Veritas NetBackup™ Troubleshooting Guide

UNIX, Windows, Linux

Release 6.5

12308352

symantec™

Veritas NetBackup Troubleshooting Guide

Copyright © 1998 - 2007 Symantec Corporation. All rights reserved.

NetBackup 6.5

Symantec, the Symantec logo, and NetBackup 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.

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

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.

THIS 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” and “commercial computer software documentation” as defined in FAR Sections 12.212 and DFARS Section 227.7202.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
www.symantec.com

Printed in the United States of America.

Third-party legal notices

Third-party software may be recommended, distributed, embedded, or bundled with this Symantec product. Such third-party software is licensed separately by its copyright holder. All third-party copyrights associated with this product are listed in the accompanying release notes.

Licensing and registration

Veritas NetBackup is a licensed product. See the *NetBackup Installation Guide* for license installation instructions.

Technical support

For technical assistance, visit http://entsupport.symantec.com and select phone or email support. Use the Knowledge Base search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and our customer email notification service.

Contents

Chapter 1 Introduction

Chapter 2 Troubleshooting procedures

Appendix A Functional overview

Appendix B Networks and hostnames

Introduction

This chapter explains the steps to take if you encounter a problem while using 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 "Using logs and reports" chapter describes the log information that NetBackup provides. The following chapters provide interpretations of NetBackup (and Media Manager) status codes and messages: "NetBackup status codes and messages" and "Media and device management 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 was the attempted operation?
- 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:

- 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 attempt. A benefit of this approach is that you can compare the results of multiple attempts. A record of attempts is also useful for others at your site and for customer support in the event that you cannot solve the problem.

The “Using logs and reports” chapter explains the various logs.

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 attempt is unsuccessful, customer support can provide further assistance. Before you call, have the following information ready.

- 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 sending information such as copies of logs.

“Problem report information” on page 15 lists the information you need and also provides methods for gathering information.

Troubleshooting the problem

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

- When you have a status code or message, proceed directly to “NetBackup status codes and messages” or “Media and device management status codes and messages”. Try the recommended corrective actions there.
- If no status code or message exists, or the actions in the status code chapters do not solve the problem, try the “Troubleshooting procedures” chapter. Those procedures describe an effective approach for isolating common problems.

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

Note: The Symantec technical support site has a wealth of information that can help you solve NetBackup problems. See http://entsupport.symantec.com for comprehensive troubleshooting details.

Problem report information

General information

Date: ______________________

Table 1-1 Servers (master and media)

Platform types and host names	OS Levels	Product version and patch levels

Table 1-2 Clients

Platform types and host names	OS Levels	Product version and patch levels

Table 1-3 Devices

Robotic library and drive models	Firmware levels	Firmware level that is listed as “tested” in the Veritas Device Compatibility Lists at www.support.veritas.com

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

____

____

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

____

____

____

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

_____ Initial installation

_____ Configuration change (explain)

_____ System change or problem (explain)

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

Logs or other failure data you have saved:

_____ All log entries report

_____ Media and Device Management debug logs

_____ NetBackup debug logs

_____ System logs (UNIX)

_____ NetBackup Configuration Validation Utility Output (UNIX)

_____ Event Viewer Application and System logs (Windows)

Can you communicate with us through any of the following:

_____ ftp

_____ telnet

_____ email

_____ fax

Gathering information for NetBackup-Java

If you encounter problems with the NetBackup-Java applications, use the following methods to gather data for Symantec 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 machine where the application was started. It logs in
  `install_path``\NetBackup\logs\user_ops\nbjlogs`.
  If NetBackup was not installed on this machine, 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 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`.

Follow these steps 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 completing NetBackup installation and each time after you change the NetBackup configuration.
3. Provide the support-script output and log file to Symantec support.

Chapter 2

Troubleshooting procedures

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

Note: The Symantec technical support site has a wealth of information that can help you solve NetBackup problems. See http://entsupport.symantec.com for comprehensive troubleshooting details.

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 chapter, 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 already tried.

The information in this chapter is divided into these sections:

- Preliminary troubleshooting
- Troubleshooting installation and configuration problems
- General test and troubleshooting procedures
- Troubleshooting NBU in a SAN environment

Start with “Preliminary troubleshooting,” which explains what to check first. It then branches off to other procedures as appropriate. “Troubleshooting installation and configuration problems” applies specifically to installation problems and configuration problems. “General test and troubleshooting procedures” defines 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

If you have problems with NetBackup, perform this procedure first.

1. Ensure that your servers and clients are running supported operating system versions and the peripherals you use (if any) are supported. See the NetBackup release notes and the NetBackup device compatibility lists on www.veritas.com for this information.

2. Check for status codes or messages.

   a. 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 in the following chapters: "NetBackup status codes and messages" or "Media and device management status codes and messages."

   b. 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 and either:

      - NetBackup does not provide a status code
      - You cannot correct the problem by following the instructions in "NetBackup status codes and messages" or "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.

   c. Check the applicable enabled debug logs and correct problems you detect.

      If these logs are not enabled, enable them before you retry the failed operation.

      See the "Using logs and reports" chapter.

d. If you performed corrective actions, retry the operation. If you did not perform corrective actions or the problem persists, go to step 3.

3. If you encountered the problem in the following manner, then go to "Troubleshooting installation and configuration problems" on page 24.
   - During a new installation
   - During an upgrade installation
   - After you make changes to an existing configuration
4. Ensure that the server and client are operational.

   If you experienced a server or a client disk crash, refer to the following chapter: "Disaster recovery," which contains procedures on how to recover the files that are critical to NetBackup operation.

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

   See the "Using logs and reports" chapter for information on how to log.
6. Determine which daemons or processes are running. Follow the procedures for UNIX or Windows NetBackup servers.

On UNIX NetBackup servers

Run the following:

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

a. 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.

b 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.

c 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
```

d 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

Stop the device daemon, `ltid`, by running:

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

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

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

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

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.

On Windows NetBackup servers

a 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:

Note: To start all of them, run `install_path\NetBackup\bin\bpup.exe`.

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:

- NetBackup Enterprise Media Manager service
- NetBackup Resource Broker service

On NetBackup media servers:

- NetBackup Device Manager service (if the system has configured devices)
- NetBackup Volume Manager service
- NetBackup Client service

On NetBackup clients (including NetBackup Remote Administration Consoles)

- NetBackup Client service

b 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.

7 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, go to "General test and troubleshooting procedures" on page 30.

If you cannot start any of these processes or services, check the appropriate debug logs for NetBackup problems.

See the "Using logs and reports" chapter.

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 you add commands for starting them to your startup scripts, so they restart in case you have to reboot.

Troubleshooting installation and configuration problems

This section outlines steps to resolve installation and common configuration issues.

To resolve installation problems

Note: Before you install or use NetBackup on a Linux client, verify that the `inetd` (or `xinetd`) 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 these questions

1 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 in as an administrator on a Windows system (you must have permission to install services on the system)
- Permission denied (ensure 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)

2 Can you install NetBackup client software on the clients?

Note: You cannot install PC client software from a UNIX NetBackup server.

- For an install to a trusting UNIX client, verify that 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. An example for a Sun system would be if your `.login` runs an `stty` (such as `stty ^erase`) before defining your terminal type. If this action caused the install process to hang, you could 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.

3 For general network communications problems, go to “Resolving network communication problems” on page 36.

To resolve common configuration problems

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

Note: On platforms that support the NetBackup Configuration Validation Utility (NCVU), run this utility against the NetBackup nodes in question and note any warnings that are generated.

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 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.

  “NetBackup status code: 174” in the “NetBackup status codes and messages” chapter provides further explanation.

  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.

  See the *NetBackup Administrator’s Guide, Volume I* for a list of these processes.
- 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.

a 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 in the following chapters: "NetBackup status codes and messages" or "Media and device management status codes and messages."

b 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 and either:

- NetBackup does not provide a status code
- You cannot correct the problem by following the instructions in the status codes chapters

c Check appropriate enabled debug logs and correct problems you detect.

If these logs are not enabled, enable them before your next attempt. For more information, see the "Using logs and reports" chapter.

d If you performed corrective actions as a result of step a through step c, retry the operation. If you did not perform corrective actions or the problem persists, go to the next section, "General test and troubleshooting procedures."

To resolve device configuration problems

Certain auto-configuration warning messages that appear in the second panel of the Device Configuration wizard if the selected device meets any of the following conditions:

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

These are the messages that relate to device configuration, along with 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: Too many drives in robot

Explanation: The robotic library has more than two installed drives—the maximum that is allowed with a NetBackup Server license.

Recommended Action: Remove all but two drives.

Message: Too many slots in robot

Explanation: The robotic library has more than 30 installed slots—the maximum that is allowed with a NetBackup Server license.

Recommended Action: If possible, configure the robotic library to have 30 or fewer slots. Only use the robotic libraries that are supported with NetBackup Server.

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:

1. Download a new device_mapping file from the Veritas support Web site, and try again.
2. Configure the robotic library manually.
3. 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 exceeds drive limit

Explanation: The NetBackup Server license allows a maximum of two drives and two drives have already been configured.

Recommended Action: To use this drive, a previously configured drive must be disabled (deleted from the device configuration).

Message: Robot exceeds robot limit

Explanation: A robotic library has already been configured.

Recommended Action: To use this robot, a previously configured robot must be disabled (deleted from the device configuration).

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. See the *NetBackup Device Configuration Guide* for SCSI adapter pass-through information.

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:

1. Download a new device_mapping file from the Veritas support Web site, and try again.
2. Configure the drive manually.
3. 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 attempts 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. If you need hardware data compression, refer to the chapter for your system type in the *NetBackup Device Configuration Guide*. This chapter provides information on how to configure tape drives.

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 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 information in the "Functional overview" appendix. If you have not read that appendix, do so before proceeding.

Testing the master server and clients

To test the master server and clients

1. Enable appropriate debug logs on the master server (see the "Using logs and reports" chapter). 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 `bplabel` command, NetBackup automatically assigns a previously unused media ID.

3. Verify that the NetBackup daemons or services are running on the master server:

   - 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. The "Functional overview" appendix explains the sequence of events (log messages are more detailed than the information in that appendix).
   If the debug logs do not reveal the problem, check the following:

   - Systems Logs or Event Viewer System logs

- Event Viewer Application and System logs on Windows systems
- `vmd` debug logs on the EMM database host for the device
- `bptm` debug logs

See the vendor manuals for information on hardware failures.

If you use a robot and the configuration is an initial configuration, verify that the robotic drive is configured correctly. In particular, verify that:

- 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 that are described in the "Robotic test utilities" appendix.

Note: 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. The "Using logs and reports" chapter explains which logs apply to specific client software.

Note: 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.

- `bparchive (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. The "Using logs and reports" chapter explains which logs apply to specific client types.

- `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)

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
- 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 by completing "Testing the master server and clients" on page 31.

To test the media server and clients

1 Enable appropriate legacy debug logs on the servers
See the "Using logs and reports" chapter.
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).

- 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.

- 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:

- NetBackup media server software
- NetBackup on the media server can mount the media and use the drive that you configured
- Communications between the master server processes `nbpem`, `nbjm`, `nbrb`, EMM server process `nbemm`, and media server processes `bpcd` and `bpbrm`
- Communications between media server process `bpbrm` and client processes `bpcd` and `bpbkar`

For the failures that relate to drives or media, ensure that the drive is in an UP state and 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
- `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 that:

- 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, `tpunmount` 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:

- 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 that are described in the "Robotic test utilities" appendix.

Note: 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 "Verifying host names and services entries" on page 43.

     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.

   `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:

   ```
   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 proceeding.

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

   ```
   ping ant 13782
   ```

or

```
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).

```
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)
```

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

```
    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
  ```

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

- If there is no problem with the port, you see:

```
tcp 0 0  ant.nul.nul.com.13782 whale.nul.nul.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.

Note: 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
  ```

  Note: 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 basic 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.

For more information, see “Using bpclntcmd” on page 47.

PC clients

To resolve network communication problems with PC clients

1 Before you retry the failed operation, do the following:

- Increase the logging level on the client (see the user’s guide for the client).

- 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.

  (Also see "Using the Host Properties window" on page 63.)

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

See "Verifying host names and services entries" on page 43.

3 Verify basic network connectivity between client and server by pinging from the server to the client and from the client to the server. Use the following command:

`ping` *hostname*

Where *hostname* is the name of the host as configured in:

- NetBackup policy configuration
- WINS
- DNS (if applicable).
- `hosts` file in the system directory:

  `%SystemRoot%\system32\drivers\etc\hosts` (Windows 2000, XP, 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 proceeding. 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:

a Ensure that the service is active, either by checking the logs (see step b) or as follows:

- On Windows 2000, 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.

b Check the `bpcd` debug logs for problems or errors.

See the “Using logs and reports” chapter for instructions on how to enable and use these logs.

c Verify that the same NetBackup client Service (bpcd) port number is specified on both the NetBackup client and server (by default, 13782).

- 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 2000, XP or 2003)
  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.
- Or, instead of the first bullet under step c: 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 63).

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).

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

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

- On Microsoft Windows clients (use the same method as in step c under 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 63.

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

- `%SystemRoot%\system32\drivers\etc\hosts` (Windows 2000, XP or 2003)
- `SYS:etc\hosts` (NetWare)
- `/etc/hosts` (UNIX)

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

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

9 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 attempt 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.

For more information, see "Using bpclntcmd" on page 47.

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

Verifying host names and services 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, refer to the following:

- The "Networks and hostnames" appendix in this document
- 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.

a 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.

- 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 in the NetBackup error log:

  ```
  Gethostbyname failed for
  <host_name>:<h_errno_string> (<h_errno>)
  ```

  ```
  One or more servers was excluded from the server
  list because gethostby name() failed.
  ```

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

See “Using the Host Properties window” on page 63.

b On UNIX NetBackup servers and clients and Macintosh clients, check the server and the client name entries in the `bp.conf` file:

- 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.

Remember, if you add or modify `SERVER` entries on the master server, you must stop and restart `bprd` and `bpdbm` before the changes take effect.

- Ensure that the `CLIENT_NAME` option (if included) is correct and matches what is in the policy client list on the master server.

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`.

c On NetWare clients, check the `SYS:VERITAS\NBUCLT\NetBack\BP.INI` file to 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.
- 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.

d On the master server, verify that you have created any required
`/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 has the required entries for NetBackup reserved port numbers.

Note: 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.

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

- `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`.

b 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 located in:
  `%SystemRoot%\system32\drivers\etc\services` (Windows 2000, XP or 2003)
- 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:

```
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.

7 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 allows you to 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 allows you to specify 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, you can verify that a NetBackup server can connect to a client. In this case, the steps are:

1 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.

2. 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.

For example:

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

Where:

- `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 (peername) 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.

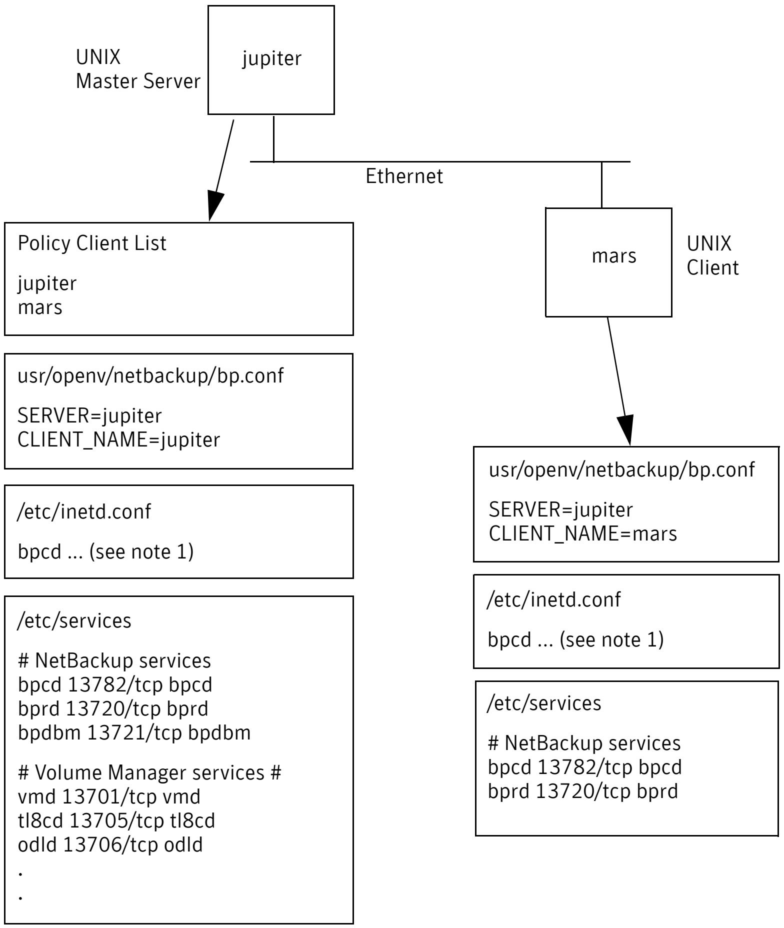
bpclntcmd -sv

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

Host name and service entry examples—UNIX

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

Figure 2-1 **Example 1: UNIX master server and client**



Policy Client List

jupiter
mars

```
usr/openv/netbackup/bp.conf

SERVER=jupiter
CLIENT_NAME=jupiter
```

```
/etc/inetd.conf

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
.
.
```

```
usr/openv/netbackup/bp.conf

SERVER=jupiter
CLIENT_NAME=mars
```

```
/etc/inetd.conf

bpcd ... (see note 1)
```

```
/etc/services

# NetBackup services
bpcd 13782/tcp bpcd
bprd 13720/tcp bprd
```

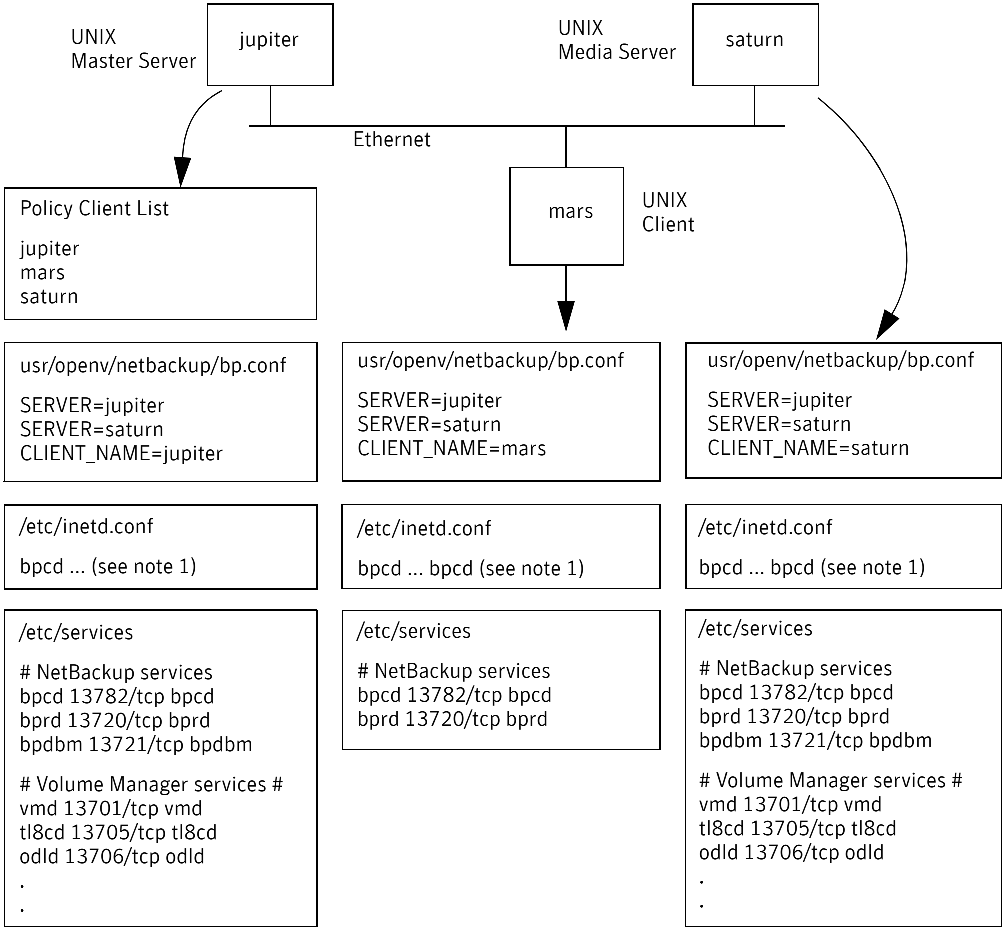
Notes:

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).

The example in Figure 2-2 includes a UNIX NetBackup media server named saturn. Note the addition of a SERVER entry for saturn in the bp.conf files on all the systems. This entry is second, beneath the one for the master server jupiter.

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



```
usr/openv/netbackup/bp.conf

SERVER=jupiter
SERVER=saturn
CLIENT_NAME=jupiter
```

```
usr/openv/netbackup/bp.conf

SERVER=jupiter
SERVER=saturn
CLIENT_NAME=mars
```

```
usr/openv/netbackup/bp.conf

SERVER=jupiter
SERVER=saturn
CLIENT_NAME=saturn
```

```
/etc/inetd.conf

bpcd ... (see note 1)
```

```
/etc/inetd.conf

bpcd ... bpcd (see note 1)
```

```
/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
.
.
```

```
/etc/services

# NetBackup services
bpcd 13782/tcp bpcd
bprd 13720/tcp bprd
```

```
/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
.
.
```

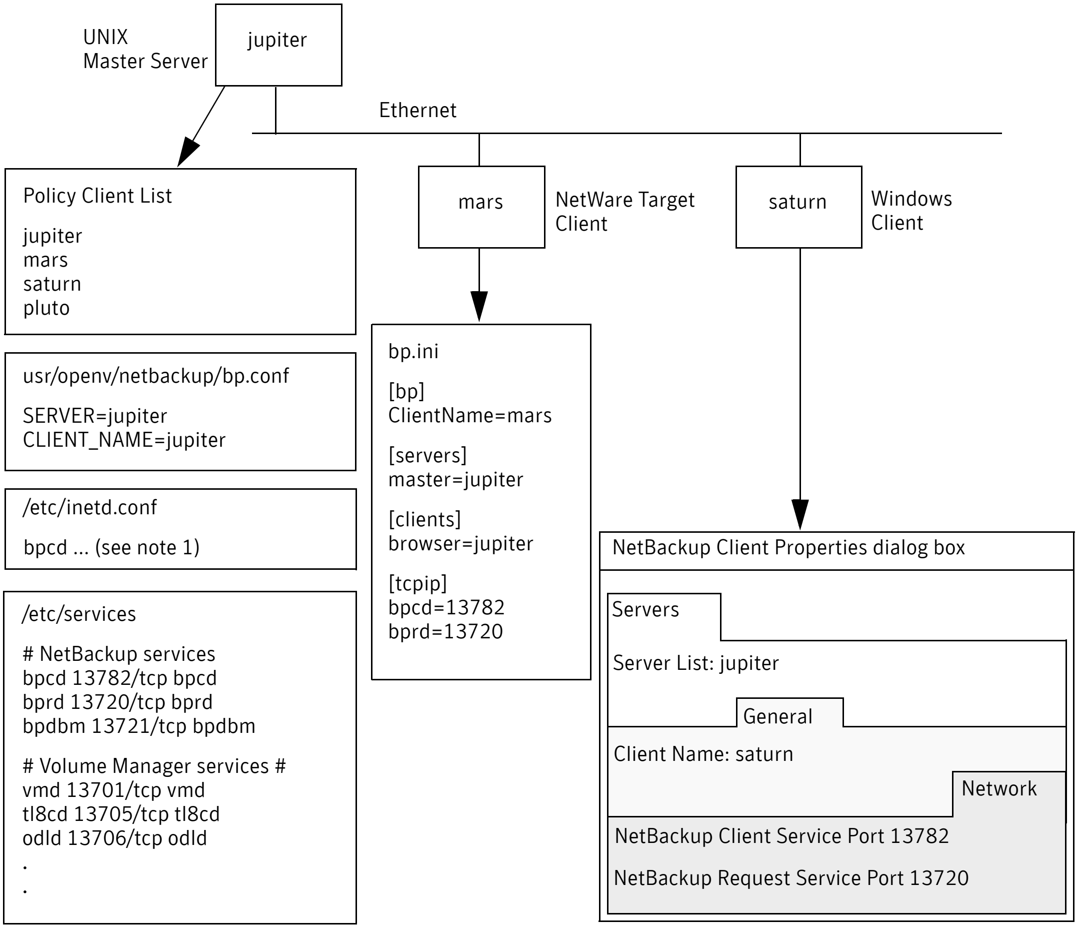
Notes:

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).

