startup
  NetBackup 632
status code
  finding message from 153
status codes
  and nbsu 139
  NetBackup
    sorted by code 154
    sorted by message 397
Status Collection Daemon 107
stderr 123
stdout 123
stopping NetBackup processes 69, 71, 176
storage units 73
SuSE 27
symbolic links 240
synthetic backup 647
  logs 111
syslogd 83, 106
system logs 83

T
  tar
    log 118
    log files 101
      NetBackup 679–680
TAR32 659
  test utility
    robotic 707
third-party copy 253
  and multiplexing 170
tld, description 695
tldtest 708–709

U
  unavailable 73
unified logging 83
  changing location of 84
  client logs 113
  command examples 93
  configuring settings 96
  controlling disk space usage 99
  controlling number of log files 98
  controlling size of 96
  deleting logs 95
  file name format 85
  file rotation 92
  format of files 93
  listing settings 98
  location 83
  message types 84
  NetBackup product ID 85
  PC clients 116
  processes using 86
unified logging  (continued)
  retention  93
  setting level on PC clients  120
  settings levels  90
  submitting to support  100
  tar log files  101
  viewing  93
upload directory  101
user-directed backups  634
user_ops log  104, 115, 119
utility
  robotic test  707

V
VERBOSE  111
verbose flag  111
VERBOSE level  91
Veritas Volume Manager  241
vm.conf  105, 111
vm.conf file  693
vmadm, overview  700
vmd  105
  debug logging  105
  overview  699
vmscd  107
  logging  106
vmscd, overview  700
vnetd log  104
Volume Configuration Wizard  581
vxassist command  241, 246
VxFS_Checkpoint snapshot  242
vxlogcfg  84, 109
vxlogcfg command  91, 96, 98, 109
vxlogmgr command  95, 98
vxlogview command  93
  query string overview  126
  with job ID option  94
vxpbx_exchanged  70
vxprint command  246
VxUL logging
  see unified logging  83
vxvm frozen image method  241
vxvol command  241

W
Windows open file backup  640
windrvr6  680

X
xinetd  27
XML  114
xml
  for nbsu  139