The example in 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.

Figure 2-3 **Example 3: UNIX PC clients**



```
Policy Client List

jupiter
mars
saturn
pluto
```

```
usr/openv/netbackup/bp.conf

SERVER=jupiter
CLIENT_NAME=jupiter
```

```
/etc/inetd.conf

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
.
.
```

```
bp.ini

[bp]
ClientName=mars

[servers]
master=jupiter

[clients]
browser=jupiter

[tcpip]
bpcd=13782
bprd=13720
```

NetBackup Client Properties dialog box

Servers

Server List: jupiter

General

Client Name: saturn

Network

NetBackup Client Service Port 13782

NetBackup Request Service Port 13720

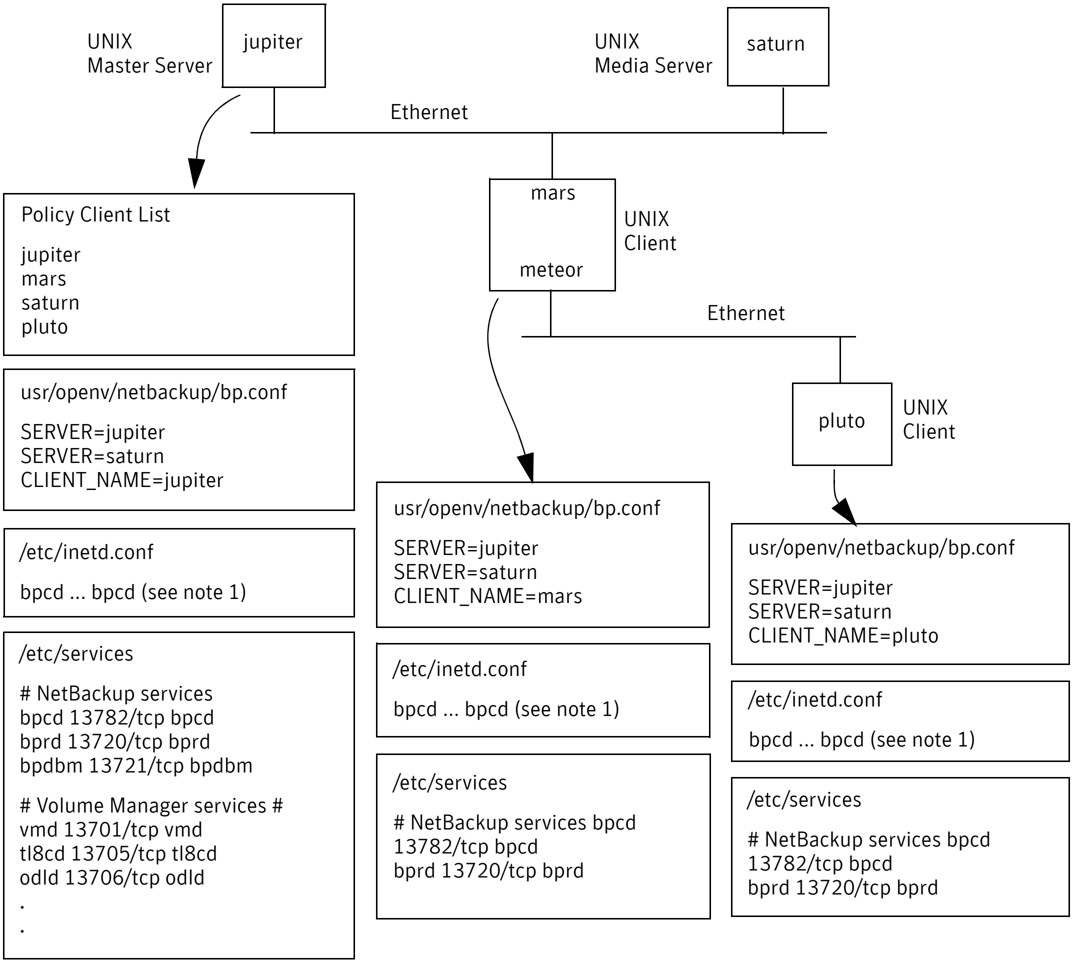
Notes:

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).

This network in the example in Figure 2-4 shows a client (mars, meteor) that is a router to clients in another network. The client's host name on the master server side is mars and the host name that is presented to the client pluto is meteor.

Figure 2-4 Example 4: UNIX clients in multiple networks



```
Policy Client List

jupiter
mars
saturn
pluto
```

```
usr/openv/netbackup/bp.conf

SERVER=jupiter
SERVER=saturn
CLIENT_NAME=jupiter
```

```
/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
.
.
```

```
usr/openv/netbackup/bp.conf

SERVER=jupiter
SERVER=saturn
CLIENT_NAME=mars
```

```
/etc/inetd.conf

bpcd ... bpcd (see note 1)
```

```
/etc/services

# NetBackup services bpcd
13782/tcp bpcd
bprd 13720/tcp bprd
```

```
usr/openv/netbackup/bp.conf

SERVER=jupiter
SERVER=saturn
CLIENT_NAME=pluto
```

```
/etc/inetd.conf

bpcd ... bpcd (see note 1)
```

```
/etc/services

# NetBackup services bpcd
13782/tcp bpcd
bprd 13720/tcp bprd
```

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).

First, we 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 peername 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
```

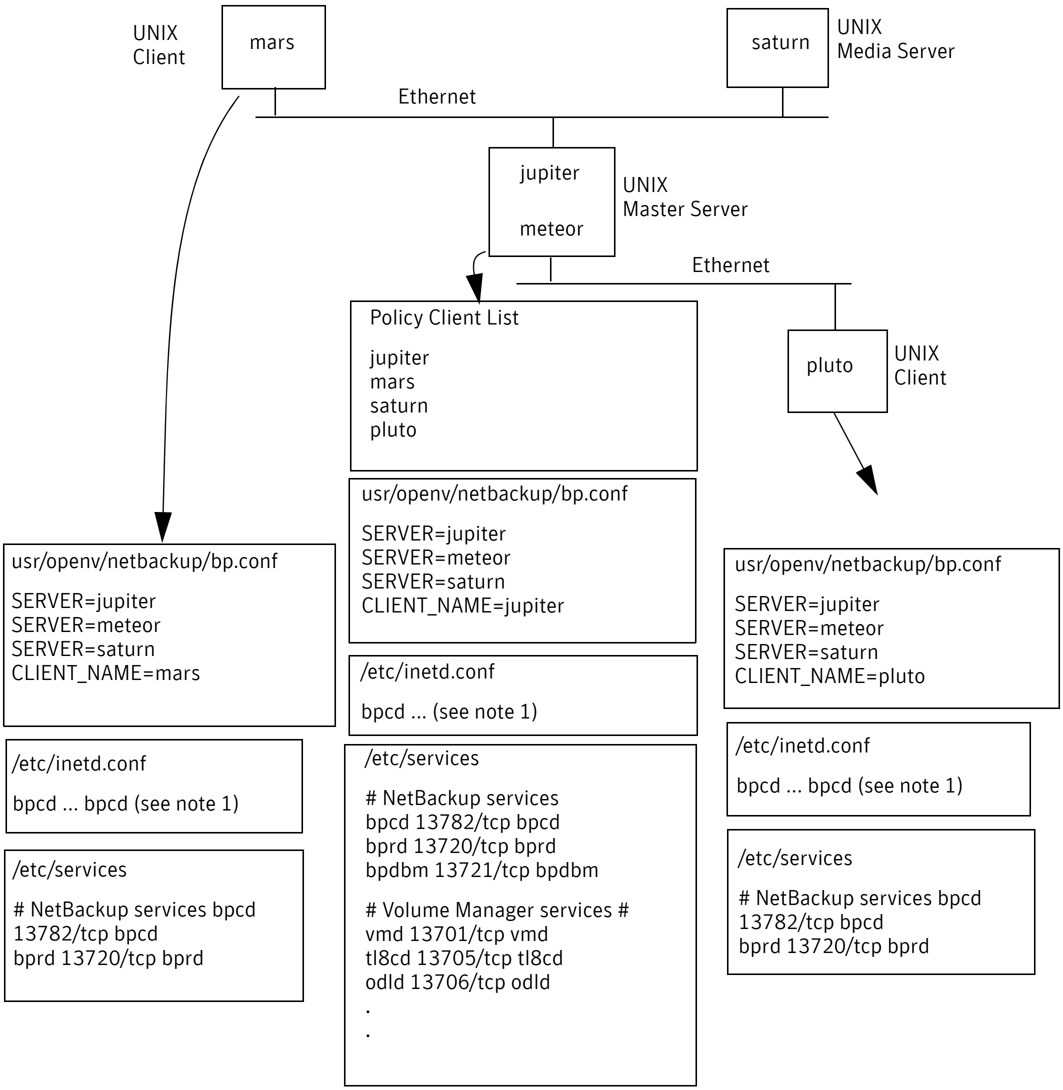
The master server now recognizes as legitimate any of the restore requests with a peername of meteor and client name of pluto.

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 peername and client name for the media server to use to establish connections.

The example in Figure 2-5 shows a NetBackup server that has two Ethernet connections and clients in both networks. The server's host name is jupiter on one and meteor on the other.

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



Policy Client List

```
jupiter
mars
saturn
pluto
```

mars:

```
usr/openv/netbackup/bp.conf

SERVER=jupiter
SERVER=meteor
SERVER=saturn
CLIENT_NAME=mars
```

```
/etc/inetd.conf

bpcd ... bpcd (see note 1)
```

```
/etc/services

# NetBackup services bpcd
13782/tcp bpcd
bprd 13720/tcp bprd
```

jupiter / meteor:

```
usr/openv/netbackup/bp.conf

SERVER=jupiter
SERVER=meteor
SERVER=saturn
CLIENT_NAME=jupiter
```

```
/etc/inetd.conf

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
.
.
```

pluto:

```
usr/openv/netbackup/bp.conf

SERVER=jupiter
SERVER=meteor
SERVER=saturn
CLIENT_NAME=pluto
```

```
/etc/inetd.conf

bpcd ... bpcd (see note 1)
```

```
/etc/services

# NetBackup services bpcd
13782/tcp bpcd
bprd 13720/tcp bprd
```

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).

Discussion for example 5: UNIX server connects to multiple networks

The first thing to note about this configuration is that 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 in order 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.

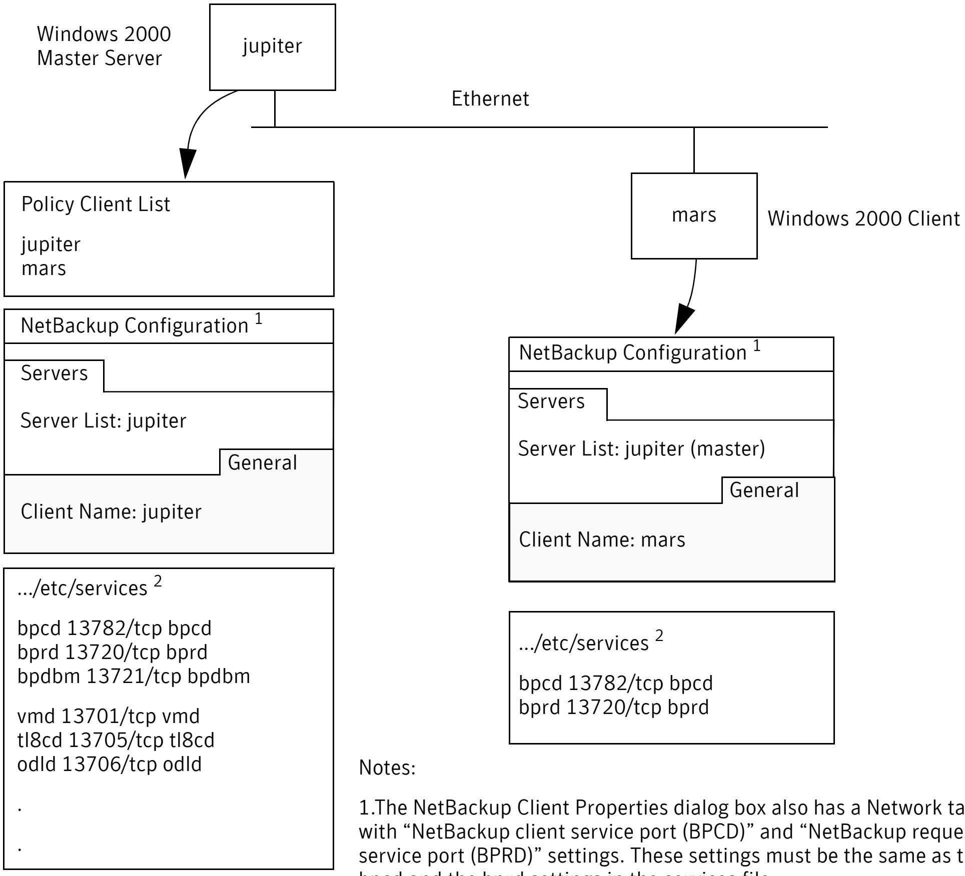
As in example 4, there would be a problem to restore the files in the following situation: the master server system is a router that hides the originating host name when routing requests between networks. For example, if pluto were on FDDI (token ring), the master server would use meteor as the peername 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 one that is discussed in "**Example 4: UNIX clients in multiple networks**" on page 52.

Host name and service entry examples—Windows 2000

Figure 2-6 shows a Windows 2000 master server with a Windows 2000 client.

Figure 2-6 Example 1: Windows 2000 master server and client



```
bpcd 13782/tcp bpcd
bprd 13720/tcp bprd
bpdbm 13721/tcp bpdbm

vmd 13701/tcp vmd
tl8cd 13705/tcp tl8cd
odld 13706/tcp odld

.

.
```

```
bpcd 13782/tcp bpcd
bprd 13720/tcp bprd
```

Notes:

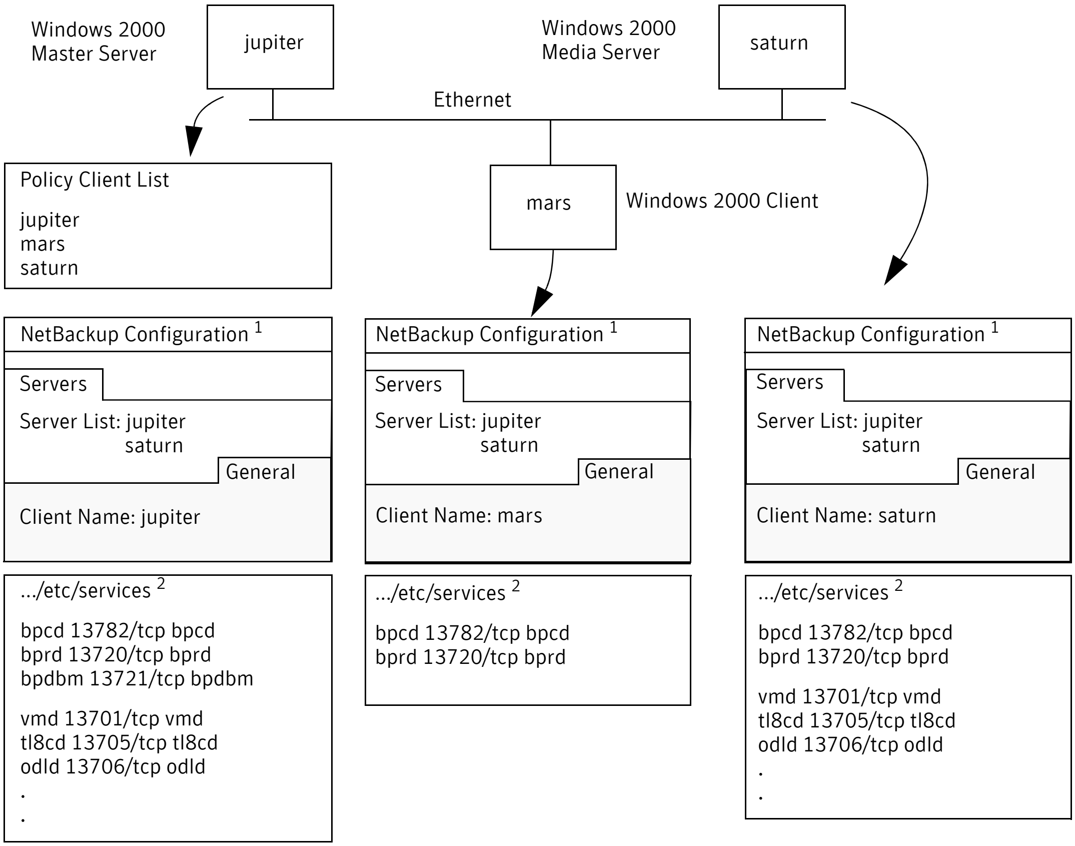
1.The NetBackup Client Properties dialog box also has a Network tab with "NetBackup client service port (BPCD)" and "NetBackup request service port (BPRD)" settings. These settings must be the same as the bpcd and the bprd settings in the services file.

2.The complete path to the Windows 2000 \etc\services file is: %SystemRoot%\system32\drivers\etc\services

3. All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this information could include the %SystemRoot%\system32\drivers\etc\hosts file and also WINS and DNS (if used).

The example in Figure 2-7 includes a NetBackup media server named saturn. Note the addition of a server list for saturn on all the systems. Jupiter is designated as the master.

Figure 2-7 **Example 2: Windows 2000 master and media servers**



```
bpcd 13782/tcp bpcd
bprd 13720/tcp bprd
bpdbm 13721/tcp bpdbm

vmd 13701/tcp vmd
tl8cd 13705/tcp tl8cd
odld 13706/tcp odld
.
.
```

```
bpcd 13782/tcp bpcd
bprd 13720/tcp bprd
```

```
bpcd 13782/tcp bpcd
bprd 13720/tcp bprd

vmd 13701/tcp vmd
tl8cd 13705/tcp tl8cd
odld 13706/tcp odld
.
.
```

Notes:

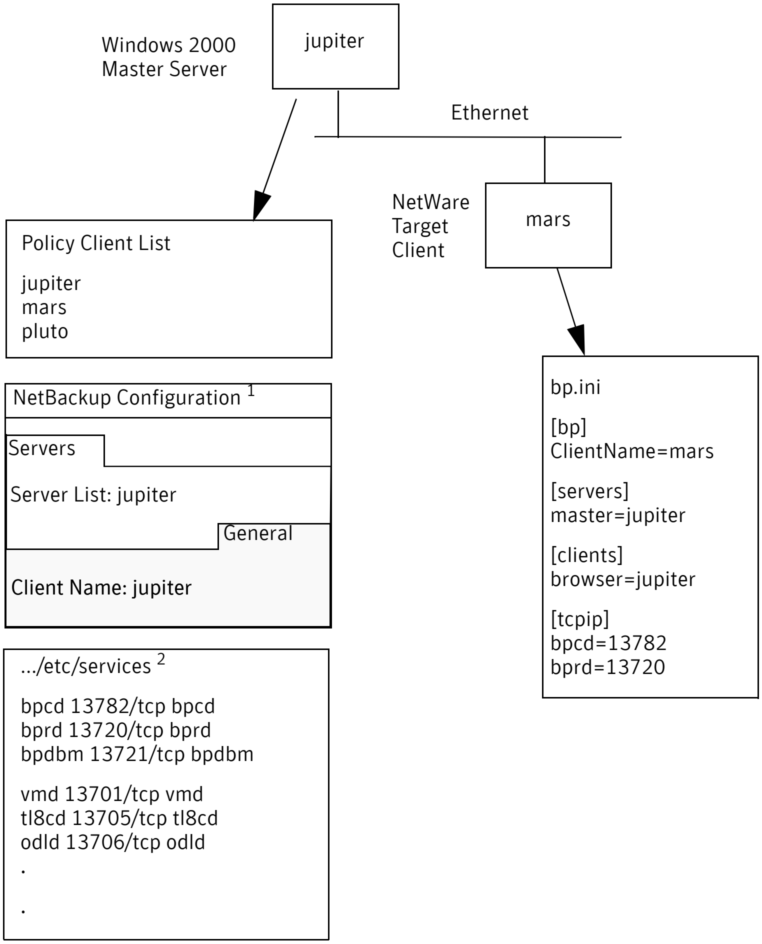
1. The NetBackup Client Properties dialog also has a Network tab with “NetBackup client service port (BPCD)” and “NetBackup request service port (BPRD)” settings. These settings must be the same as the bpcd and the bprd settings in the services file.

2. The complete path to the Windows 2000 \etc\services file is: %SystemRoot%\system32\drivers\etc\services

3. All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this information could include the %SystemRoot%\system32\drivers\etc\hosts file and also WINS and DNS (if used).

Figure 2-8 shows a master server with a NetWare client. Entries for NetWare are in the `\veritas\nbuclt\netback\bp.ini` file.

Figure 2-8 Example 3: Windows 2000 PC clients



Policy Client List

jupiter
mars
pluto

NetBackup Configuration [1]

Server List: jupiter

Client Name: jupiter

.../etc/services [2]

```
bpcd 13782/tcp bpcd
bprd 13720/tcp bprd
bpdbm 13721/tcp bpdbm

vmd 13701/tcp vmd
tl8cd 13705/tcp tl8cd
odld 13706/tcp odld
.

.
```

```
bp.ini

[bp]
ClientName=mars

[servers]
master=jupiter

[clients]
browser=jupiter

[tcpip]
bpcd=13782
bprd=13720
```

Notes:

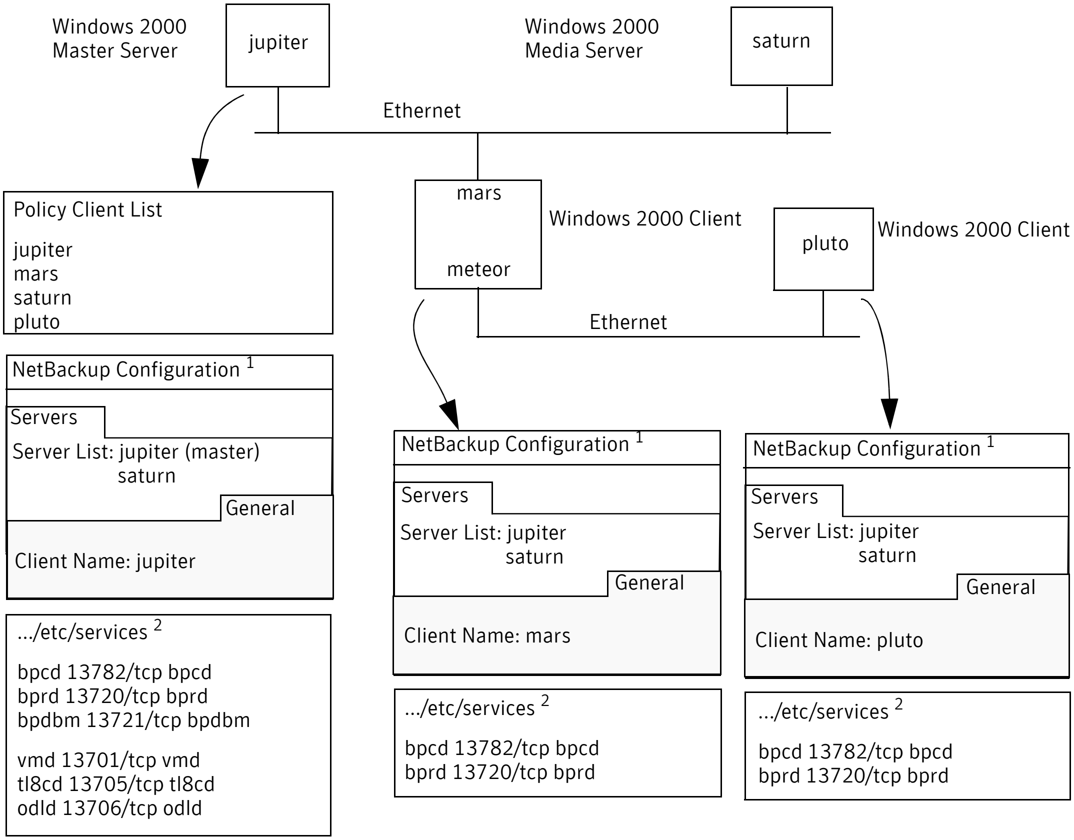
1. The NetBackup Client Properties dialog box also has a Network tab with “NetBackup client service port (BPCD)” and “NetBackup request service port (BPRD)” settings. These settings must be the same as the bpcd and the bprd settings in the services file.

2. The complete path to the Windows 2000 \etc\services file is: %SystemRoot%\system32\drivers\etc\services

3. All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this information could include the %SystemRoot%\system32\drivers\etc\hosts file and also WINS and DNS (if used).

The example in Figure 2-9 shows a client (mars, meteor) that is a router to clients in another network. The client's host name on the master server side is mars and the host name that is presented to the client pluto is meteor.

Figure 2-9 Example 4: Windows 2000 clients in multiple networks



Policy Client List

jupiter
mars
saturn
pluto

Server List: jupiter (master)
saturn

Client Name: jupiter

```
.../etc/services 2

bpcd 13782/tcp bpcd
bprd 13720/tcp bprd
bpdbm 13721/tcp bpdbm

vmd 13701/tcp vmd
tl8cd 13705/tcp tl8cd
odld 13706/tcp odld
```

Server List: jupiter
saturn

Client Name: mars

```
.../etc/services 2

bpcd 13782/tcp bpcd
bprd 13720/tcp bprd
```

Server List: jupiter
saturn

Client Name: pluto

```
.../etc/services 2

bpcd 13782/tcp bpcd
bprd 13720/tcp bprd
```

Notes:

1. The NetBackup Client Properties dialog box also has a Network tab with "NetBackup client service port (BPCD)" and "NetBackup request service port (BPRD)" settings. These settings must be the same as the bpcd and the bprd settings in the services file.

2. The complete path to the Windows 2000 \etc\services file is: %SystemRoot%\system32\drivers\etc\services

3. All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this information could include the %SystemRoot%\system32\drivers\etc\hosts file and also WINS and DNS (if used).

Discussion for example 4: Windows 2000 clients in multiple networks

First, we 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 that name 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, 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 peername 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 2000 NetBackup server, the file path is:

```
install_path\NetBackup\db\altnames\meteor
```

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

```
pluto
```

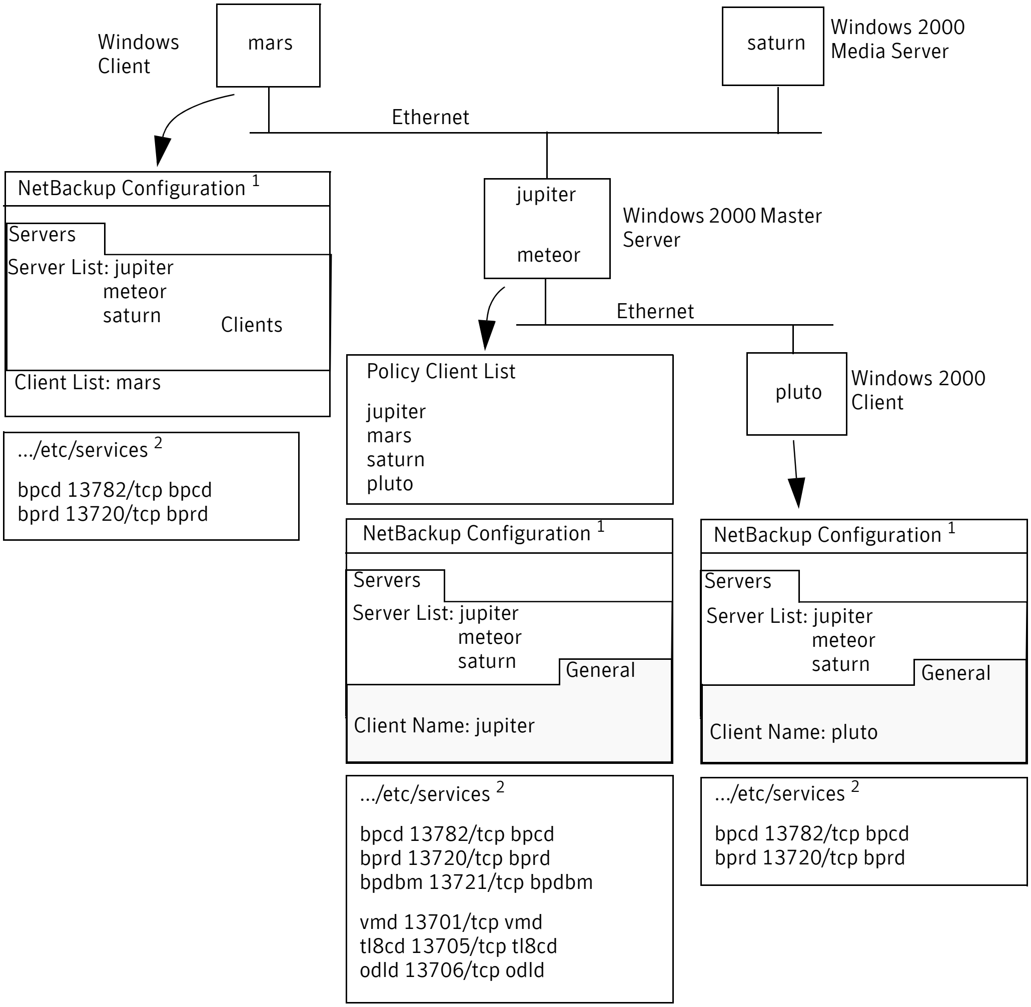
The master server now recognizes as legitimate any of the restore requests with a peername of meteor and client name of pluto.

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 still 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 peername and client name for the media server to use to establish connections.

The example in Figure 2-10 shows a NetBackup server with two Ethernet connections and clients in both networks. The server's host name is mars on one and meteor on the other.

Figure 2-10 Example 5: Windows 2000 server connects to multiple networks



mars — NetBackup Configuration [1]

Servers

Server List: jupiter
meteor
saturn

Clients

Client List: mars

mars — .../etc/services [2]

```
bpcd 13782/tcp bpcd
bprd 13720/tcp bprd
```

jupiter/meteor — Policy Client List

jupiter
mars
saturn
pluto

jupiter/meteor — NetBackup Configuration [1]

Servers

Server List: jupiter
meteor
saturn

General

Client Name: jupiter

jupiter/meteor — .../etc/services [2]

```
bpcd 13782/tcp bpcd
bprd 13720/tcp bprd
bpdbm 13721/tcp bpdbm

vmd 13701/tcp vmd
tl8cd 13705/tcp tl8cd
odld 13706/tcp odld
```

pluto — NetBackup Configuration [1]

Servers

Server List: jupiter
meteor
saturn

General

Client Name: pluto

pluto — .../etc/services [2]

```
bpcd 13782/tcp bpcd
bprd 13720/tcp bprd
```

Notes:

1. The NetBackup Client Properties dialog box also has a Network tab with “NetBackup client service port (BPCD)” and “NetBackup request service port (BPRD)” settings. These settings must be the same as the bpcd and the bprd settings in the services file.

2. The complete path to the Windows 2000 \etc\services file is: %SystemRoot%\system32\drivers\etc\services

3. All other applicable network configuration must also be updated to reflect the NetBackup information. For example, this information could include the %SystemRoot%\system32\drivers\etc\hosts file and also WINS and DNS (if used).

Discussion for example 5: Windows 2000 server connects to multiple networks

The first thing to note about this configuration is that 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 current 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 (the hosts file, WINS, 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 type that hides the originating host name when routing requests between networks. For example, if pluto were on FDDI (token ring), the master server would use meteor as the peername 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 one in “Discussion for example 4: Windows 2000 clients in multiple networks” on page 60.

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.

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.
4. On the **Actions** menu, select **Properties**.
5. In the properties dialog box, select the appropriate tab and make your change.

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.

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 the problem, check the following:

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

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

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

  See the “Using logs and reports” chapter for more information on unified logging.

To correct the situation, do the following:

1. Clear up disk space in the directory where NetBackup is installed.
   - You may need to delete log files manually, reduce logging levels, and adjust log retention to have log files automatically deleted sooner.

     Refer to the sections on logging levels, log file retention, and how to configure unified logging in the following chapter for assistance: “Using logs and reports.”
   - Consider moving the NetBackup unified logging files to a different file system. See “Changing log file locations” on page 82 for assistance.
2. 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.
3. 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.

Note: 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.

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.

PBX must be installed

NetBackup requires the Symantec Private Branch Exchange service (PBX). PBX can be installed before NetBackup or during NetBackup installation, as described in the *NetBackup Installation Guide*. If you uninstall PBX, you must re-install it.

- To see if PBX is installed, look for the following directory on the NetBackup master server:
  On UNIX: `/opt/VRTSpbx`
  On Windows: `install_path\VxPBX`
- To check the version of PBX, enter the following:
  On UNIX:
  ```
  /opt/VRTSpbx/bin/pbxcfg -v
  ```
  On Windows:
  ```
  install_path\VxPBX\bin\pbxcfg -v
  ```

PBX must be running

To see if PBX is running, do the following on the NetBackup master server:

On UNIX, check for the PBX process:

```
ps | grep pbx_exchange
```

To start PBX on UNIX, enter:

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

On Windows, make sure the “Veritas 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 these settings, do the following.

1 Display the current PBX settings:

On UNIX:

```
/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
```

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

On Windows:

```
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
```

Note: `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:

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

The unified logging originator number for PBX is 103.

For a description of unified logging, see “Unified logging” on page 82.

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 or “Configuring and using unified logging” on page 90.

- 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 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).

```
5/12/2005 16:32:17.477 [Error] V-103-11 User MINOV\Administrator
not authorized to register servers
5/12/2005 16:32:17.477 [Error] Unauthorized Server
```

To correct this problem, do the following:

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

   `UNIX:`

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

   Windows:

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

   Verity the PBX security settings by entering the following:

   ```
   pbxcfg -p
   ```

2. Stop NetBackup:

   UNIX:

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

   Windows:

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

3. Stop PBX:

   UNIX:

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

   Windows:

Go to **Start > Run**, enter `services.msc`, and stop the “Veritas Private Branch Exchange” service.

4 Start PBX:

UNIX:

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

Windows:

Go to **Start > Run**, enter `services.msc`, and start the “Veritas Private Branch Exchange” service.

5 Start NetBackup:

UNIX:

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

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
05/17/05 10:00:47.179 [Info] PBX_Client_Proxy::parse_line, line =
extension=EMM
05/17/05 10:00:47.180 [Info] hand_off looking for proxy for = EMM
05/17/05 10:00:47.180 [Error] No proxy found.
05/17/05 10:00:47.180 [Info] PBX_Client_Proxy::handle_close
```

To correct the problem, try the following.

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.

UNIX:

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

Windows:

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

New network interfaces (NIC cards)

If the NIC card 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 assistance on how to view and reset duplex mode for a particular host or device, consult the documentation that the manufacturer provides, or try the following.

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
   e9a: flags=108042<BROADCAST,RUNNING,MULTICAST,TCPCKSUM> mtu 1500
   ether 00:07:e9:3e:ca:b4 (auto-unknown-cfg_down) flowcontrol full
   e9b: flags=108042<BROADCAST,RUNNING,MULTICAST,TCPCKSUM> mtu 1500
   ether 00:07:e9:3e:ca:b5 (auto-unknown-cfg_down) flowcontrol full
   ```

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

   Note: 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

Beginning with NetBackup 6.5, 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 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 ...
```

Changes to bptm (5.x media servers only)

When a backup job fails with error code 219, the problem usually is due to the following: a misconfigured storage unit or a storage unit in which all drives are down. To make it easier to distinguish between these states, bptm logs the following messages to the NetBackup error log:

`all standalone drives of the specified density=`*`drive_density`*` are down`

This message is logged when all drives of the specified density are down. If the backup job storage unit is configured with stand-alone drives of this density, error code 219 is due to drives that are down.

`all drives are down for the specified robot number=`*`robot_num`*`, robot type=`*`robot_type`*`, and density=`*`drive_density`*

This message is logged when all the drives in the specified robot are down. If the storage unit in the backup job uses this robot, error code 219 is due to drives that are down in the robot.

`no standalone drives of the specified density=`*`drive_density`*` were found`

This message is logged when no stand-alone drive of the specified density is found. If the storage unit in the backup job uses a stand-alone drive of this density, error code 219 is due to the following: the lack of a stand-alone drive of the specified density.

`no drives were found with the specified robot number=`*`robot_num`*`, and robot type=`*`robot_type`*`, bad robot number/type`

This message is logged when no drives are found with the specified robot number or type. If you see this message in the error log and your backup job fails with error code 219, do the following: check the robot number and the robot type in the storage unit configuration. Ensure that the entries in the storage unit configuration match the robot number and robot type of an existing robot.

`no drives were found with the specified density=`*`drive_density`*

This message is logged when no drives are found that match the specified density. If your backup job fails with error code 219, check the density that is defined in the storage unit. It must match the density of the drives that are configured for the robot that is defined in the storage unit.

`no NDMP drives connected to host=`*`host_name`*` were found in robot number=`*`robot_num`*`, robot type=`*`robot_type`*`, density=`*`drive_density`*

This message is logged when no NDMP drives connected to *host_name* are found matching the specified robot number, robot type, and density. This message indicates that the following exist: the specified robot number and type and drives that match the specified density. But the combination of that robot number and type with that drive density does not exist. In other words, the robot is configured with drives of a density other than the specified density. Ensure that the storage unit is configured with the following: the correct robot number and type and the density that matches the configured drives for the robot.

```
no drives matching the requested criteria were found (robot
number=robot_num, and robot type=robot_type, and
density=drive_density)
```

This message is logged when the specified robot contains the drives that are not of the specified density. This message indicates that the following exist: the specified robot number and type and the drives that match the specified density. But the combination of that robot number and type with that drive density does not exist. In other words, the robot is configured with drives of a density other than the specified density. Ensure that the storage unit is configured with the following: the correct robot number and type and with a density that matches the configured drives for the robot.

Troubleshooting NBU in a SAN environment

Three common problems NetBackup administrators may encounter in a SAN (Storage Area Network) environment are:

- 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 allows you to 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 provides guidance to NetBackup administrators when they design, configure, or implement solutions, 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

Troubleshooting steps:

1. Check the NetBackup device monitor to see whether a device is down.
2. If it is, try to bring the drive back up.
3. 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:
   - Syslog
   - Device logs
   - NetBackup logs
4. Check the NetBackup logs for status 83, 84, 85, and 86 (these codes relate to write, read, open, position failures to access the drive)
5. Try a `robtest` to determine connectivity.
6. If there is no connectivity, the likely problem is with hardware. From the master server, select the robot or device the storage unit is associated with. Then launch CommandCentral Storage for a view of the media server and devices. Once CommandCentral Storage is launched, check 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* online 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.

Troubleshooting steps:

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.
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.

Troubleshooting steps:

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.

Chapter 3

Using logs and reports

NetBackup produces the following categories of information that you can use for troubleshooting problems.

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

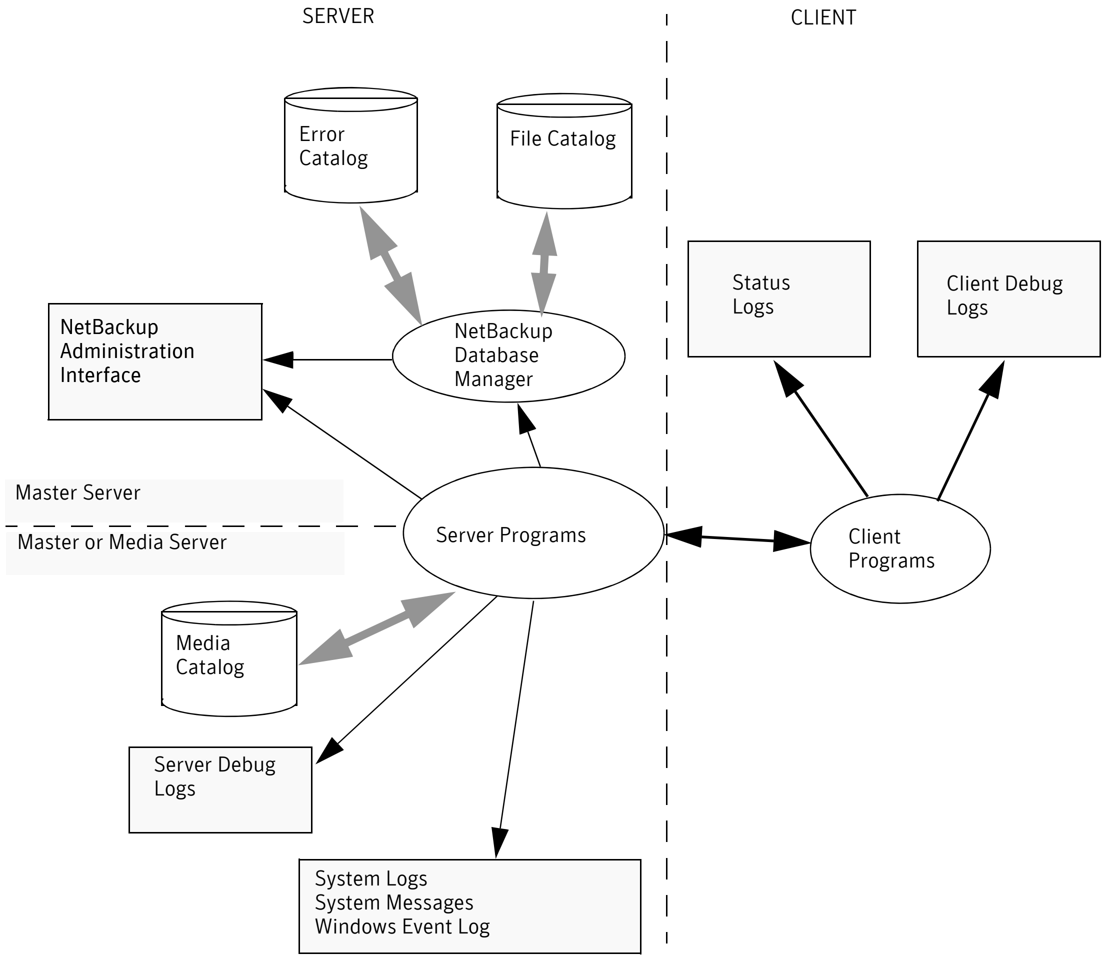
Note: The term *media server*, as distinct from *master server* or *server*, does not apply to the NetBackup Server product. When you troubleshoot a NetBackup Server installation, ignore any references to media server in this guide. (This note does not apply to NetBackup *Enterprise* Server.)

Where is this information?

Figure 3-1 shows whether log and report information is available on the client or server and the processes that make the information available. The topics in this chapter describe the reports and logs.

See Appendix A, "Functional overview" for more information on the programs and daemons that are mentioned in this figure and elsewhere in this chapter.

Figure 3-1 Log and report location



Reports

NetBackup provides standard reports that give you most of the status and the error information you need. To run these reports, use the NetBackup Administration Console. See the *NetBackup Administrator's Guide, Volume I,* for instructions and detailed descriptions on these reports.

Table 3-1 provides an outline of the reports.

Table 3-1 NetBackup reports

Report	Description
Status of Backups	Displays status 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.
Client Backups	Displays detailed information on the jobs that complete within the specified time period.
Problems	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.
All Log Entries	Lists all log entries for the specified time period. This report includes the information from the Problems report and Media Logs report.
Images on Media	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.
Media Logs	Displays the media errors or the informational messages that are recorded in the NetBackup error catalog.
Tape Reports	Displays information about the images that are stored on tape media (such as tape logs, tape contents, and tape summary).
Disk Reports	Displays information about the images that are stored on disk media (such as disk logs, and disk storage unit and disk pool status).

Status for user operations

NetBackup allows you to 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 `syslogd`. `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 also "Enabling system logs" on page 102 for more information.

Debug logs on servers

If a problem requires more information than is available through the normal logs and reports, consult the debug logs, which 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.

For a list of the processes that use unified logging, see "Unified logging: originator IDs and NetBackup processes" on page 84 and the client sections later in this chapter.

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.

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

Three kinds of messages can appear in unified logging files:

- **Application log messages:** these include informational, warning, and error messages. Application messages are always logged and cannot be disabled. These messages are localized.

  Example of application message:

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

- **Diagnostic log messages:** these 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.

  Example of diagnostic message:

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

- **Debug log messages:** These are primarily for Symantec 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.

  Example of debug message:

  ```
  10/29/04 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`

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 89.

Example log file name:

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

Where:

51216	The product ID (entity ID) for NetBackup.
116	The originator ID of the nbpem process (the NetBackup policy execution manager).
2201360136	The host ID for the host that created this log.
041029	The date in YYMMDD format.
0000000000	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 89 for more information.

Processes that use unified logging

Table 3-2 lists the NetBackup server processes that use unified logging. The processes are listed by unified logging originator ID. 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` directory on UNIX or to `*install_path*\NetBackup\logs` on Windows (except as noted in this table).

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

Originator ID	Processes that use the originator ID
103	Private Branch Exchange service (PBX). Writes logs to `/opt/VRTSpbx/log` (UNIX) and `install_path\VxPBX\log` (Windows).
111	nbemm: Enterprise Media Manager (EMM). This process runs only on the EMM server.

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

Originator ID	Processes that use the originator ID
116	nbpem: NetBackup Policy Execution Manager. This process runs only on the master server.
117	nbjm: NetBackup Job Manager. This process runs only on the master server.
118	nbrb: NetBackup Resource Broker. This process runs only on the EMM server.
119	bmrd and bmrbd: Bare Metal Restore (BMR) master (or boot) server daemons. bmrbd runs on the BMR boot server.
121	bmrsavecfg: Bare Metal Restore data collection utility. bmrsavecfg runs on the NetBackup client, not server.
122	bmrc: 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.
123	bmrs: the Bare Metal Restore commands and database interface.
124	bmrcreatefloppy.exe: (Windows only) used by Bare Metal Restore commands that create floppy disks. bmrcreatefloppy.exe runs on the BMR boot server.
125	bmrsrtadm: The Bare Metal Restore utility that creates a shared resource tree and bootable CDs, and runs on the BMR boot server.
126	bmrprep: The Bare Metal Restore utility that prepares BMR servers for a client restoration.
127	bmrsetupmaster and bmrsetupboot: Bare Metal Restore installation, configuration, and upgrade processes.
128	Bare Metal Restore libraries get their log messages from this catalog.
129	bmrconfig: The Bare Metal Restore utility that modifies a client's configuration.
130	bmrpkg and bmrcreatepkg: Bare Metal Restore utilities to add the following: Windows drivers, service packs, and hot fixes to the BMR master server so they can be used in a restore.
131	bmrrst.exe and bmrmap.exe (Windows systems only). Utilities that restore Windows Bare Metal Restore clients. They run on the restoring client.
132	nbsl: NetBackup Service Layer.

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

Originator ID	Processes that use the originator ID
134	ndmpagent: NDMP Agent daemon that manages NDMP backup and restore.
137	Controls the logging level in the NetBackup libraries. The application and diagnostic messages are for customer use; debug messages are intended for Symantec engineering.
142	bmrepadm: a utility that manages the Bare Metal Restore external procedures that are used during a restore.
143	mds: the media and device selection component of Enterprise Media Manager (EMM).
144	Device Allocator, for shared drives.
146	Operations Manager Reporting Service (NOMTRS), part of NetBackup Operations Manager (NOM).
147	The Operations Manager client (NOMClient), part of NetBackup Operations Manager (NOM).
148	The Operations Manager server (NOMCServer), part of NetBackup Operations Manager (NOM).
151	NetBackup for NDMP, avrd, and robotic processes.
154	bmrovradm: a utility that manages custom override functions for Bare Metal Restore.
156	Controls the logging level in the (ACE/TAO) CORBA components for any process that uses a CORBA interface. The default level is 0 (only very important messages are logged). This logging is intended for Symantec engineering. Note: If you are instructed to increase the logging level by Symantec support, you must increase the debug level for OID 137 to 4 or higher. Caution: A debug logging level greater than 0 generates large amounts of data.
157	nbnos: NetBackup Notification Service.
163	NetBackup Service Monitor (svcmon), which monitors the NetBackup services and attempts to restart a service that unexpectedly terminates.
166	NetBackup Vault.
178	Disk Service Manager (DSM), which performs set and get operations on disk storage and disk storage units.

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

Originator ID	Processes that use the originator ID
199	nbftsrvr: the FT Server process, part of SAN Client.
200	nbftclnt: the FT Client process, part of SAN Client.
201	FT Service Manager (FSM) component of the Enterprise Media Manager (EMM), for SAN Client.
202	The Storage Server Interface (STS) process that runs within the Remote Manager and Monitor Service. RMMS runs on media servers.
219	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.
221	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.
222	Remote Monitoring and Management Service (RMMS), which is the conduit through which EMM discovers and configures disk storage on media servers.
226	The Storage Lifecycle Manager (libssmgr), which controls lifecycle image duplication operations.
230	The Remote Disk Service Manager interface (RDSM) that runs within the Remote Manager and Monitor Service. RMMS runs on media servers.
231	Event Manager Service (nbevtmgr). nbevtmgr provides asynchronous event management services for cooperating participants.
248	BMR launcher (bmrlauncher). A utility in the Windows BMR Fast Restore image that configures the BMR environment.
263	NetBackup Administration Console for Windows (nbconsole).
272	The Expiration Manager (libexpmgr), which handles capacity management and image expiration for storage lifecycle operations.

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).

You can change the logging level in the NetBackup Administration Console with the **Global logging level** setting. Click **Host Properties**, then **Master** or **Media Servers, Properties > Logging**.

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

To set logging levels for PBX, see "PBX logging" on page 66. For logging information on media manager, see "Media and device management legacy debug logs" on page 101.

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 106.

To set the logging level for unified logging without affecting legacy logging, use the vxlogcfg command.

See "Configuring and using unified logging" on page 90.

The NetBackup Administration Console **Global logging level** field allows values of 0 to 5. The Table 3-3 lists the kind of detail each level includes.

Table 3-3 Global logging levels

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

Please note the following:

- In the **Global logging level** field of the Administration Console, a 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 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 90.

- 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.
- It 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 several options as set by the 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 `vxlogcfg` command with the RolloverMode option. See “vxlogcfg command” on page 92 and following for examples.

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

Note: Logs for the processes that are listed in Table 3-2 on page 84 can use rotation. Certain legacy logs also can use rotation: see “Legacy logging file rotation (robust logging)” on page 103.

Log file recycling (removing older log files)

There are two ways of automatically deleting log files.

- Unified logging files can be automatically deleted when the number of log files exceeds a certain number. That number is defined by the NumberOfLogFiles option on the vxlogcfg command. See "vxlogcfg command" on page 92 for an example.
- Both unified and legacy logs can be deleted by the **Keep logs For** setting, 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 files are not manually deleted or moved using `vxlogmgr`, the **Keep logs For** setting removes the old logs, both for unified and legacy logging.

Note: If the LogRecycle option (on the vxlogcfg command) 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 specified by NumberOfLogFiles on the vxlogcfg command.

Configuring and using unified logging

This section describes commands for controlling unified logging, with examples.

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

vxlogview command

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

Note: 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.

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 -i option shows the messages that the named originator process logs, such as nbpem. It also shows messages that are logged by the library that the originator uses. The -o option shows only the messages that the originator process logs.

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/51216-118-1342895976-050503-0000000000.log
/usr/openv/logs/51216-118-1342895976-050504-0000000000.log
/usr/openv/logs/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/51216-118-1342895976-050504-0000000000.log
/usr/openv/logs/51216-118-1342895976-050503-0000000000.log
Total 2 file(s)
Are you sure you want to delete the file(s)? (Y/N):
Y
Deleting
/usr/openv/logs/51216-118-1342895976-050504-0000000000.log ...
Deleting
/usr/openv/logs/51216-118-1342895976-050503-0000000000.log ...
```

Example 2

Delete the unified log files that were created by NetBackup 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:

- `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 103.
- 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 nbpem (originator ID 116) to periodic and sets the interval until the next nbpem 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 also "Controlling the number of log files with vxlogmgr" on page 94.

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. The following sections provide additional examples.

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, NumberOfLogFiles, 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
NumberOfLogFiles = 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 *`NumberOfLogFiles`* option to manually delete log files.

For example, you currently have 10 unified logging files and the `vxlogcfg` command's *`NumberOfLogFiles`* 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:

```
NumberOfFiles for originator * 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:

```
Number of NetBackup originators * default MaxLogFileSizeKB * default NumberOfFiles
```

To see the current unified logging settings, use the `vxlogcfg` command as shown under “Listing unified logging settings” on page 94.

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:

```
Number of NetBackup originators * default MaxLogFileSizeKB * default NumberOfFiles.
```

Which is 10 * 5120 * 3 KB, or 15360 kilobytes of disk space at the end of each hour.

Submitting unified logging files to Symantec support

The following is an example of the steps for gathering unified logs for NetBackup:

1 Create a directory:

```
mkdir /upload
```

2 Enter one of the following:

To copy all unified logs (including those for PBX) to the /upload directory:

```
vxlogmgr -c --dir /upload
```

To copy unified logs (for NetBackup only) to the /upload directory:

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

Example output:

```
Following are the files that were found:
/usr/openv/logs/51216-157-2202872032-050125-0000000000.log
/usr/openv/logs/51216-111-2202872032-050125-0000000000.log
/usr/openv/logs/51216-118-2202872032-050125-0000000000.log
/usr/openv/logs/51216-117-2202872032-050125-0000000000.log
/usr/openv/logs/51216-116-2202872032-050125-0000000000.log
/usr/openv/logs/51216-132-2202872032-050125-0000000000.log
Total 6 file(s)
Copying
/usr/openv/logs/51216-157-2202872032-050125-0000000000.log ...
Copying
/usr/openv/logs/51216-111-2202872032-050125-0000000000.log ...
Copying
/usr/openv/logs/51216-118-2202872032-050125-0000000000.log ...
Copying
/usr/openv/logs/51216-117-2202872032-050125-0000000000.log ...
Copying
/usr/openv/logs/51216-116-2202872032-050125-0000000000.log ...
Copying
/usr/openv/logs/51216-132-2202872032-050125-0000000000.log ...
```

3 Change to the /upload directory and list its contents:

```
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:

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

Legacy NetBackup logging

Certain NetBackup processes use unified logging as described in “Unified logging” on page 82.

All other NetBackup processes use legacy logging.

Enabling legacy logging

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

UNIX:

```
/usr/openv/netbackup/logs
/usr/openv/volmgr/debug
```

Windows:

```
install_path\NetBackup\logs
install_path\Volmgr\debug
```

For the Status Collector Daemon, see "Enabling the status collector daemon" on page 103.

The "NetBackup legacy logs (not media and device management)" and "Media and device management legacy debug logs" tables list the log directories that you must create.

IMPORTANT: 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 NetBackup legacy logs (not media and device management)

Debug log directory to create	Create directory under	Associated process
admin	/usr/openv/netbackup/logs (UNIX) *install_path*\NetBackup\logs (Windows)	Administrative commands.
bpbrm	/usr/openv/netbackup/logs (UNIX) *install_path*\NetBackup\logs (Windows)	Net backup and restore manager.

Table 3-4 NetBackup legacy logs (not media and device management)

Debug log directory to create	Create directory under	Associated process
bpcd	/usr/openv/netbackup/logs (UNIX) *install_path*\NetBackup\logs (Windows)	NetBackup client daemon or manager. The NetBackup Client service starts this process
bpdbjobs	/usr/openv/netbackup/logs (UNIX) *install_path*\NetBackup\logs (Windows)	NetBackup jobs database manager program.
bpdm	/usr/openv/netbackup/logs (UNIX) *install_path*\NetBackup\logs (Windows)	NetBackup disk manager.
bpdbm	/usr/openv/netbackup/logs (UNIX) *install_path*\NetBackup\logs (Windows)	NetBackup database manager. This process runs only on master servers. On Windows systems, it is the NetBackup Database Manager service.
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 login through the Login 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. (On all Windows platforms.)

Table 3-4 NetBackup legacy logs (not media and device management)

Debug log directory to create	Create directory under	Associated process
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 or optical media 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)

Debug log directory to create	Create directory under	Associated process
user_ops	/usr/openv/netbackup/logs (UNIX) *install_path*\NetBackup\logs (Windows)	The `user_ops` directory is created during the install of NetBackup on all servers and clients. NetBackup Java interface programs use it for the following: temporary files and for job and progress log files that the 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 execute permissions. `user_ops` contains a directory for every user that uses the Java programs. In addition, on NetBackup-Java capable platforms, the NetBackup Java interface log files are written in the `nbjlogs` subdirectory. All files in the `user_ops` directory hierarchy are removed according to the setting of the KEEP_LOGS_DAYS configuration option.
vnetd	/usr/openv/netbackup/logs (UNIX) *install_path*\NetBackup\logs (Windows)	The Veritas network daemon, used to create "firewall friendly" socket connections. Started by the inetd(1M) process. **Note:** Before the 6.0 release, on UNIX, the vnetd log directory was located in `/usr/openv/logs` rather than `/usr/openv/netbackup/logs`. For 6.0 and later, logging occurs in either location if the vnetd directory exists there. If the vnetd directory exists in both locations, logging occurs only in `/usr/openv/netbackup/logs/vnetd`.

See the "Functional overview" appendix for more information on the programs and daemons that write the logs.

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 and device management processes. Note the following.

- NetBackup creates one log per day in each of the debug directories.
- See “Standard file name format for legacy logs, without log file rotation:” on page 105 for the format of the log file names.
- On UNIX: to disable vmd debug logging, either delete the /usr/openv/volmgr/debug/daemon directory or rename it.
- 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 Media and device management legacy debug logs

Debug log directory to create	Create directory under	Associated process
acsssi	/usr/openv/volmgr/debug (UNIX)	Debug information on transactions between NetBackup and the Storage Tek ACSLS server.
daemon	/usr/openv/volmgr/debug (UNIX) *install_path*\Volmgr\debug (Windows)	Debug information for vmd (NetBackup Volume Manager service, Windows) and its associated processes (oprd and rdevmi). Stop and restart vmd after creating the directory.
ltid	/usr/openv/volmgr/debug (UNIX) *install_path*\Volmgr\debug (Windows)	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.

Table 3-5 Media and device management legacy debug logs

Debug log directory to create	Create directory under	Associated process
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. vmscd maintains a persistent connection with NetBackup 5.x servers and monitors the status of drives that are attached to NetBackup 5.x servers. 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. This command can be:

- 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`).

Note: 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. On Compaq Tru64 the `uerf` command 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 starting nbemm. As an alternative, you can stop and restart nbemm after creating this directory.

UNIX

```
/usr/openv/volmgr/debug/reqlib
```

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.

For instructions 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)."

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 104 instead.

This feature involves file rotation, as used in unified logging ("Unified logging file rollover" on page 89). 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.

Legacy logs using rotation

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

Note: 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

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 logging directory is 3.

Note: If **Enable robust logging** is disabled, the standard log-file behavior remains in effect: one log file is created per logging 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 the maximum number of log files per logging directory to 10. It sets the default values for the following: all unified logging processes and for the legacy processes listed in "Legacy logs using rotation" on page 104, for NetBackup (product ID 51216).

See "Configuring and using unified logging" on page 90 for more examples of the `vxlogcfg` command. You also can refer to the `vxlogcfg` man page or to the *NetBackup Commands* manual.

Legacy logging file name format

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

Standard file name format for legacy logs, without log file rotation:

In the standard, legacy logging system, a NetBackup process creates one debug log file per day. The log file name is of this format:

On UNIX:

log.*mmddyy*

For example:

`log.040805`

On Windows:

mmddyy.log

For example:

`040105.log`

File name format for legacy logs 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.

Notes on legacy file-naming formats:

- 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 the note under "Legacy logs using rotation" on page 104.

How to set legacy logging levels

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

Legacy logging (not including media and device management)

The following settings affect legacy logging, except media and device management. (See "Media and device management legacy logging" on page 107.)

- 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.
  For synthetic backup, see "Logs to accompany problem reports for synthetic backup" on page 107.
- 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 logging detail, enter `VERBOSE = 2` or a higher value. This setting affects legacy logging only.

Caution: High verbose values can cause debug logs to become very large.

- Also note: You can use the Logging dialog box to set the logging level for individual processes. (Click Host Properties > Master Server Properties > Logging tab > Logging dialog box.)
  See the *NetBackup Administrator's Guide, Volume I*.
  Or, specify the verbose flag (if available) when you start the program or daemon.

Media and device management legacy logging

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 directions on how to gather unified logging files relevant to the problem, see "Submitting unified logging files to Symantec support" on page 95.
- 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.
  - Create these directories:
    On the master server:
    `<install_path>/netbackup/logs/bpsynth`
    `<install_path>/netbackup/logs/bpdbm`
    `<install_path>/netbackup/logs/vnetd`
    On the media server:
    `<install_path>/netbackup/logs/bpcd`
    `<install_path>/netbackup/logs/bptm`
    `<install_path>/netbackup/logs/bpdm`

- Set the logging level:
  Use the **Global logging level** option on the **Logging** tab in the Master Server Properties dialog box.
  To display this dialog box, see "Using the Host Properties window" on page 63.
- 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.

  Note: 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/bppllistpolicy_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.

Refer to “Unified logging” on page 82 for a discussion of unified logging file name format and other details. Unified logging is enabled by default.

Legacy logging on UNIX clients

To enable legacy debug logging on UNIX clients, create the appropriate directories under:

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

The following table lists the legacy debug log directories that apply to UNIX clients.

See “Legacy NetBackup logging” on page 96 for additional information on legacy logging.

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

Table 3-6 UNIX client debug logs: Legacy logging

Debug log directory	Associated process
`bp`	Menu driven client-user interface program.
`bparchive`	Archive program. Also useful for debugging `bp`.
`bpbackup`	Backup program. Also useful for debugging `bp`.
`bpbkar`	Program that is used to generate backup images.
`bpcd`	NetBackup client daemon or manager.
`bphdb`	Program that starts a script to back up a database on a NetBackup database agent client. See the system administrator's guide for the appropriate NetBackup database agent for more information.
`bpjava-msvc`	The NetBackup-Java application server authentication service that `inetd` starts during startup of the NetBackup Java interface applications. This program authenticates the user that started the application.

Table 3-6 UNIX client debug logs: Legacy logging (continued)

Debug log directory	Associated process
bpjava-usvc	The NetBackup program that bpjava-msvc 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 host where bpjava-msvc is running.
bplist	Program that lists backed up and archived files. Also useful for debugging bp.
bpmount	Program that determines local mount points and wildcard expansion for Multiple Data Streams.
bporaexp	Command-line program on clients to export Oracle data in XML format. Communicates with bprd on server.
bporaexp64	64-bit command-line program on clients to export Oracle data in XML format. Communicates with bprd on server.
bporaimp	Command-line program on clients to import Oracle data in XML format. Communicates with bprd on server.
bporaimp64	64-bit command-line program on clients to import Oracle data in XML format. Communicates with bprd on server.
bprestore	Restore program. Also useful for debugging bp.
db_log	For more information on these logs, see the NetBackup guide for the database-extension product that you use.
mtfrd	These logs have information about the mtfrd process, which is used for phase 2 imports and restores of Backup Exec media.
tar	tar process during restores.
user_ops	The user_ops directory is created during the install of NetBackup on all servers and clients. The NetBackup Java interface programs use it for the following: temporary files and for job and progress log files that the 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.

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 89.

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 103.

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

For a description of logging file name format, refer to the following: "Unified logging file name format" on page 83 and "Legacy logging file name format" on page 105.

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.

Refer to "Unified logging" on page 82 for a discussion of file name format and other unified logging details.

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\`
- NetWare clients - `SYS:VERITAS\NBUCLT\NetBack\logs\`

The following table lists the legacy debug log directories that apply to these clients:

Table 3-7 PC client debug logs: Legacy logging

Debug log directory	NetBackup client	Associated process
bp	NetWare target	Client-user interface program for NetWare.
bpinetd	Windows 2000/2003	Client service logs. These logs have information on the bpinetd32 process.
bparchive	Windows 2000/2003	Archive program that is run from the command line.
bpbackup	Windows 2000/2003	The backup program that is run from the command line.
bpbkar	Windows 2000/2003	Backup and archive manager. These logs have information on the bpbkar32 process.
bpcd	All Windows and NetWare clients	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.

Table 3-7 PC client debug logs: Legacy logging (continued)

Debug log directory	NetBackup client	Associated process
bpjava-msvc	The NetBackup-Java application server authentication service that the Client Services service starts during startup of the NetBackup Java interface applications. This program authenticates the user that started the application. (On all Windows platforms.)	bpjava-msvc
bpjava-usvc	NetBackup program that bpjava-msvc 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 bpjava-msvc is running.(On all Windows platforms.)	bpjava-usvc
bplist	Windows 2000/2003	List program that is run from the command line.
bpmount	Windows 2000/2003	The program that is used to collect drive names on the client for multistreaming clients.
bprestore	Windows 2000/2003	The restore program that is run from the command line.
bpsrv	NetWare nontarget	NetBackup service utility. This program allows the system with the user interface to communicate with the NetBackup for NetWare client.
nbwin	Windows 2000/2003	Client-user interface program for Windows 2000.
tar	Windows 2000/2003	tar process. These logs have information about the tar32 process.

Table 3-7 PC client debug logs: Legacy logging (continued)

Debug log directory	NetBackup client	Associated process
user_ops	Windows 2000/2003	The user_ops directory is created during the install of NetBackup on all servers and clients. The NetBackup Java interface programs use it for the following: temporary files and for job and progress log files that the 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.

Controlling log size on PC clients

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

See “Unified logging file rollover” on page 89.

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 103.

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

For a description of logging file name format, refer to the following: "Unified logging file name format" on page 83 and "Legacy logging file name format" on page 105.

How to set logging levels on PC clients

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

- On Windows clients, set the debug level with the **Verbose** field on the **TroubleShooting** tab of the NetBackup Client Properties dialog box. On the Backup, Archive, and Restore interface, click **File > NetBackup Client Properties**.
- 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 90.
- 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.

Note: 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

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
   ```

   The next topic explains the format of the entry. If you do not add an entry, a default value is used, which is also explained in the next topic.

eventlog file entries

The `eventlog` entry has 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 as documented in the "NetBackup status codes and messages" and "Media and device management status codes and messages" chapters.

  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 "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 at the end of the "NetBackup status codes and messages"chapter. 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 as documented in the "NetBackup status codes and messages"chapter.

  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
  ```

  or

  ```
  vrts.nbu.NBUCommandExecutionException
  ```

  Java exceptions usually appear in one of 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 (see "Enabling detailed debug logging" for more detail)
- 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).

   Refer to “Debug logs on servers” in this chapter for more information.

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.

3. 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
   ```

4. 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 3-8 Data types

Field name	Type	Description	Example
PRODID or prodid	Integer or string	Provide the product ID or the abbreviated name of product.	PRODID = 100 or PRODID = 'NBU'
ORGID or orgid	Integer or string	Provide the originator ID or the abbreviated name of the component.	ORGID = 1 or ORGID = 'VxAM'
PID or pid	Long Integer	Provide the process ID	PID = 1234567
TID or tid	Long Integer	Provide the thread ID	TID = 2874950
STDATE or stdate	Long Integer or string	Provide the start date in seconds or in the locale specific short date and time format. For example, a locale may have format 'mm/dd/yy hh:mm:ss AM/PM'	STDATE = 98736352 or STDATE = '4/26/04 11:01:00 AM'
ENDATE or stdate	Long Integer or string	Provide the end date in seconds or in the locale specific short date and time format. For example, a locale may have format 'mm/dd/yy hh:mm:ss AM/PM'	ENDATE = 99736352 or ENDATE = '04/27/04 10:01:00 AM'
PREVTIME or prevtime	String	Provide the hours in 'hh:mm:ss' format. This field should be used only with operators =, <, >, >= and <=	PREVTIME = '2:34:00'
SEV or sev	Integer	Provide the severity type. The severities to use are as follows: ■ INFO or info ■ WARNING or warning ■ ERR or err ■ CRIT or crit ■ EMERG or emerg	SEV = 0 or SEV = INFO

Table 3-8 Data types

Field name	Type	Description	Example
MSGTYPE or msgtype	Integer	Provide the message type. The message types to use are as follows: ■ DEBUG or debug - debug messages ■ DIAG or diag - diagnostic messages ■ APP or app - application messages ■ CTX or ctx - context messages. ■ AUDIT or audit - audit messages	MSGTYPE = 1 or MSGTYPE = DIAG
CTX or ctx	Integer or string	Provide the context token as string identifier or 'ALL' to get all the context instances to be displayed. This field should be used only with the operators = and !=.	CTX = 78 or CTX = 'ALL'

String constants

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

Syntax for providing start and end date

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

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

2. ((prodid = 'NBU') && ((stdate >= ‘11/18/03 0:0:0 AM’) && (endate
<= ‘12/13/03 13:0:0 AM’))) || ((prodid = 'BENT') && ((stdate >=
‘12/12/03 0:0:0 AM’) && (endate <= ‘12/25/03 25:0:0 PM’)))

3. (STDATE <= ‘04/05/03 0:0:0 AM’) - This query will retrieve log
messages, which are logged on or before 2003-05-04 for all the
installed Veritas products.
```

Chapter 4

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. Two kinds of logging are used: legacy logging and unified logging, described in the "Using logs and reports" chapter. 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 log(s). 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`
- `backupdbtrace` consolidates the debug log messages for specified NetBackup offline (cold) catalog backup jobs and writes them to standard output.
- `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
```

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, nbpem, nbjm, nbrb, bpdbm, bpbrm, bptm, bpdm, 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, see the *NetBackup Commands* manual, or use the command with the -help option.

backuptrace

The backuptrace utility can be used for regular file system, database extension, and alternate backup method backup jobs. It consolidates the debug logs for specified NetBackup jobs. The utility writes the relevant debug log messages to standard output and sorts the messages by time. backuptrace attempts to compensate for time zone changes and clock drift between remote servers and clients. The format of the output makes it relatively easy to sort or grep by time stamp, program name, and server or client name.

The backuptrace utility works with the nbpem, nbjm, and nbrb logs on the master server. You should enable debug logging for bpbrm and bptm or bpdm on the media server and for bpbkar on the client. For best results, set the verbose logging level to 5. Enable debug logging for the following: bpdbm and bprd on the master server and for bpcd on all servers and clients in addition to the processes already identified.

This command requires administrative privileges.

restoretrace

restoretrace consolidates the debug logs for specified NetBackup restore jobs. The utility writes debug log messages relevant to the specified jobs to standard output and sorts the messages by time. restoretrace attempts to compensate for time zone changes and clock drift between remote servers and clients. The format of the output makes it relatively easy to sort or grep by time stamp, program name, and server or client name.

At a minimum, you must enable debug logging for bprd on the master server. Enable debug logging for bpbrm and bptm or bpdm on the media server and tar on the client. For best results, set the verbose logging level to 5. Enable debug logging for bpdbm on the master server and for bpcd on all servers and clients.

This command requires administrative privileges.

bpgetdebuglog

bpgetdebuglog is a helper program for backuptrace and restoretrace. It can also be useful as a stand-alone program and is available for all NetBackup server platforms. bpgetdebuglog prints to standard output the contents of a specified debug log file. If only the remote machine parameter is specified, bpgetdebuglog prints the following to standard output: the number of seconds of clock drift between the local machine and the remote machine.

This command requires administrative privileges.

backupdbtrace

backupdbtrace consolidates the debug log messages for specified NetBackup database backup jobs and writes them to standard output. It sorts the messages by time. backupdbtrace attempts to compensate for time zone changes and clock drift between remote servers and clients.

At a minimum, you must enable debug logging for admin on the master server, and for bptm and bpbkar on the media server. For best results, set the verbose logging level to 5 and enable debug logging for the following: bpdbm on the master server and bpcd on all servers in addition to the processes already identified.

This command requires administrative privileges.

duplicatetrace

duplicatetrace consolidates the debug logs for the specified NetBackup duplicate jobs and writes them to standard output. It sorts the messages by time. duplicatetrace attempts to compensate for time zone changes and clock drift between remote servers and clients.

At a minimum, you must enable debug logging for admin on the master server and for bptm or bpdm on the media server. For best results, set the verbose logging level to 5 and enable debug logging for the following: bpdbm on the master server and bpcd on all servers and clients in addition to the processes already identified.

This command requires administrative privileges.

importtrace

importtrace consolidates the debug log messages for the specified NetBackup import jobs and writes them to standard output. It sorts the messages by time. importtrace attempts to compensate for time zone changes and clock drift between remote servers and clients.

At a minimum, you must enable debug logging for admin on the master server, and for bpbrm, bptm and tar on the media server. For best results, set the verbose logging level to 5 and enable debug logging for the following: bpdbm on the master server and bpcd on all servers and clients in addition to the processes already identified.

This command requires administrative privileges.

verifytrace

verifytrace consolidates the debug log messages for the specified verify job[s] and writes them to standard output. It sorts the messages by time. verifytrac*e* attempts to compensate for time zone changes and clock drift between remote servers and clients.

At a minimum, you must enable debug logging as follows: for admin on the master server and for bpbrm, bptm (or bpdm) and tar on the media server. For best results, set the verbose logging level to 5 and enable debug logging for the following: bpdbm on the master server and bpcd on all servers and clients in addition to the processes already identified.

This command requires administrative privileges.

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:

UNIX

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

Windows

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

For a description of the nbsu command options, refer to the nbsu man page or to the *NetBackup Commands Guide*.

When to use nbsu

Symantec 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 Symantec 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\

    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:

UNIX

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

Windows

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

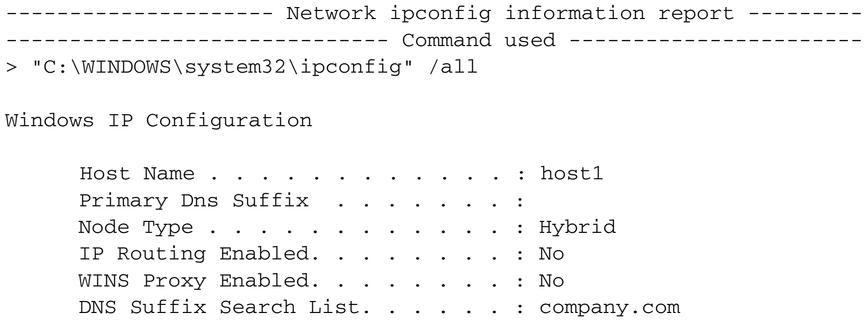
The NetBackup environment where nbsu runs determines the particular files that nbsu creates. nbsu runs only those diagnostic commands that are appropriate to the operating system and the NetBackup version and configuration. For each diagnostic command that it runs, nbsu writes the command output to a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

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."

The actual command(s) and output follow the header.

Figure 4-1 Example nbsu output file: ipconfig command (excerpt)

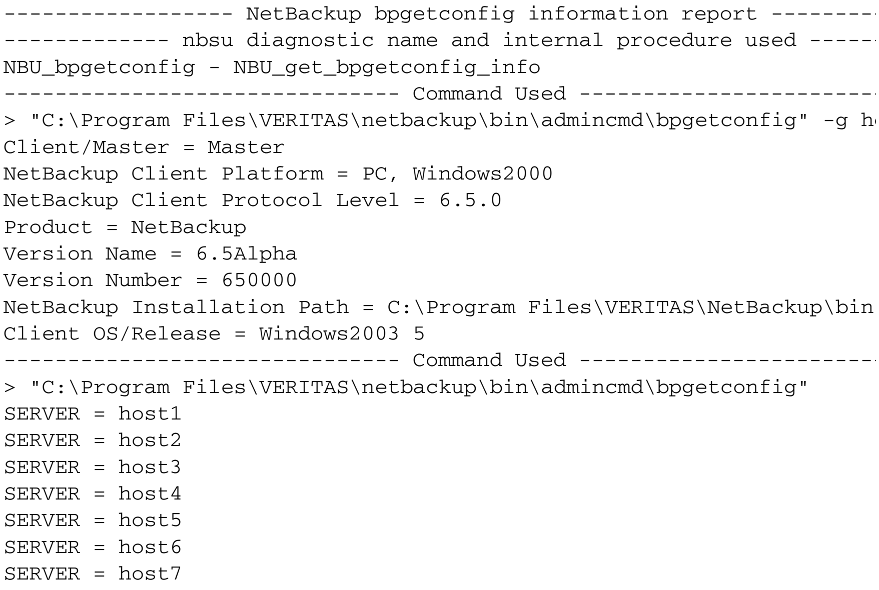


```
--------------------- Network ipconfig information report ---------
----------------------------- Command used -----------------------
> "C:\WINDOWS\system32\ipconfig" /all

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 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 h
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
```

Non-zero status for NetBackup command output

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

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

NetBackup command STDERR output

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:

```
/usr/openv/netbackup/bin/support/output/nbsu/host1_master_20060814_
164443/host1_master_20060814_164443.tar.gz
```

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

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

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

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 Symantec 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: the “NetBackup status codes and messages” chapter or in the Media Manager group in the “Media and device management status codes and messages” chapter.

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.

See “Output files: format” on page 129 for a description of the output files that nbsu generates.

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

- For a list of nbsu prerequisites and examples, and for more detail on how to gather diagnostic information to send to Symantec support, refer to the following: nbsu command in the *NetBackup Commands Guide* or see the nbsu man page.
- 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.
- In some cases, a NetBackup process or service that is not running can prevent nbsu from gathering the required data. To determine what diagnostics to run, nbsu interrogates various NetBackup components and their configuration. It then determines what NetBackup host roles exist on the system (master server, media server, client). If a NetBackup component is not operational (for example, bpgetconfig does not return anything), nbsu may be unable to investigate and report on the system.

nbsu examples

For examples on how to use nbsu, refer to the nbsu man page or to the *NetBackup Commands Guide*.

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:

      UNIX

      ```
      /usr/openv/netbackup/bin/support/nbsu 2>&1
      ```

      Windows

      ```
      install_path\NetBackup\bin\support\nbsu.exe 2>&1
      ```

    - To send all nbsu screen output including error messages to a file, enter:

      ```
      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.

  See “nbsu output” on page 129 for the location of this file.

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 status codes and messages

This chapter lists all the status codes and messages that NetBackup provides.

For the codes that relate to Media and device management, see the “Media and device management status codes and messages” chapter.

This chapter is divided into two parts

- The first section, “Status codes,” lists the NetBackup status codes in numerical order and includes an explanation of what occurred along with recommended actions.
- The second section, “Messages,” lists the same status codes but sorts them alphabetically according to the message.

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 systems:

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

On Windows systems:

```
install_path\NetBackup\bin\admincmd\bperror -statuscode
statuscode [-recommendation]
```

where *statuscode* is the number of the message.

Example:

On UNIX: `/usr/openv/netbackup/bin/admincmd/bperror -statuscode 150`

On Windows: `install_path\NetBackup\bin\admincmd\bperror -statuscode 150`

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

Note: The Symantec technical support site has a wealth of information that can help you solve NetBackup problems. Visit http://entsupport.symantec.com for comprehensive troubleshooting details.

Status codes

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

NetBackup status code: 0

Message: the requested operation was successfully completed

Explanation: No problems were detected with the requested operation.

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

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 that 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.”
- Cannot open a file.
  The file may have been locked for some reason.

- On a UNIX system, NetBackup cannot get the link name of a file.
- On a UNIX system, 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.
- On a UNIX system, the `lstat` system call fails on a file that is eligible to be backed up. This error may be a permission problem.
- On a UNIX system, 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 NetBackup 5.0 or later 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 multi-streamed backup jobs are enabled, log messages similar to the following appear that indicate volume snapshots were not enabled for the multi-streamed backup job:

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

  If multi-streamed 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 -
  ===============================
  ```

```
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
EXIT STATUS 11: system call failed
1:59:41.799 PM: [2076.2088] <4>
V_Snapshot::V_Snapshot_CreateSnapshot: INF - Snapshot creation
was not successful
1:59:41.799 PM: [2076.2088] <4>
V_Snapshot::V_Snapshot_CreateSnapshot: INF -
===============================
```

In this case, examine the `bpfis` logs for error messages regarding snapshot creation failures.

See the *NetBackup Snapshot Client Administrator’s Guide* for more details on the `bpfis` logs.

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: vfm_freeze_commit:
method: VSP, type: FIM, function: VSP_make
04:01:14.168 [376.2364] <32> onlfi_fi_split: VfMS method error
3; see following message:
04:01:14.168 [376.2364] <32> onlfi_fi_split: snapshot services:
snapshot creation failed: invalid argument(s).
```

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: your Event Viewer's Application and System Logs for error information.

- A snapshot error may have occurred if you have the following:
  - NetBackup 5.0 or later installed
  - 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. For example:

```
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.

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 of the backups related to the job have failed. It should not occur for standard file system backups.

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

Recommended action:

- For 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 Symantec support document 276903.pdf.
- See the troubleshooting chapter of the appropriate guide for a description of troubleshooting tools:
  - *NetBackup for Microsoft SQL Server Administrator's Guide*
  - *NetBackup for Lotus Notes 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 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:

1. 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.
2. 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.
3. Check ownership and permission on directories where files are restored.
4. Correct the problems that you find and retry the restore.
5. For OpenVMS clients, make sure the NetBackup client software is version 3.4 or higher.
6. If you attempted 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:

1. 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.
2. On Windows clients, verify that the account used to start the NetBackup Client service has read access to the files.
3. On Macintosh clients, this code can be due to multiple backups being attempted simultaneously on the same client. Some possible solutions are:
   - 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).
4. For a UNIX 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 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:

1. Check the All Log Entries and Problems reports to determine the system call that failed and other information about the error.
2. 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.
3. 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 exited with
status 11 (system call failed)
```

On UNIX 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.

4 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:

   a Display the Control Panel.

   b Double-click **System**.

   c On the **Performance** tab, set **Virtual Memory** to a higher value.

5 On UNIX systems, check for a semaphore problem. A possible cause for this error: the system does not have enough allocated semaphores. This error 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.

6 Run the NetBackup Configuration Validation Utility (NCVU) and note the semaphore settings in the kernel checks in section one.

7 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.

Recommended action:

- This error can occur in the following situation: when a disk storage unit attempts 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.” In NetBackup 6.0 and later: 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.

  Try the following:

  - 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: 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, 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 the following: the policy is configured with either **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.

  For instructions on how to create the `3pc.` file, refer to the *NetBackup Snapshot Client Administrator's Guide.*

- For a FlashBackup policy:

  If the CACHE= entry follows the source data entry (the entry for the data to back up), the backup fails with status code 12. Messages such as the following appear in the `/usr/openv/netbackup/logs/bpbkar` logs on the client:

  ```
  09:55:33.941 [6092] <16> bpfsmap: ERR - open_snapdisk: NBU
  snapshot enable failed error 3
  09:55:33.942 [6092] <32> bpfsmap: FTL - bpfsmap: can't open
  snapshot disk /dev/rdsk/c4t1d0s3 errno 0
  09:55:33.950 [6092] <16> bpbkar Exit: ERR - bpbkar FATAL exit
  status = 12: file open failed
  09:55:33.956 [6092] <4> bpbkar Exit: INF - EXIT STATUS 12: file
  open failed
  09:55:33.957 [6092] <2> bpbkar Exit: INF - Close of stdout
  complete
  ```

  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. Possible causes include:

- An I/O error occurred during a read from the file system.
- Read of an incomplete file or a corrupt file.
- Socket read failure. A network problem or a problem with the process that writes to the socket can cause socket read failure.
- A problem specific to NetBackup Snapshot Client (see recommended actions).

Recommended action:

1. Check the NetBackup Problems report for clues on where and why the problem occurred.
2. 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.
3. 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.
4. For NetBackup Snapshot Client only:

   Status code 13 may appear in the /usr/openv/netbackup/logs/bpbkar log, and 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
     ```

     and the following 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
     bpbkar: ERR - bpbkar FATAL exit status = 13: file read failed
     bpbkar: INF - EXIT STATUS 13: file read failed
     ```

   - 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 above the directory that was specified as the snapshot source.

NetBackup status code: 14

Message: file write failed

Explanation: A write to a file or socket failed. Possible causes include:

- An I/O error 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:

- 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 69.
- 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 using 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 if it is configured.)

Recommended action:

1. Check the NetBackup Problems report for clues on why the failure occurred.
2. On a UNIX system, check that `/etc/services` and NIS services map (if applicable) have entries for the NetBackup services: `bpcd`, `bpdbm`, and `bprd`.
3. Run the NetBackup Configuration Validation Utility (NCVU) and note the services configuration checks in section one.

4 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.
Also, see "Verifying host names and services entries" on page 43.

5 Check the level of network activity. An overloaded network can cause this error.

6 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 6.5 and the media server or the client has NetBackup 4.5.

This error can also occur if the wrong parameters are used when you run a command line.

Recommended action:

1 Check the NetBackup Problems report for clues.

2 If the error occurs when you run a command on the command line, verify that the parameters are valid.

3 An online, hot catalog backup may have been directed to a 5.x media server. The online, hot catalog backup feature was introduced in NetBackup 6.0. In the online catalog backup policy, specify a storage unit that is hosted on a 6.0 or later media server.

4 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.

5 For 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_brm_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> bpmap_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> bpmap_mm_get_devid: keepalive child:
15822 killed
14:47:02.030 [15773] <4> bpmap_mm_get_devid: DEVICE_INDEX -1
14:47:02.031 [15773] <16> bpmap_send_extend: ERR - can't obtain
device id string EMC:SYMMETRIX:601092014000
14:47:33.167 [15773] <16> bpbkar Exit: ERR - bpbkar FATAL exit
status = 227: no entity was found
14:47:33.167 [15773] <4> bpbkar Exit: INF - EXIT STATUS 227: no
entity was found
14:47:33.168 [15773] <2> bpbkar Exit: INF - Close of stdout
complete
```

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

- For a FlashBackup policy that was configured in the earlier (pre-5.0) manner: if the Backup Selections list contains the actual file name of the raw device rather than the symbolic link form, the backup fails. An example actual file name is `/devices/pci@1f,0/pci@1/scsi@3/sd@1,0:d,raw` and an example of the symbolic link form is /dev/rdsk/c0t0d0s1. Messages such as the following appear in the /usr/openv/netbackup/logs/bpbkar logs on the client:

```
09:41:30.785 [5998] <32> bpfsmap: FTL - bpfsmap: couldn't get
block name for /devices/pci@1f,0/pci@1/scsi@3/sd@1,0:d,raw
09:41:30.792 [5998] <16> bpbkar Exit: ERR - bpbkar FATAL exit
status = 20: invalid command parameter
09:41:30.797 [5998] <4> bpbkar Exit: INF - EXIT STATUS 20:
invalid command parameter
09:41:30.799 [5998] <2> bpbkar Exit: INF - Close of stdout
complete
```

  Use the symbolic link form of the device name (such as /dev/rdsk/c0t0d0s1) and retry the backup.

  CAUTION: For a FlashBackup policy that is configured with NetBackup Snapshot Client with the Perform snapshot backups option selected, the backup may complete. But the data cannot be restored if the Backup Selections list contains the actual file name of a raw device.

- The HP VxFS snapshot mechanism requires a dedicated cache partition for each snapshot. A check is made in the mount table to make sure 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/vol4c
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.

6 Compare the NetBackup version level on the server to the version level on the clients:

- On UNIX 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 in the Java log with the parameters listed in the commands usage statement.

7 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:

- 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.
- 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.

NetBackup status code: 22

Message: socket close failed

Explanation: A socket was not closed.

Recommended action:

1. 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.
2. On Sun Solaris, verify that all operating system patches are installed.

See the Operating Notes section of the *NetBackup Release Notes*.

3 On Windows, 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:

1 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.

2 Corrupt binaries are one possible cause for this error.
Load a fresh `bptm` from the install media to try to resolve the problem.

3 On Sun Solaris, verify that all operating system patches are installed.
See the Operating Notes section of the *NetBackup Release Notes*.

4 On Windows, verify that the recommended service packs are installed.

5 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.

6 Run the NetBackup Configuration Validation Utility (NCVU) on the master server and clients. Note the name resolution checks in section seven and NCVU summary.

NetBackup status code: 24

Message: socket write failed

Explanation: A write operation to a socket failed.

Recommended action:

1. 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.

2. 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)
   ```

3. On Sun Solaris, verify that all operating system patches are installed

   See the Operating Notes section of the *NetBackup Release Notes*.

4. On Windows, verify that the recommended service packs are installed.

5. 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
   ```

6. Run the NetBackup Configuration Validation Utility (NCVU) on the master server and clients. Note the name resolution checks in section seven and NCVU summary.

NetBackup status code: 25

Message: cannot connect on socket

Explanation: A process that timed out while connecting 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 (`bprd`) 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.

Other possible causes of this error:

- 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.

These errors are caused either by network connectivity issues or if a required process such as pbx_exchange is not running.

Recommended action:

1. Verify that the following are running: bpcompatd, vnetd, and Private Branch Exchange (PBX).

   For information on how to start PBX, see "Resolving PBX problems" on page 65.

   If necessary, stop and restart NetBackup:

   UNIX

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

   Windows

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

2. On a UNIX 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.

- 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.

3 Verify that the server list specifies the correct master server.

- On 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.
- On UNIX, 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.
- Make sure all recommended NetBackup patches were installed. Check the Symantec support Web site for current patch information.

  (Go to www.support.veritas.com. Then select “NetBackup” followed by “files and updates.”)
- If failure occurs when you run a user-directed backup from a client, make sure 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.
- On UNIX 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) or the NetBackup Database Manager and NetBackup Request Manager services (Windows).

4 Check the `services` file.

On UNIX, verify that the /etc/services file (and NIS services if NIS is used) has entries for the NetBackup services: bpcd, bpdbm, and bprd.

Run the NetBackup Configuration Validation Utility (NCVU) and note the services port checks in section one. Note the NetBackup daemon running and listening check and the bpps check in section three.

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** number and the **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.

Also, see "Verifying host names and services entries" on page 43.

5. On Sun Solaris, verify that all operating system patches are installed
   See the Operating Notes section of the *NetBackup Release Notes.*

6. On Windows, verify that the recommended service packs are installed.

7. 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.

8. For NetBackup Snapshot Client:
   When many devices are configured on a media server, it may take a long time for the bptpcinfo command to generate the 3pc. file. 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 3pc. file, then try the backup again.

9. Run the NetBackup Configuration Validation Utility (NCVU) on the master server and clients. Note the name resolution checks in section seven and NCVU summary.

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) 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:

1. Check the NetBackup All Log Entries report for clues on where and why the failure occurred.
2. Check the permissions on the command to be run.
3. 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: could not 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. With a UNIX client, the email was not sent to an email address 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 waiting 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:

- 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:

1. 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.
2. 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.
3. 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 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 63.

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 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.

Run the NetBackup Configuration Validation Utility (NCVU) media server checks. Note the media server and storage unit checks in sections four and five.

NetBackup status code: 38

Message: could not get group information

Explanation: Could not get the group entry that describes a UNIX 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.

Run the NetBackup Configuration Validation Utility (NCVU) `-conf` *<media server option>* and `-conf` *<client option>* checks for the associated NetBackup nodes. On the media server check, note the client configuration in the policy checks in section five.

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:

1. Try pinging the client from the server. If pinging is not possible, check for loose connections or other network problems.
2. 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.
     To display this dialog box, see “Using the Host Properties window” on page 63.
   - On UNIX and Macintosh systems the master server is the first `SERVER` entry in the `bp.conf` file.
   - On NetWare target and OS/2 clients the master server name is the first `SERVER` entry in the `bp.ini` file.

   If you change the server list on a UNIX 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.
3. Status code 40 can also be due to denial of a mount request by the operator.

4 Run the NetBackup Configuration Validation Utility (NCVU) `-conf` *<media server option>* and `-conf` *<client option>* checks for the associated NetBackup nodes. Note the ping checks in section seven.

5 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:

1 On UNIX 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 63.

You can also monitor CPU utilization to determine if this condition exists.

On UNIX clients:

- The `bpbkar` client process is hung on a file that has 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:

```
touch /usr/openv/netbackup/bpbkar_path_tr
 /usr/openv/netbackup/logs/bpbkar
```

Then retry the operation. The names of the files are logged in 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. It also occurs when it backs up file systems or the directories that reside on optical disk, which is considerably slower than magnetic disk.
  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.

2 On Windows systems, try the following:

- Disable the following file:

```
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.

3 If the server cannot connect to the client, do the following: create bpcd or bpbkar (UNIX 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:

```
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, if both the NIS and the DNS files are used, verify that they match.

Also, see "Resolving network communication problems" on page 36.

4 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.

5 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.

6 Make sure all recommended NetBackup patches are installed. Check the Symantec support Web site for current patch information. (Go to www.support.veritas.com. Then select “NetBackup” followed by “files and updates”.)

Run the NetBackup Configuration Validation Utility (NCVU) for the associated NetBackup nodes. Note the pack checks in section two.

7 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.

See the *NetBackup Administrator’s Guide, Volume II,* for more information on CLIENT_READ_TIMEOUT.

8 Make sure 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:

1 Verify that both the client and the server are operational.

2 Perform “Resolving network communication problems” on page 36.

3 Check the Problems report for clues.

NetBackup status code: 43

Message: unexpected message received

Explanation: The client and the server handshake was not correct.

Recommended action:

1. Verify that the correct version of software is running on the client and the server.
2. Enable detailed debug logging:
   - 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 the "Using logs and reports" chapter.
3. Retry the operation and examine the logs.

Note: If you use `bpstart_notify` scripts on UNIX 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:

1. Check the Problems report for information about the error.
2. Verify that the client and servers are operational and connected to the network.
3. 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.
4. Perform "Resolving network communication problems" on page 36.

NetBackup status code: 45

Message: request attempted on a non reserved port

Explanation: An attempt 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 NetBackup servers and clients, check the `/usr/openv/netbackup/bin/version` file.
- Run the NetBackup Configuration Validation Utility (NCVU) for the associated NetBackup clients. Note the client software checks in section two.

- 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 attempts to make a non-encrypted backup of the client. Since the client is configured to require encryption, the backup failed.

Recommended action:

- 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 and Macintosh clients, add a `SERVER` entry in the `bp.conf` file.
  - On NetWare target and OS/2 clients, add a `SERVER` entry in the `bp.ini` file.

    If you continue to have problems, review "Resolving network communication problems" on page 36 and "Verifying host names and services entries" on page 43.
- To make non-encrypted backups of the client, set CRYPT_OPTION on the client to *allowed* or *denied*.

For more information, 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, use the following command on the server:
  `/usr/openv/netbackup/bin/admincmd/get_license_key`.
  Select option **`f`** 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:

1. Verify that the name service (or services) used by the client are configured to resolve the host names of the NetBackup server correctly.
2. Verify that the name service (or services) used by the server are configured to resolve the host name of the NetBackup client correctly.
3. Try to ping the client from the server and the server from the client.
4. If you continue to have problems, perform "Resolving network communication problems" on page 36.
5. Run the NetBackup Configuration Validation Utility (NCVU) for the associated NetBackup nodes. Note the hostname checks in sections four and seven.

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:

1. Verify that the client name is correct in:

- 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 and Macintosh clients.
- The `bp.ini` file on OS/2 and NetWare target clients.

2 On clients and servers, verify that the name service is set up to resolve the NetBackup client names correctly.
  On UNIX clients, verify that the client's host name is in the `/etc/hosts` file or the YP hosts file or NIS maps.

3 For the NetBackup policy configuration, run the NetBackup Configuration Validation Utility (NCVU) `-conf` *<media server option>* and note the policy checks in section five. For the client hostname, note the hostname checks in sections four and seven.

NetBackup status code: 49

Message: client did not start

Explanation: The client failed to start up correctly.

Recommended action:

1 Make sure that software is installed on the client and it is the correct version. If necessary, reinstall the client software.

2 Check for full file systems on the client.

3 Enable detailed debug logging on the client:
  - Create `bpcd` and `bpbkar` (UNIX or Windows only) debug log directories.
  - On a UNIX client, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.
  - On PC clients, increase the debug or log level as explained in the debug log topics in Chapter 3.

4 Retry the operation and examine the resulting logs.

5 On UNIX 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:

1. Enable detailed debug logging:
   - Create a `bpbkar` debug log directory (UNIX or Windows only).
   - Create a `bpcd` debug log directory (this log is created automatically on Macintosh clients.)
   - On UNIX clients, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.
   - On PC clients, increase the debug or log level as explained in the debug log topics in Chapter 3.
2. Retry the operation and examine the resulting logs.
3. 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) or *`install_path`*`\NetBackup\logs` (Windows).
4. On UNIX clients, check for core files in the / directory.
5. On UNIX clients, check the system log (`/usr/adm/messages` on Solaris) for system problems.
6. This problem can sometimes be due to a corrupt binary.
   On UNIX 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.
   Run the NetBackup Configuration Validation Utility (NCVU) for the associated NetBackup clients. Note the client software checks in section two.
   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:

1. Verify that the NetBackup Database Manager service or daemon is running.
2. Verify that the file system that contains the NetBackup catalogs has enough space.
3. Create `bpbrm` and `bpdbm` debug log directories on the server and retry the operation.
4. 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:

1. Verify that the requested volume is available and an appropriate drive is ready and in the UP state.
2. 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.
3. Verify that the tape is not a cleaning tape that is configured as a regular volume.
4. When an Automated Cartridge System controls the robot, verify that the ACSLS system is up.
5. If it is an initial installation, refer to “To resolve common configuration problems” on page 25.
6. On Windows, check the Event Viewer Application log for the error messages that indicate why the tape mount did not complete. On UNIX, 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:

1. Create bpbrm debug log directories on the server.
2. On a UNIX 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, see "Using the Host Properties window" on page 63.
   Increase the unified logging levels (use the vxlogcfg command as explained in "Configuring and using unified logging" on page 90).
3. 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.

Recommended action:

1. 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:
   ```
   :System Folder:Preferences:NetBackup:logs:inetd:log.mmddyy
   ```
2. Perform "Resolving network communication problems" on page 36.
3. On UNIX clients, verify that the /usr/openv/netbackup/bin/bpcd binary exists and that it is the correct size.
4. 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
   ```
5. On the systems that include the following, make sure 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).

6. Run the NetBackup Configuration Validation Utility (NCVU) for the associated NetBackup nodes. Note the `bpcd` checks in sections one and three.

NetBackup status code: 55

Message: permission denied by client during rcmd

Explanation: The UNIX 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 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) when the client performed 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.

Run the NetBackup Configuration Validation Utility (NCVU) `-conf` *<media_server option>* and `-conf` *<client option>* checks for the associated NetBackup nodes. Note the ping checks in section seven.

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:

1. 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
```

2 For UNIX servers:

- 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.
- Run the NetBackup Configuration Validation Utility (NCVU) for the associated NetBackup nodes. Note the NetBackup services port number checks in section one.

3 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.

4 Perform "Resolving network communication problems" on page 36.

NetBackup status code: 58

Message: can't connect to client

Explanation: The server was unable to connect to the client.

Recommended action: Perform "Resolving network communication problems" on page 36.

Run the NetBackup Configuration Validation Utility (NCVU) for the associated NetBackup nodes. Note the NetBackup services port number, bpcd, and services checks in section one, and the bpcd checks in section three.

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.

Recommended action:

1 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 Macintosh clients: add a `SERVER` entry in the `bp.conf` file.
- On NetWare target and OS/2 clients: add a `SERVER` entry in the `bp.ini` file.

If you change the server list on a UNIX 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.

2 On Windows clients, enable `bpinetd` debug logging as follows:

a Create a `bpinetd` debug log directory on the client.

b Increase the debug or log level as explained in the debug log topics in Chapter 3.

c Retry the backup and examine the resulting logs to determine the cause of the failure.

3 On all clients, enable `bpcd` debug logging as follows:

a Create a `bpcd` debug log directory on the client.

b On a UNIX client, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.

c On PC clients, increase the debug or log level as explained in the debug log topics in Chapter 3.

d Retry the backup and examine the resulting logs to determine the cause of the failure.

4 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 attempts 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.

5 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 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.

6 If the preceding steps do not resolve this problem, see "Resolving network communication problems" on page 36.

7 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.

8 Run the NetBackup Configuration Validation Utility (NCVU) for the associated NetBackup clients. Note the media server checks in sections four and seven.

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:

1 Run a `df` to see if the system can read the mount table.

2 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.

3 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:

1. On all clients, enable `bpcd` debug logging as follows:
   - a Create a `bpcd` debug log directory on the client.
   - b On a UNIX client, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.
   - c On PC clients, increase the debug or log level as explained in the debug log topics in Chapter 3.
2. On a UNIX or Windows client, create the `bpbkar` debug log directory on the client.
3. On Windows clients, verify that the NetBackup Client service is running.
4. On a UNIX client, use the `ps` command to check for a client process that uses too much CPU time.
5. 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.

For detailed debug information:

1. Create a `bptm` debug log directory on the server.
2. On a UNIX 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 63.
3. Retry the operation and check the `bptm` debug log file for information on the drive, robot, and tape that causes the timeout.

4 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: Verify that the server did not crash. If that is not the problem and you need more information:

1 On UNIX and Windows clients, enable `bpbkar` debug logging.

   a Create a `bpbkar` debug log directory.

   b On a UNIX 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.

2 On other PC clients except Macintosh, create a debug log directory for `bpcd` (the `bpcd` log is created automatically on Macintosh).
To increase the amount of information that appears in the logs, see the logging topics in Chapter 3.

3 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 explained in "Configuring and using unified logging" on page 90.
If there are media servers involved, create a `bpbrm` debug log directory on them.

4 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: First, verify that the server did not crash. If that is not the problem and you need more information:

1 Set up debug logging:

   a On the server, create a `bpbrm` debug log directory.

   b On UNIX and Windows clients, create a `bpbkar` debug log directory.

c. On other PC clients except Macintosh, create a debug log directory for `bpcd` (the `bpcd` log is created automatically on Macintosh).

To increase the amount of information that appears in the logs, see the logging topics in Chapter 3.

2. 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: First, verify that the server did not crash. If that is not the problem and you need more information:

1. Set up debug logging:

   a. On the server, create a debug log directory for `bpbrm`.

   b. On UNIX and Windows clients, create a `bpbkar` debug log directory.

   c. On other PC clients except Macintosh, create a debug log directory for `bpcd` (the `bpcd` log is created automatically on Macintosh).

   To increase the amount of information that appears in the logs, see the logging topics in Chapter 3.

2. 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.

Recommended action:

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.

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:

1. Verify that the correct file list is specified for this client.
2. 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.
3. Check the All Log Entries report for clues.
4. Set up debug logging:
   - On UNIX 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).

   To increase the amount of information that appears in the logs, see the logging topics in Chapter 3.
5. Retry the operation and check the resulting debug logs.
6. On Novell systems, check 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.

Note: 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.

Run the NetBackup Configuration Validation Utility (NCVU) for the associated NetBackup clients. Note the client software checks in section two.

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 NetBackup server. On a

Windows NetBackup server, use Host Properties to set **Backup Start Notify Timeout**.

See "Using the Host Properties window" on page 63.

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 `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 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 CLLIENT_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:

1. Verify that the command is specified correctly.
2. For NetBackup Snapshot Client only:
   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.
3. Run the command manually to see if the wanted result is produced.
4. For detailed troubleshooting information, set up debug logging:
   a. On UNIX and Windows clients, create a debug log directory for `bpbkar`.
   b. On other PC clients except Macintosh, create a debug log directory for `bpcd` (the `bpcd` log is created automatically on Macintosh).

To increase the amount of information that appears in the logs, see the logging topics in Chapter 3.

c 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:

1. Check the NetBackup Problems Report for additional information on why the command failed.
2. 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.
3. Try running the `vos` command manually to duplicate the problem.

NetBackup status code: 79

Message: unsupported image format for the requested database query

Explanation: Possible causes are that the images to be synthesized were generated as follows: using an ASCII catalog, for a pre-5.0 client, on a pre-5.0 master server. Or one or more of the images to be synthesized was encrypted. These images cannot be synthesized.

Recommended action:

- Make sure that NetBackup is configured to use a binary catalog.
- Ensure that none of the images was encrypted.
- Upgrade the client to NetBackup 5.0 or later. Regenerate the full and the incremental images on the 5.0 or later master server that uses the binary catalog. Rerun the synthetic backup job.

NetBackup status code: 80

Message: Media Manager device daemon (`ltid`) is not active

Explanation: If the server is UNIX, the NetBackup device manager daemon, `ltid`, is not running. If the server is Windows, the NetBackup Device Manager service is not running.

Recommended action:

1. 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.

2 On UNIX, 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.

3 On UNIX, check the system logs to verify that ltid starts.

Note: On UNIX 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, 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:

  ```
  13:22:49 [1347] <16> bpbkar: ERR - Extra output - - ECONNRESET
  Connection reset by peer (UNIX/errno status)
  ```

  To resolve the problem, increase the CLIENT_READ_TIMEOUT value (in this instance 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:

1. For additional information, check the following:
   - NetBackup Problems report
   - System log (UNIX)
   - Event Viewer Application log (Windows)
2. Typically, this status code indicates a drive configuration problem that allows more than one process at a time to open the device.
   On UNIX, the problem may be due to:
   - 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.
3. Windows: make sure the tapes are not write protected.
4. For detailed troubleshooting information:
   a. Create a debug log directory for `bpdm` (if the device is disk) or `bptm` (if the device is tape).
   b. On UNIX, 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.
   c. 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.
   d. Retry the operation and check the resulting debug log files.

e. On Windows systems, look at the `install_path\VERITAS\NetBackup\db\media\errors` log for a drive that frequently produces errors.
   On UNIX 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:

1. 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*.
2. 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)
   - Event Viewer Application and System logs (Windows)
3. 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.
4. Windows: make sure the tapes are not write protected.
5. If bpbackupdb was used to back up the NetBackup catalog to a disk path on a UNIX system: 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.
6. If the media is tape or optical disk, check for:
   - 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. On an optical drive, the platters may not be formatted correctly.
- 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 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 a message “too many data blocks written, check tape and drive block size configuration.”

NetBackup status code: 85

Message: media read error

Explanation: The system device driver returned an I/O error while NetBackup reads from tape, optical disk, or a disk file.

Recommended action:

1. 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)
   - Event Viewer Application and System logs (Windows)
2. 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 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, 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 media (tape or optical disk).

Recommended action:

1 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)
   - Event Viewer Application and System logs (Windows)

2 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 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.
   - 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 or optical disk.

Recommended action:

1 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)
   - Event Viewer Application and System logs (Windows)

2 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.

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 8, the default shminfo_shmmax value is 1 megabyte and 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 8 or 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
  ```

- For Solaris 8, the default shminfo_shmseg value is 6. 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 10 has been used in this example. (This parameter is not applicable to Solaris 9 or 10).

```
set shmsys:shminfo_shmseg=10
```

- For Solaris 8, if your /etc/system file does set shmsys:shminfo_shmmin, then it must be less than or equal to 100 for NetBackup processes to run. (This parameter is not applicable to Solaris 9 or 10).

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:

1. Check the All Log Entries report.
2. 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.
3. 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)
   - Event Viewer Application log (Windows)
4. Verify the Media and Device Management and system configuration for the drive.
   For example, on UNIX 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.

5. Verify that the Media and Device Management configuration for the backup device matches what is specified for the storage unit in the NetBackup policy.
6. Verify that you use the correct media in the drive.
7. 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.
8. 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:

1. Check the All Log Entries report for more information.
2. 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.
3. Verify that the disk partition on which the catalog resides has enough space.
4. If these actions do not explain the problem, check the NetBackup Problems report.
5. For detailed troubleshooting information, create a bptm debug log directory on the server and retry the operation. Check the resulting debug log file.
6. 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:

1. Perform a bpverify of the affected image to determine if it is written correctly.

2. Check the NetBackup Problems report for additional information about the error.

3. Verify the Media and Device Management and system configuration for the drive.

   For example, on some UNIX 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.

4. 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.

5. 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:

- 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). 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 (`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:

1. Try the restore on another drive if possible.
2. 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)
   - Event Viewer Application and System logs (Windows)
3. For detailed troubleshooting information, create a debug log directory for `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 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 tape manager (`bptm`) 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.

1. 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, 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.
2. 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.
3. 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).
   - 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, `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 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.

4. The NetBackup `bptm` process is rejected when it requests media from the `vmd` process (UNIX) 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 systems that use it
   - Running DNS with reverse addressing not configured

5. Create `bptm` and `vmd` debug log directories and retry the operation.

6. 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, the `vmd` log is:

   `/usr/openv/volmgr/debug/daemon/log.xxxxxx`

   On Windows, the `vmd` log is:

   `install_path``\Volmgr\debug\daemon\xxxxxx.log`

7. 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 and optical manager (`bptm`) 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).

Recommended action:

- 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) 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:

1. Enable debug logging for bparchive, bpbackup, bplist, or bprestore (as appropriate) by creating debug log directories for them.
   On UNIX, if a nonroot user has problems, verify that the directory that was created has mode 666. Look for and correct any reported errors.
2. 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, they start with a slash character [/].) Also, verify that the files exist and the permissions allow NetBackup to access them.

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:

1. If the error occurred on a command line, examine the standard error output from the command for an explanatory message.

2 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.

3 Check the NetBackup Problems report for clues.

4 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.

5 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, the `/usr/openv/netbackup/bp.conf` file does not exist.

Recommended action: On Windows, reinstall NetBackup software on the client. On UNIX, 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, the `SERVER =` *server_name* line is omitted from the `bp.conf` file. On Windows, the server list contains no entries.

Recommended action:

- On a UNIX 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.

- Run the NetBackup Configuration Validation Utility (NCVU) for the associated NetBackup clients. Note the `bp.conf` or `bpgetconfig` checks in section four.

- On an OS/2 or 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:

1. Specify at least one file to be restored.
2. 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:

1. Ensure that the Veritas Security Services is installed and configured.

   For complete installation instructions, see the *Veritas Security Services Installation Guide*.
2. Check that both parties have a valid certificate. Examine the expiry date that is listed from a `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 2003 GMT
   Authentication method: Microsoft Windows
   Operation completed successfully.
   ```

   Shows an expiry date of September 19th, 2003. After 12:51:55 GMT this credential is no longer valid and a new credential is required.

3 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 *Veritas Security Services Administrator's Guide*.

4 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 *Veritas Security Services Administrator's Guide* for more information on broker hierarchies and how to establish trust relationships between brokers.

5 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.

6 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:

1 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.

2 Ensure that the system has sufficient swap space and the following directories are not full:

- `/home/`*`username`*
- `/user/openv/netbackup/logs`
- `/tmp`

3 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:

```
17:19:27.653 [904.872] <2> GetAzinfo: Peer Cred Info.
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 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:

1. Ensure that the Authorization Service or Daemon is running.

   Refer to the *Veritas Security Services Administrator's Guide* for more information on authentication and authorization daemons.

2. 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.

3. Ensure that the system has sufficient swap space and the following directories are not full:

- `/home/<userName>`
- `/user/openv/netbackup/logs`
- `/tmp`

4 Ensure that the server that contacts the master has a valid certificate. The machine certificate can be examined as follows:

For UNIX:

```
# 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: Veritas Private Security
Operation completed successfully.
```

If the expiry date was exceeded, use `bpnbat -LoginMachine` to obtain a new credential for the machine.

See the *Netbackup Commands* manual for more information on `bpnbat`.

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: `Program Files\VERITAS\var\vxss\credentials` for Windows, `/usr/openv/var/vxss/credentials` for UNIX.

This credential should have the full name of the machine as in the following example: `machine1.company.com`.

5 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\Communicati
on\ClientMaxConnections
```

UNIX: `/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 service or daemon. Note that extreme increases in the maximum number of connections can cause performance degradation.

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:

1. Check the NetBackup Problems report for additional information about the error.
2. For detailed troubleshooting information, create `admin` and `bpdbm` debug log directories and retry the operation. Check the resulting debug logs.
3. 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.

Run the NetBackup Configuration Validation Utility (NCVU) on the master server. Note the NetBackup database configuration checks in section six.

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) that does not exist.

Recommended action: Retry the command by using a valid device file name.

Run the NetBackup Configuration Validation Utility (NCVU) on the master server. Note the NetBackup database configuration checks in section six.

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:

1. Check the NetBackup Problems report for additional information about the error. Some possible causes are:
   - The path does not exist.
   - On a UNIX system, one of the paths contains a symbolic link.
2. 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:

1. Fix the problem that was reported in the error message in the bprecover output.
2. Refer to the following to identify which NetBackup services to shut down before a NetBackup database recovery attempt:
   "Catalog recovery from an online backup" on page 540 or "Catalog recovery from offline backup" on page 566.
   The NetBackup services should be shut down except for the NetBackup Client Service, which must be running for the database recovery to succeed.
3. Check the NetBackup Problems report for additional information about the error. Some possible causes are:
   - 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:

1. Either free sufficient space or add more space to the file system for this storage unit.
2. 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.
3. 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:

1. Check the NetBackup Problems report for additional information about the error.
2. Check the system log for reported problems.
3. For detailed troubleshooting information, create `bpdbm`, `bptm`, and `bprd` debug log directories on the master server. Increase the unified logging level.
   Use the `vxlogcfg` command as explained in "Configuring and using unified logging" on page 90.
   Retry the operation and check the resulting debug logs.
4. 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:

1. Examine the NetBackup Problems report.
2. 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:

   - 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 master server, create a soft link in the NetBackup image catalog.
3. Review "Verifying host names and services entries" on page 43.
4. Run the NetBackup Configuration Validation Utility (NCVU) -conf *<client option>* on the master server for the associated NetBackup clients. Note the client hostname checks in section seven.

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 NetBackup server

or in the registry on a Windows NetBackup server. These options deny list and restore requests from all NetBackup clients.

Recommended action:

1 If you suspect that the software versions are the problem, verify that all NetBackup software is at the same version level.

   - On UNIX 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.

2 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 NetBackup server or from the registry on a Windows NetBackup server. Then, stop and restart the NetBackup request daemon (UNIX) or NetBackup Request Manager service (Windows).

3 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 attempted that did not come from the root user (on UNIX) or the administrator (on Windows).

Recommended action: Retry the operation as a root user (on UNIX) 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) 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 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.

- 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 Veritas 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:

  ```
  10:09:56.566 [1146] <32> bpfsmap: FTL - bpfsmap: FlashBackup
  abort - required VxFS dynamic linked libraries for NetBackup are
  not installed. Please visit the Veritas support web site, and
  refer to Technote number 262225 for further information.
  10:09:56.571 [1146] <16> bpbkar Exit: ERR - bpbkar FATAL exit
  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) 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) 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:

1 Examine the NetBackup Problems and All Log Entries reports.

2 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, 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.

3 If the problem persists longer than ten minutes, it may be necessary to reboot 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:

1. Restart the service at a later time and investigate the system problems that limit the number of processes.
2. 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), or the NetBackup Database Manager service (on Windows). This error usually occurs because different versions of software are used together.

Recommended action:

1. Verify that all software is at the same version level.

2. 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 attempted 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 storage unit that is involved are appropriate for the backup attempted:

- For NetBackup Snapshot Client only:
  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-tl4-0`) 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: This status code indicates a snapshot-backup related error regarding Windows Open File Backup or Snapshot Client.

Recommended action:

1 For Windows Open File Backup: If the client is using Open File Backup to back up open or active files, it is possible that the VSP/VSS cache files are too small for the number of files being backed up using VSP/VSS.

```
8:51:14.569 AM: [1924.2304] <2> tar_base::V_vTarMsgW: ERR -
failure reading file: D:\ test.file (WIN32 5: Access is denied.
)
8:51:14.569 AM: [1924.2304] <4> tar_base::V_vTarMsgW: INF - tar
message received from dos_backup::tfs_readdata
8:51:14.569 AM: [1924.2304] <2> tar_base::V_vTarMsgW: ERR -
Snapshot Error while reading test.file
8:51:14.569 AM: [1924.2304] <4> tar_base::V_vTarMsgW: INF - tar
message received from tar_backup::nextfile_state_switch
8:51:14.569 AM: [1924.2304] <2> tar_base::V_vTarMsgW: FTL -
Backup operation aborted!
8:51:14.569 AM: [1924.2304] <2> tar_base::V_vTarMsgW: INF -
Client completed sending data for backup
8:51:14.569 AM: [1924.2304] <2> tar_base::V_vTarMsgW: INF - EXIT
STATUS 156: snapshot error encountered
```

If this is the case, and `bpbkar` debug logs are turned on, a message similar to the one above should appear in the `bpbkar` debug log for the backup.

Increase the sizes of the VSP/VSS cache files used by the backup. This action depends on whether VSP (Veritas Volume Snapshot Provider) or VSS (Microsoft Volume Shadow Copy Service) was used as the Windows Open File Backup Snapshot Provider. If VSP is being used as the snapshot provider, try one of the following:

- (preferred) Change the VSP Cache File Size configuration for the affected client in the VSP tab for the client's Host Properties in the NetBackup Administration Console. Ensure that the "Customize the cache sizes" check box is unchecked to let NetBackup automatically determine the best VSP cache file sizes. In most cases, NetBackup will be able to create a large enough VSP cache file for backups if the "Customize the cache sizes" check box is unchecked.
- Increase either the initial VSP cache size and the maximum VSP cache size on your own, depending on the requirements of your installation and your usage of VSP. To specify your own Initial and Maximum Cache File sizes, select the **Customize the cache sizes** checkbox and specify your own Initial and Maximum Cache File Sizes either in MBs or percentage of disk space. Use caution when manually specifying sizes for the Initial and Maximum Cache Size since it is used regardless of the sizes of the volumes being backed up. If enough space is not allocated, the backup job could fail with a snapshot error.

See the *NetBackup Administrator's Guide, Volume I,* for information on changing the configuration of VSP cache file sizes.

If backups still abort with error status 156 after making changes to the VSP cache file size configuration, there may not be enough free disk space on the affected client. Free up as much disk space on the drives of the affected client as possible.

If VSS is being used as the Window Open File Backup Snapshot Provider, increase the cache size being used by VSS by using the Shadow Copy configuration in Windows 2003. Use the following steps to increase the cache size.

a. Open the Windows 2003 Computer Management application. To open Computer Management, click **Start**, point to **Settings**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Computer Management**.

b. In the console tree, right-click **Shared Folders**, select **All Tasks**, and select **Configure Shadow Copies**.

c. Select the volume where you want to make changes, and then select **Settings**.

d. In the Settings dialog box, change the **Maximum Size** setting to either No Limit or a size large enough to suit the requirements of your installation and your usage of VSS.

2. For backups using Snapshot Client and the NAS_Snapshot method, with or without SnapVault:

   - If the backup fails with status code 156, consult the following NetBackup client logs for more detail:
     - bpfis legacy log, in `/usr/openv/netbackup/logs` (UNIX) or *`install_path`*`\NetBackup\logs` (Windows). If the bpfis directory does not already exist, you must create it and rerun the job.
     - ndmp unified log (originator ID 151), in `/usr/openv/logs` (UNIX) or *`install_path`*`\NetBackup\logs` (Windows).

     If necessary, increase the logging level and retry the job.

     For assistance with legacy and unified logging, refer to the “Using logs and reports” chapter.

   - On Windows clients, when restoring files from a backup made with the NAS_Snapshot method, the “NetBackup Client Service” must be logged in 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 log-in to the Administrator account and restart the service.
- Retry the restore.

3 For other NetBackup Snapshot Client issues:

- The file system 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 - vfm_freeze: method: nbu_snap, type:
FIM, function: nbu_snap_freeze
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 specified for the snapshot source has been mounted.

- The file system 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/datafile` and `/oracle`, are actually symbolic links 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 - vfm_freeze: method: vxvm, type:
FIM, function: vxvm_freeze
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 prior to running the backup, or another backup is currently running that is using 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 - vfm_freeze: method: vxvm, type:
FIM, function: vxvm_freeze
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 running the backup.

- **vxvm** was selected as the snapshot method, and a Veritas Volume Manager Veritas snapshot mirror of the snapshot source volume has been created. However, two different backup jobs (A and B) attempt to back up the same volume (for example, `vol01`), but job A starts just before job B. Because there is a brief pause between finding an available snapshot mirror and actually forming the snapshot of it, job B (running slightly behind job A) might attempt to create a snapshot of the snapshot mirror just before job A (running slightly ahead) actually 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 - vfm_freeze: method: vxvm, type:
FIM, function: vxvm_freeze
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 above 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 were not automatically deleted by `nbu_snap`.)

```
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 - vfm_freeze: method: nbu_snap, type:
FIM, function: nbu_snap_freeze
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
```

a Look for stale snapshots by running the `/usr/openv/netbackup/bin/driver/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
```

b 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 above 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 `/usr/openv/netbackup/logs/bpfis` log:

```
15:21:45.716 [4236] <4> create_mount_point: INF - Created mount
point /tmp/_vtrax_test_fastrax_dlt: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_fastrax_dlt: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 - vfm_freeze: method:
VxFS_Checkpoint, type: FIM, function: VxFS_Checkpoint_freeze
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 will not be able to use **VxFS_Checkpoint** to back up any data in the file system where the checkpoint is mounted.

a 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. Following is sample output. 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
```

b Remove the checkpoint by entering the following:

```
/usr/lib/fs/vxfs/fsckptadm remove checkpoint /file_system
```

c If the checkpoint cannot be removed, unmount the checkpoint and retry step b.

- If a snapshot backup failed 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/VfMSAAAq7aOqD 2>/var/tmp/VfMSBAAr7aOqD
```

```
19:13:07.687 [14981] <2> onlfi_vfms_logf: INF - --- Dumping file
/var/tmp/VfMSAAAq7aOqD (stdout):
19:13:07.687 [14981] <2> onlfi_vfms_logf: INF - --- End of file
/var/tmp/VfMSAAAq7aOqD
19:13:07.687 [14981] <2> onlfi_vfms_logf: INF - --- Dumping file
/var/tmp/VfMSBAAr7aOqD (stderr):
19:13:07.687 [14981] <2> onlfi_vfms_logf: INF -     clone group
and volume already exists
19:13:07.688 [14981] <2> onlfi_vfms_logf: INF - --- End of file
/var/tmp/VfMSBAAr7aOqD
```

NetBackup automatically creates VxVM clones for TimeFinder, ShadowImage, or BusinessCopy backups of data configured over volumes. After the backup has completed, NetBackup removes the VxVM clone. In this case, a system crash or reboot 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.)

a When no backups are running, use the following VxVM command to list any clones: `vxdg list`
The clone name will be of the form `clone_`*disk_group*`_clone`.

b 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 removing a VxVM clone, refer to the *NetBackup Snapshot Client Administrator's Guide*. For `vxdg`, refer to the *Veritas Volume Manager Administrator's Guide*.

c 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 failed using the FlashSnap or VVR snapshot method, there may be a VxVM snapshot left over from a previous backup. You may see messages similar to the following in the `/usr/openv/netbackup/logs/bpfis` log:

```
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 - vfm_freeze_commit:
method: FlashSnap, type: FIM, function: FlashSnap_freeze_commit
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 configured over volumes. After the backup completes, NetBackup removes the VxVM snapshot. In this case, a system crash or reboot 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.)

a Find the VxVM disk group:

```
vxdg list
```

The format of the disk group name is as follows:

```
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, including deported ones, by entering:

```
vxdisk -o alldgs list
```

The disk groups listed in parentheses are not imported on the local system.

b Deport the VxVM disk group:

```
vxdg deport primaryhost_diskgroup_split
```

Enter the following on the primary (original) client:

c Import and join the VxVM disk group:

```
vxdg import primaryhost_diskgroup_split
vxrecover -g primaryhost_diskgroup_split -m
vxdg join primaryhost_diskgroup_split diskgroup
```

d 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:

a Enter the following to display unsynchronized mirror disks:

```
vxprint -g diskgroup
```

b Enter the following to resynchronize the mirror disks:

```
vxassist -g diskgroup -v volume snapback
```

- When using a snapshot method such as VxFS_Checkpoint to back up a VxFS file system, the backup will fail if the Veritas File System (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 - vfm_freeze:
method: VxFS_Checkpoint, type: FIM, function:
VxFS_Checkpoint_freeze
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).

```
13:43:39.095 [16375] <2> onlfi_vfms_logf: INF - Executing
command:
13:43:39.095 [16375] <2> onlfi_vfms_logf: INF -
/usr/sbin/vxprint -g rootdg -q -t -e 'assoc=“pfi_concat“'
</dev/null >/var/tmp/VfMSAA Arja4.F 2>/var/tmp/VfMSBAAsja4.F
13:43:39.215 [16375] <2> onlfi_vfms_logf: INF -
pfi_find_snapdone: 0 SNAPDONE plexes found

13:43:39.215 [16375] <2> onlfi_vfms_logf: INF - Executing
command:
13:43:39.215 [16375] <2> onlfi_vfms_logf: INF -
/usr/sbin/vxassist -g rootdg snapprint pfi_concat  </dev/null
>/var/tmp/VfMSAAArja4.F 2>/var/tmp/VfMSBAAsja4.F
13:43:39.512 [16375] <2> onlfi_vfms_logf: INF - 0 active plexes
for /rootdg/pfi_concat:  0 are PFI  0 non-PFI
13:43:39.512 [16375] <2> onlfi_vfms_logf: INF -
pfi_find_active.3309: exiting with VXVM_E_SYS = 3
13:43:39.512 [16375] <2> onlfi_vfms_logf: INF -
pfi_snapshot.3866: No PFI snapshot. err= 3
```

Configure the VxVM mirrors as described in the Instant Recovery chapter of the *NetBackup Snapshot Client Administrator's Guide.*

- When using the VxFS_Checkpoint snapshot method, the backup will fail 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:
14:54:27.531 [23563] <32> onlfi_freeze_fim_fs: FTL - open_ckpt:
Cannot open checkpoint on /mnt_vxvm/2G_concat :
fsckpt_get_api_version returns 1; mountable checkpoints not
supported with this version
```

Upgrade the client file system to a version that supports mountable VxFS Storage Checkpoints, or 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:

1. Examine the NetBackup error log to determine why the system call failed. Then correct the problem. It may be a permission problem.
2. 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 "Configuring and using unified logging" on page 90.)
   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 attempt to authenticate one another.

Recommended action:

1. Ensure that the authentication libraries exist:

   Windows:

   ```
   install_path\NetBackup\lib\libvopie.dll
   install_path\NetBackup\lib\libvnoauth.dll
   ```

   UNIX (except HP-UX):

   ```
   /usr/openv/lib/libvopie.so
   /usr/openv/lib/libvnoauth.so
   ```

   UNIX (HP-UX only):

   ```
   /usr/openv/lib/libvopie.sl
   /usr/openv/lib/libvnoauth.sl
   ```

   Macintosh:

   ```
   :System Folder:Extensions:libvopie.dll
   :System Folder:Extensions:libvnoauth.dll
   ```

2. 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: `/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.

3 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.

4 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:

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

5 Add back the names that were removed in step 3 and retry the operation.

6 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. See www.veritas.com for ordering information

Explanation: The time that was allowed for the NetBackup evaluation software ended.

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 attempted 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:

- 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 attempted 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 `DISALLOW_BACKUPS_SPANNING_MEDIA` option was present in `bp.conf` (on UNIX) 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 attempted 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 attempted 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 attempted 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:

- 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 actually 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 in the *NetBackup Release Note.*

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 attempted 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:

- 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, attempt 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:

- 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:

1. 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 Symantec customer support:

   ```
   "attempted to write 32767 bytes, not a multiple of 512"
   ```

2. On UNIX, 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*. Also see step 7 of this procedure.

   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.

3. If the problem occurs with a particular client only, verify that the client binaries are correct, especially for bpcd.

4. 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

5. Verify the following:

   - The media, by using the NetBackup image verify option.
   - That you used the correct media type for the device.

6. Check the system or the console log for errors (on UNIX) or the Event Viewer Application log (on Windows).

7. 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, 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.

Take the corrective action that is suggested in step 2.

8. 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:

1. Check the NetBackup Problems report and the status lot or the progress log on the client for additional information about the error
2. 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 attempted 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

Recommended action:

1. Check the NetBackup Problems report to find the exact cause of the failure.
2. 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 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.

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:

1. Check the NetBackup Problems report for the cause of the problem.
2. Verify that the NetBackup Volume Manager (`vmd`) is active on UNIX or the NetBackup Volume Manager service is active on Windows.
3. 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 attempted 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 attempted 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:

- On a UNIX 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 as explained in 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:

1. Create a `bpcd` debug log directory on the client (on a Macintosh, NetBackup creates the log automatically).
2. On a Windows client, create a `tar` debug log directory.
3. Increase the logging level on the client:
   - On a UNIX client, add the `VERBOSE` option to the `/usr/openv/netbackup/bp.conf` file.
   - On PC clients, increase the debug or log level as explained in the debug log topics in Chapter 3.
4. 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:

- If the problem is with a UNIX client, create a `/usr/openv/netbackup/logs/tar` debug log directory on the client and rerun the operation.

  a. Check the tar debug log file for any error messages that explain the problem.
  b. Reboot the client to see if it clears the problem.
  c. 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:
  a. Create a bpcd debug log directory on the client (on a Macintosh NetBackup creates the log automatically).
  b. On a Windows client, create a tar debug log directory.
  c. Increase the debug or log level as explained in the debug log topics in Chapter 3.
  d. Rerun the operation and check the resulting debug logs.
  e. Reboot 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:

- If the problem is with a UNIX client, create a /usr/openv/netbackup/logs/tar debug log directory on the client and rerun the operation.
  a. Check the tar debug log file for any error messages that explain the problem.
  b. Reboot the client to see if it clears the problem.
  c. 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:
  a. Create a bpcd debug log directory on the client (on a Macintosh NetBackup creates the log automatically).
  b. Increase the debug or log level as explained in the debug log topics in Chapter 3.
  c. On a Windows client, create a tar debug log directory.
  d. Retry the operation and check the resulting debug logs.
  e. Reboot 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:

- If the problem is with a UNIX client:
  - a Enable `bpcd` debug logging by creating the `/usr/openv/netbackup/logs/bpcd` directory on the client.
  - b 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:
  - a Create a `bpcd` debug log directory on the client (on a Macintosh NetBackup creates the log automatically).
  - b Increase the debug or log level as explained in the debug log topics in Chapter 3.
  - c On a Windows client, create a `tar` debug log directory.
  - d Retry the operation.
  - e Check the resulting debug logs for the parameters that were passed to `tar` and call customer support.

NetBackup status code: 186

Message: tar received no data

Explanation: NetBackup did not send data to `tar`.

Recommended action:

1. Retry the operation and check the status or the progress log on the client for any error messages that reveal the problem.
2. Verify that the tape is available and readable.
3. Verify that the drive is in an UP state. Use the Device Monitor.
4. For detailed troubleshooting information:
   - a Create a `bptm` debug log on the server.
   - b On a Windows client, create a `tar` debug log.
   - c 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 client, delete `DISALLOW_SERVER_FILE_WRITES` from the `/usr/openv/netbackup/bp.conf` file.
- On a Microsoft Windows or NetWare nontarget client, select **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 `DISALLOW_SERVER_FILE_WRITES` from the `bp.conf` file in the NetBackup folder in the Preferences folder.
- On a NetWare target client, set `ALLOW_SERVER_WRITE` to yes in the `bp.ini` file.

NetBackup status code: 190

Message: found no images or media matching the selection criteria

Explanation: A verify, duplicate, or import was attempted 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 attempted and failed for all selected images.

Recommended action:

- 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 `sid`*`xxx`* directories to determine the root cause:

  ```
  UNIX: /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. Setting the value to 0 disables 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 63.

NetBackup status code: 195

Message: client backup was not attempted

Explanation: A backup job was in the NetBackup scheduler's worklist but was not attempted.

Recommended action:

1. Retry the backup either immediately with a manual backup or allow the normal scheduler retries.
2. 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 "Configuring and using unified logging" on page 90.)
   After the next backup attempt, check the logs.
   Some actions to perform are:
   - Verify that the `vmd` and the `ltid` daemons (UNIX) 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 attempted because the backup window was no longer open.

Recommended action:

- 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 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:

1. Check the client progress log (if available) to determine the policy and schedule that were specified.
2. 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
- Run the NetBackup Configuration Validation Utility (NCVU) `-conf` *<media server option>* on the master server. Note the policy checks in section five.

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 "Configuring and using unified logging" on page 90.
  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:

1. 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.
2. 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 nbrb.

     Use the `vxlogcfg` command as explained in “Configuring and using unified logging” on page 90.
   - 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.
3. 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.
4. 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.

1. Verify that the schedule specifies the correct storage unit.
2. 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 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 "Using the Host Properties window" on page 63.
3. Verify that the master server can communicate with `bpcd` on the host that has the storage unit.
4. See "Testing media server and clients" on page 34 and "Resolving network communication problems" on page 36.
5. 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 "Configuring and using unified logging" on page 90.
     Also, check the `bpcd` legacy debug logs.
   - If the error occurred 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:

1. From the master server, ping the master and all media servers by using the host names in the storage unit configuration.
2. 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 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 "Using the Host Properties window" on page 63.
3. See "Testing media server and clients" on page 34 and "Resolving network communication problems" on page 36.
4. 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.
5. Run the NetBackup Configuration Validation Utility (NCVU) `-conf` *<media server option>* on the master server for the associated NetBackup media servers. Note the media server host name checks in sections four and seven.

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:

Note: Also, see "Resolving network communication problems" on page 36.

---

1. From the master server, ping the master and all media servers by using the host names in the storage unit configuration.
2. 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 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 "Using the Host Properties window" on page 63.

3 On UNIX 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 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.

---

4 On Windows servers:

a Verify that the bpcd entries are correct in the following:
%SystemRoot%\system32\drivers\etc\services

b 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.

c Stop and restart the NetBackup services.

5 See "Testing media server and clients" on page 34 and "Resolving network communication problems" on page 36.

6 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.

7 Run the NetBackup Configuration Validation Utility (NCVU) `-conf` *<media server option>* on the master server for the associated NetBackup media servers. Note the NetBackup services, ports, and bpcd checks in section one, the media server hostname and ping checks in sections four and seven.

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:

Note: Also, see "Resolving network communication problems" on page 36.

1 From the master server, ping the master and all media servers by using the host names in the storage unit configuration.

2 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 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 "Using the Host Properties window" on page 63.

3 On a UNIX 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)

4 On Windows servers:

a Verify that the bpcd entries are correct in the services file:
`%SystemRoot%\system32\drivers\etc\services`

b 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.

c Stop and restart the NetBackup services.

5 See "Testing media server and clients" on page 34 and "Resolving network communication problems" on page 36.

6 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.

7 Run the NetBackup Configuration Validation Utility (NCVU) -conf <*media server option*> on the master server for the associated NetBackup media servers. Note the NetBackup services, ports, and bpcd checks in section one, the media server hostname and ping checks in sections four and seven.

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 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 "Using the Host Properties window" on page 63.

Recommended action:

1 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) or the NetBackup Database Manager and NetBackup Request Manager services (Windows).

2 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.

NetBackup status code: 207

Message: error obtaining date of last backup for client

Explanation: When nbpem tries to obtain the date of the last backup for a particular client, policy, and schedule combination, an error occurs.

Recommended action:

1. Verify that the NetBackup database manager (bpdbm) process (on UNIX) or the NetBackup Database Manager service (on Windows) is running.
2. Examine the All Log Entries report for the appropriate time frame to gather more information about the failure.
3. For detailed troubleshooting information, create a bpdbm log directory on the master server. Increase the logging level for the diagnostic and debug logs for nbpem.
   Use the vxlogcfg command as explained in "Configuring and using unified logging" on page 90.
   Retry the operation, then check the resulting logs.

NetBackup status code: 209

Message: error creating or getting message queue

Explanation: When a NetBackup process attempts 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 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 servers, also gather the output of the 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 attempts 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 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 servers, also gather the output of the `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 attempts 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 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 a UNIX server, 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:

1. Examine the Backup Status and All Log Entries report for the appropriate time period to determine the policy or schedule that received the error.
2. Verify that the storage unit's drives are not down.
3. 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
4. Verify that the robot number and host name in the storage unit configuration matches the Media and Device Management device configuration.
5. 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.

6 If the storage unit is on a UNIX 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.

7 For detailed troubleshooting information, increase the logging levels of nbrb and mds on the master server.
   Use the vxlogcfg command as explained in "Configuring and using unified logging" on page 90.
   Retry the operation and check the resulting debug logs.

8 Run the NetBackup Configuration Validation Utility (NCVU) -conf <*media server option*> on the master server for the associated NetBackup media servers. Note the storage unit and tpconfig checks in section five.

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:

1 On a UNIX 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.

2 Attempt to view the global configuration settings by using the NetBackup administration interface (on UNIX systems), or by using Host Properties (on Windows systems).

3 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:

1 On a UNIX 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.

2 For detailed troubleshooting information, create a debug log directory for bpdbm on the master server. Increase the logging level for nbpem (use the vxlogcfg command as explained in "Configuring and using unified logging" on page 90). 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:

1 On a UNIX server, verify that the NetBackup database manager (bpdbm) process is running. On a Windows server, verify that the NetBackup Database Manager service is running.

2 Attempt to view the storage unit configuration by using the NetBackup administration interface.

3 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.

4 Run the NetBackup Configuration Validation Utility (NCVU) -conf *<media server option>* on the master server for the associated NetBackup media servers. Note the storage unit checks in section five.

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:

1 On a UNIX server, verify that the NetBackup Database Manager (bpdbm) process is running. On a Windows server, verify that the NetBackup Database Manager service is running.

2 Attempt to view the policy configuration by using the NetBackup administration interface.

3 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 attempts to use the storage unit within the current backup session.

Recommended action: Look in the Job Details window for the failed job.

1. Verify that the schedule specifies the correct storage unit and the storage unit exists.
2. Verify that the following devices are running: the Media Manager device daemon (`ltid`) (UNIX server) or the NetBackup Device Manager service (Windows server). Use `bpps` on UNIX and the Activity Monitor on Windows or the Services application in the Windows Control Panel.
3. 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
4. If the storage unit is a tape or optical disk, verify that at least one of the drives is in the UP state. Use the Device Monitor.
5. Verify that the robot number and host in the storage unit configuration match what is specified in the Media and Device Management device configuration.
6. Verify that the master server can communicate with the `bpcd` process on the server that has the storage unit.

   a. Verify that `bpcd` listens on the port for connections.

   On a UNIX 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
   ```

   b. Check the nbrb and the mds logs by using the `vxlogview` command.

  c If the cause of the problem is not obvious, perform some of the steps in "Resolving network communication problems" on page 36.

7 Run the NetBackup Configuration Validation Utility (NCVU) `-conf` <*media server option*> on the master server for the associated NetBackup media servers. Note the policy, storage unit, and `tpconfig` checks in section five, and the `bpcd` checks in section one.

NetBackup status code: 220

Message: database system error

Explanation: The `bpdbm` process (UNIX), 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 "Configuring and using unified logging" on page 90.

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) 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) 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) 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:

1. If this status involves a media server, verify that its server list specifies the correct master server. On a UNIX 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 "Using the Host Properties window" on page 63.
2. 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.

Run the NetBackup Configuration Validation Utility (NCVU) `-conf` *<media server option>* on the master server for the associated NetBackup media servers. Note the policy checks in section five.

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) 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 eof 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:

1. Verify that all NetBackup software is at the same version level. Update earlier versions of NetBackup software.

- On UNIX 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.

2 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) 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 catalog entry. This error 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 attempt to recreate the error. The debug logs to create are as follows:

- On the server, `bptm`, `bpbrm`, and `bpdbm`.
- On UNIX and Windows clients, `bpbkar`.
- On other clients, `bpcd`.

Note: To increase the amount of information that is included in the logs, see “Debug logs on PC clients” on page 111.

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 attempted 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 (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:
/usr/openv/netbackup/vault/sessions/vault_name/session.last
Windows:
install_path\Netbackup\vault\sessions\vault_name\session.last
```

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:
/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`, `vlteject`, `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 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: /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 sid*xxx session id* directory for the specified profile. Either no Vault jobs were run for this profile or the corresponding sid*xxx session id* directory (or directories) were removed from the following directory:

```
UNIX: /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: /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, nbvault.exe on Windows). Possible causes are:

- The Symantec 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: /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 vaulting 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: /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: /usr/openv/netbackup/vault/sessions/vault_name/sidxxx
Windows:
install_path\NetBackup\vault\sessions\vault_name\sidxxx
```

(where *xxx* is the session ID)

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: /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: /usr/openv/netbackup/vault/sessions/vault_name/sidxxx
Windows:
install_path\NetBackup\vault\sessions\vault_name\sidxxx
```

(where *xxx* is the session ID)

Use the robtest utility to ensure that you can communicate with the Vault robotic library. Once 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: /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: /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: /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: /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: /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: /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 attempt 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:

- Review the Vault debug log in the following directory for detailed information about why the process failed:

  ```
  UNIX: /usr/openv/netbackup/logs/vault
  Windows: install_path\NetBackup\logs\vault
  ```

- Also review the `summary.log` in each of the `sid`*`xxx`* directories that had problems:

  ```
  UNIX: /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: /usr/openv/netbackup/logs/vault
Windows: install_path\NetBackup\logs\vault
```

Also review the `summary.log` in each of the `sid`*`xxx`* directories that had problems:

```
UNIX: /usr/openv/netbackup/vault/sessions/vault_name/sidxxx
Windows:
install_path\NetBackup\vault\sessions\vault_name\sidxxx
```

(where *xxx* is the session ID)

Once the problem is resolved, rerun the Vault session, `vlteject` command, or `vltopmenu` command.

NetBackup status code: 302

Message: error encountered attempting 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: /usr/openv/netbackup/logs/vault
Windows: install_path\NetBackup\logs\vault
```

Review the `summary.log` in each of the `sid`*`xxx`* directories that had problems:

```
UNIX: /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: /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: /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: /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 `bpduplicate` 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: /usr/openv/netbackup/logs/vault
Windows: install_path\NetBackup\logs\vault
```

Also review the `summary.log` in each of the `sid`*xxx* directories that had problems:

```
UNIX: /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 bpduplicate 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 `vltejec`t 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: /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 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:

- On UNIX, 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: /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

Explanation: 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:

1. Remove the media from the MAP if it is already full.
2. 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 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: 340

Message: vault configuration tag not found

Explanation: An optional attribute may be missing in the Vault configuration file. This internal error generally does not cause problems in Vault's functioning. Note that the Vault configuration file is located at `install_path/netbackup/db/vault/vault.xml.`

Recommended action: If Vault's functioning 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:

- Select a valid server group type: MediaSharing, NOM, 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:

- 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:

- Verify that the specified server group name is not in use.
- Attempt 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:

- 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 attempted by using a server group that does not exist.

Recommended action:

- 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, attempt 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:

- 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 machine 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:

- 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, attempt 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:

- 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 failed because the server group owns one or more media.

Recommended action:

- 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 that is being added.

Recommended action:

- Ensure that the server group member that you are adding 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. Refer to the *NetBackup Administrator's Guide, Volume I,* for more details on the `auth.conf` file.

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 login dialog box.

Recommended action: Check the `auth.conf` file on the machine (host name) specified in the NetBackup-Java login dialog box for the proper authorization. If the file does not exist, create it with the proper entry for this user name.

Refer to the *NetBackup Administrator's Guide, Volume I,* for more details on the `auth.conf` file.

NetBackup status code: 503

Message: Invalid username.

Explanation: For UNIX host login, the NetBackup Java application server on the host where the login is requested does not recognize the user name.

For Windows host login, the NetBackup-Java authentication service on the host where the login is requested does not have sufficient privileges to grant the request.

Recommended action:

- For UNIX hosts: the user name must be a valid user name in the `passwd` file on the host that is specified in the login 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 login to a UNIX host, the user name is recognized on the host where the login is requested, but the supplied password is incorrect.

For login 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:

- 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:

1. On UNIX: 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.
2. 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: Once 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 attempted between the NetBackup-Java interface and the user service on host (*host*) on the port number that was specified in the error message.

Refer to the various port configuration options that are described in the *NetBackup Administrator's Guide, Volume I.*

The NetBackup Administration Console log file should contain more detail about this error.

- On UNIX: 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:

1 Restart the NetBackup-Java interface and log in again.

2 If the problem persists, enable detailed debug logging.

3 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:

1 Retry the last operation.

2 If the problem persists, restart the NetBackup-Java interface and try again.

3 If the problem still persists, enable detailed debug logging.
See "Enabling detailed debug logging" on page 119.

4 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 attempts to write to a file that does not have write permissions. The solution is to enable write privileges.
- The NetBackup-Java user service attempts 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 "Enabling detailed debug logging" on page 119.

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. Once 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:

1 If the problem persists, restart the NetBackup-Java interface and try again.

2 If the problem still persists, enable detailed debug logging as explained in “Enabling detailed debug logging” on page 119.

3 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 is enabled, you the details can be retrieved 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 attempt to create a file that already exists.

Recommended action: Remove the file, which can be identified in the user service log files.

Refer to “Troubleshooting the Administration Console for UNIX” on page 117.

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:

1 If the problem persists, restart the NetBackup-Java interface and try again.

2 If the problem still persists, enable detailed debug logging as explained in “Enabling detailed debug logging” on page 119.

3 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 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:

1. If the problem persists, restart the NetBackup-Java interface and try again.
2. If the problem still persists, enable detailed debug logging as explained in "Enabling detailed debug logging" on page 119.
3. 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 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:

- Log in to a different NetBackup remote host.
- Upgrade the NetBackup software on either of the following: the machine that is specified in the login 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 login to a different NetBackup host or exit the application. The remote NetBackup host will have 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:

- Log in to a different NetBackup remote host.
- Upgrade the NetBackup software on either of the following: the specified machine in the login 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 locale configuration (or Windows regional settings) defined on the host that was specified in the NB-Java login dialog box. At login, 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 *`install_path`*`\msg\lc.conf` on Windows. When the locale is validated, initialization of the locale in the user service's environment is attempted (by means of `setlocale`).

Recommended action: On the specified host in the NB-Java login 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 login 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 prior to this, retry your last operation. Check the log file for more details.

Explanation: Once the NB-Java authentication service validates the username on the login dialog box for access, all Administration console service requests use an NB-Java user service. Communication between the Administration console and user service is attempted 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:

1 On UNIX: 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.

2. 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:

1. Restart the NetBackup-Java interface and try again.
2. 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) 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) 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) 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:

1. If the problem persists, restart the NetBackup-Java interface and try again.
2. If the problem still persists, enable detailed debug logging as explained in "Enabling detailed debug logging" on page 119.
3. 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: Can not 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 username that is provided in the login dialog box. Communication between the NetBackup Administration Console and the authentication service is attempted 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:

1. On UNIX: 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.
2. Ensure that no other application uses the port that is configured for VNETD.

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.

For a complete list of required logs and configuration information, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

NetBackup status code: 604

Message: no target storage unit specified for the new job

Explanation: A mismatch occurred between storage units 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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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), 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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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:

- 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.
- For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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 `bppllist` command configuration.
- Check the logs for nbjm, which uses unified logging (OID 117).

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

Recommend action: Contact customer support and send appropriate logs.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

NetBackup status code: 643

Message: unexpected message received from `bpcoord`

Explanation: This error code is no longer used.

Recommended action: Submit a problem report along with appropriate logs.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

NetBackup status code: 645

Message: unable to start the writer on the media server

Explanation: The bpsynth process was unable to start the following: the bptm or the 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 bpsynth logged. For more information, refer to the following: the debug logs for bpsynth on the master server and 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 to run the bptm or the 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:

```
<install_path>/netbackup/bin/bptm -count -rn 0 -rt 8
```

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 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 bpdm binary by running the following command:

```
<install_path>/netbackup/bin/bpdm
```

It should print the following: "bpdm: media manager operation not specified". Retry the synthetic backup job. If the problem persists, contact customer support and send appropriate logs.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

NetBackup status code: 646

Message: unable to get the address of the local listen socket

Explanation: The bpsynth process cannot obtain the address of the opened listen socket. The bpsynth process needs the address to receive incoming connections from the bptm or the 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 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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

NetBackup status code: 647

Message: validation of synthetic image failed

Explanation: This error is returned when 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: bpsynth and bptm or 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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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 the 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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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) 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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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) 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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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 under "Logs to accompany problem reports for synthetic backup" on page 107, and rerun the job. Then send the logs to customer support.

See "Submitting unified logging files to Symantec support" on page 95 regarding unified logs.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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.

For a complete list of logs and configuration information to provide, refer to "Logs to accompany problem reports for synthetic backup" on page 107.

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 attempted 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. You can generate the report by means of either bperror or the 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) 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) 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) 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) 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) 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) 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 or *`install_path`*`\NetBackup\bin\bpdown` 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) 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) 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) 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), nbrb (118), and PBX (103). All unified logging is written to `/usr/openv/logs` (UNIX) 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) 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) 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 (nbrb) 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: 811

Message: failed to communicate with resource requester

Explanation: Job manager (nbjm) attempts to notify a process (usually bptm) of the status of a resource it requested. That notification fails because of a communication problem.

Recommended action:

1. Verify connectivity between the master and the media server.
2. Verify Private Branch Exchange (PBX) configuration and permissions. For information on PBX, see "Resolving PBX problems" on page 65.

NetBackup status code: 812

Message: failed to communicate with resource broker

Explanation: Job manager (nbjm) attempts to make a request to the resource broker (nbrb). The request fails because of a communication problem.

Recommended action:

1. Verify connectivity between the master sever and the EMM server.
2. Verify Private Branch Exchange (PBX) configuration and permissions. For information on PBX, see "Resolving PBX problems" on page 65.

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: 823

Message: no BRMComm to join

Explanation: The job was unable to join the multiplex group. This is an internal error.

Recommended action: 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) or *`install_path`*`\NetBackup\logs` (Windows).
- The following 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) 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) or *`install_path`*`\NetBackup\db\jobs\trylogs` (Windows).
- bpdbjobs output: run bpdbjobs to obtain the state and status of all jobs.

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:

1. 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) or *`install_path`*`\NetBackup\logs` (Windows).
2. 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:

1. 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) or *install_path*`\NetBackup\logs` (Windows).
2. 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:

1. 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) or *install_path*`\NetBackup\logs` (Windows).
2. 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:

1. 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) or *install_path*`\NetBackup\logs` (Windows).
2. 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) 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:

1. Configure the backup schedule with a storage unit or storage unit groups that can be run on the same media server.
2. 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) 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:

- 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) 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 cancelled.

Recommended action:

- 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) 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:

- 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) 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:

1. 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) or *`install_path`*`\NetBackup\logs` (Windows).
2. 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 happens when the NetBackup Resource Broker (nbrb) receives an allocation request for a read media that was never reserved. This situation could result from an internal error in bpduplicate, nbjm, or nbrb.

Recommended action:

1. 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) or to `*install_path*\NetBackup\logs` (Windows).

2 If necessary, set global logging to a higher level: **Host Properties > Master Server > Properties > Logging**. Retry the operation and examine the nbrb logs.

Messages

This section lists the NetBackup error messages alphabetically. The status code is included in parentheses after the message. Refer to the previous list of status codes for explanations and recommended actions.

/usr/openv/netbackup/bp.conf not found

(NetBackup status code 110)

a protocol error has occurred

(NetBackup status code 232)

access to server backup restore manager denied

(NetBackup status code 206)

access to the client was not allowed

(NetBackup status code 59)

afs/dfs command failed

(NetBackup status code 78)

all configured vault steps failed

(NetBackup status code 351)

all volumes are not available to eject

(NetBackup status code 297)

allocation failed

(NetBackup status code 10)

an entry in the filelist expanded to too many characters

(NetBackup status code 70)

an exception condition occurred

(NetBackup status code 600)

an extension package is needed but was not installed

(NetBackup status code 9)

an invalid entry was encountered

(NetBackup status code 223)

another NB database backup is already in progress

(NetBackup status code 125)

archive file removal failed

(NetBackup status code 4)

a session is already running for this vault

(NetBackup status code 275)

a synthetic backup request for media resources failed

(NetBackup status code 660)

authentication failed

(NetBackup status code 160)

Backup Exec operation failed

(NetBackup status code 151)

backup restore manager failed to read the file list

(NetBackup status code 53)

backups are not allowed to span media

(NetBackup status code 166)

bpcoord startup validation failure

(NetBackup status code 669)

bpjava-msvc: the client is not compatible with this server version (*server_version*)

(NetBackup status code 513)

bpstart_notify failed

(NetBackup status code 73)

cannot connect on socket

(NetBackup status code 25)

cannot connect to nbvault server

(NetBackup status code 282)

cannot connect to read media server

(NetBackup status code 613)

cannot connect to server backup restore manager

(NetBackup status code 205)

Can not connect to the NB-Java authentication service on the configured port - *configured_port_number*. Check the log file for more details.

(NetBackup status code 505)

Can not connect to the NB-Java authentication service via VNETD on (*host*) on port (*vnetd_configured_port_number*). Check the log file for more details.

(NetBackup status code 525)

Can not connect to the NB-Java user service on port *port_number*. Check the log file for more details.

(NetBackup status code 506)

Can not connect to the NB-Java user service via VNETD on (host) or port (configured_port_number)

(NetBackup status code 517)

cannot consolidate reports of sessions from container and slot-based vaults

(NetBackup status code 289)

Can not execute program

(NetBackup status code 509)

cannot find configuration database record for requested NB database backup

(NetBackup status code 120)

cannot find requested volume pool in EMM database

(NetBackup status code 167)

cannot find robot in vault configuration file

(NetBackup status code 323)

cannot find robot, vault, or profile in the vault configuration

(NetBackup status code 266)

cannot find the local host name

(NetBackup status code 267)

cannot find vault in vault configuration file

(NetBackup status code 322)

cannot get a bound socket

(NetBackup status code 146)

cannot make required directory

(NetBackup status code 35)

cannot modify - stale view

(NetBackup status code 342)

cannot overwrite media, data on it is protected

(NetBackup status code 168)

cannot perform specified media import operation

(NetBackup status code 176)

cannot position to correct image

(NetBackup status code 94)

cannot read backup header, media may be corrupted

(NetBackup status code 173)

cannot read media header, may not be NetBackup media or is corrupted

(NetBackup status code 172)

\cannot register handler for accepting new connections

(NetBackup status code 603)

cannot send extents to bpsynth

(NetBackup status code 612)

cannot set non blocking mode on the listen socket

(NetBackup status code 602)

cannot start reader on the media server

(NetBackup status code 614)

Can not write file

(NetBackup status code 508)

can’t connect to client

(NetBackup status code 58)

child process killed by signal

(NetBackup status code 27)

client backup failed to read the file list

(NetBackup status code 67)

client backup failed to receive the CONTINUE BACKUP message

(NetBackup status code 66)

client backup was not attempted

(NetBackup status code 195)

client backup was not attempted because backup window closed

(NetBackup status code 196)

client cannot read the mount table

(NetBackup status code 60)

client connection refused

(NetBackup status code 57)

client did not start

(NetBackup status code 49)

client hostname could not be found

(NetBackup status code 48)

client is not validated to perform the requested operation

(NetBackup status code 135)

client is not validated to use the server

(NetBackup status code 131)

client name mismatch
(NetBackup status code 39)

client process aborted
(NetBackup status code 50)

client timed out reading file
(NetBackup status code 76)

client timed out waiting for bpend_notify to complete
(NetBackup status code 75)

client timed out waiting for bpstart_notify to complete
(NetBackup status code 74)

client timed out waiting for the continue message from the media manager
(NetBackup status code 65)

client timed out waiting for the file list
(NetBackup status code 68)

client’s network is unreachable
(NetBackup status code 56)

client/server handshaking failed
(NetBackup status code 26)

communication interrupted
(NetBackup status code 234)

connection refused by server backup restore manager
(NetBackup status code 204)

connection to the peer process does not exist
(NetBackup status code 622)

container cannot hold any media from the specified robot
(NetBackup status code 321)

container database close operation failed
(NetBackup status code 317)

container database lock operation failed

(NetBackup status code 318)

container database open operation failed

(NetBackup status code 319)

container database truncate operation failed

(NetBackup status code 314)

container does not exist in container database

(NetBackup status code 313)

container_id is not unique in container database

(NetBackup status code 316)

continue

(NetBackup status code 221)

could not deassign media due to Media Manager error

(NetBackup status code 177)

could not get group information

(NetBackup status code 38)

could not get passwd information

(NetBackup status code 30)

could not set group id for process

(NetBackup status code 32)

could not set user id for process

(NetBackup status code 31)

daemon fork failed

(NetBackup status code 148)

daemon is already running

(NetBackup status code 145)

data marshalling error

(NetBackup status code 625)

data un-marshalling error

(NetBackup status code 626)

database system error

(NetBackup status code 220)

density is incorrect for the media id

(NetBackup status code 179)

disk is full

(NetBackup status code 155)

Disk storage unit is full

(NetBackup status code 129)

done

(NetBackup status code 222)

duplicate backup images were found

(NetBackup status code 642)

duplicate MAP

(NetBackup status code 346)

duplicate reference string specified

(NetBackup status code 813)

EC_badop

(NetBackup status code 113)

(there is no explanation for status code 113)

EC_end

(NetBackup status code 115)

(there is no explanation for status code 115)

EC_error

(NetBackup status code 114)

(there is no explanation for status code 114)

eject process could not obtain information about the robot

(NetBackup status code 295)

eject process failed to start

(NetBackup status code 292)

eject process has already been run for the requested vault session

(NetBackup status code 307)

eject process has been aborted

(NetBackup status code 293)

eject process is complete

(NetBackup status code 279)

end point terminated with an error

(NetBackup status code 610)

error creating or getting message queue

(NetBackup status code 209)

error encountered attempting backup of catalog (multiple tape catalog backup)

(NetBackup status code 302)

error encountered executing Media Manager command

(NetBackup status code 303)

error getting information from EMM database

(NetBackup status code 332)

error getting information from media manager command line

(NetBackup status code 333)

error obtaining date of last backup for client

(NetBackup status code 207)

error occurred during initialization, check configuration file

(NetBackup status code 103)

error(s) occurred during vault report distribution

(NetBackup status code 284)

error receiving information on message queue

(NetBackup status code 210)

error requesting media (tpreq)

(NetBackup status code 98)

error sending information on message queue

(NetBackup status code 212)

error(s) occurred during vault report generation

(NetBackup status code 283)

Evaluation software has expired. See www.veritas.com for ordering information

(NetBackup status code 161)

events out of sequence - image inconsistency

(NetBackup status code 229)

execution of a command in a forked process failed

(NetBackup status code 623)

execution of a vault notify script failed

(NetBackup status code 272)

execution of the specified system command returned a nonzero status

(NetBackup status code 77)

extent directive contained an unknown media id

(NetBackup status code 644)

failed accessing daemon lock file

(NetBackup status code 158)

failed appending to container database

(NetBackup status code 315)

failed closing mail pipe

(NetBackup status code 102)

failed opening mail pipe

(NetBackup status code 101)

failed reading policy database information

(NetBackup status code 218)

failed reading global config database information

(NetBackup status code 215)

failed reading retention database information

(NetBackup status code 216)

failed reading storage unit database information

(NetBackup status code 217)

failed to communicate with resource broker

(NetBackup status code 812)

failed to communicate with resource requester

(NetBackup status code 811)

failed to get job data

(NetBackup status code 257)

failed to send signal

(NetBackup status code 260)

failed trying to allocate memory

(NetBackup status code 36)

failed trying to exec a command

(NetBackup status code 29)

failed trying to fork a process

(NetBackup status code 28)

failed waiting for child process

(NetBackup status code 34)

failed while trying to send mail

(NetBackup status code 33)

failure occurred while suspending media for eject

(NetBackup status code 335)

failure occurred while updating session information

(NetBackup status code 336)

failure occurred while updating the eject.mstr file

(NetBackup status code 337)

fatal NB media database error

(NetBackup status code 91)

File already exists: *file_name*

(NetBackup status code 510)

file close failed

(NetBackup status code 15)

file does not exist

(NetBackup status code 142)

file open failed

(NetBackup status code 12)

file path specified is not absolute

(NetBackup status code 141)

file pathname exceeds the maximum length allowed

(NetBackup status code 105)

file read failed

(NetBackup status code 13)

file write failed

(NetBackup status code 14)

found no images or media matching the selection criteria

(NetBackup status code 190)

getservbyname failed

(NetBackup status code 19)

handshaking failed with server backup restore manager

(NetBackup status code 201)

host is unreachable

(NetBackup status code 47)

image does not have a fragment map

(NetBackup status code 663)

inadequate buffer space

(NetBackup status code 235)

incorrect catalog backup policy

(NetBackup status code 349)

Incorrect password

(NetBackup status code 504)

Incorrect server platform identifier

(NetBackup status code 162)

incorrect vault catalog backup schedule

(NetBackup status code 350)

insufficient data received

(NetBackup status code 628)

internal error 615

(NetBackup status code 615)

internal error 616

(NetBackup status code 616)

internal error 618

(NetBackup status code 618)

internal error 619

(NetBackup status code 619)

internal error 620

(NetBackup status code 620)

internal error 654

(NetBackup status code 654)

Internal error - a bad status packet was returned by NB-Java application server that did not contain an exit status code

(NetBackup status code 512)

invalid arguments specified
(NetBackup status code 638)

invalid command parameter
(NetBackup status code 20)

invalid command protocol
(NetBackup status code 143)

invalid command usage
(NetBackup status code 144)

invalid container database entry
(NetBackup status code 312)

invalid container description
(NetBackup status code 331)

invalid container id
(NetBackup status code 328)

invalid database host
(NetBackup status code 330)

invalid data found in retention map file for duplication
(NetBackup status code 324)

invalid date specified
(NetBackup status code 109)

invalid date specified
(NetBackup status code 109)

invalid file pathname
(NetBackup status code 104)

invalid file pathname found, cannot process request
(NetBackup status code 106)

invalid filelist specification
(NetBackup status code 69)

invalid job id

(NetBackup status codes 273 and 805)

invalid media type specified in the storage unit

(NetBackup status code 640)

Invalid NBJAVA_CLIENT_PORT_WINDOW configuration option value: (*option_value*)

(NetBackup status code 519)

invalid recall status

(NetBackup status code 329)

invalid request

(NetBackup status code 133)

Invalid username

(NetBackup status code 503)

Invalid value for NB-Java configuration option (*option_name*): (*option_value*)

(NetBackup status code 520)

Iron Mountain report is already created for this session

(NetBackup status code 311)

JM internal error

(NetBackup status code 801)

JM internal protocol error

(NetBackup status code 802)

JM terminating

(NetBackup status code 803)

licensed use has been exceeded

(NetBackup status code 159)

logic error encountered

(NetBackup status code 256)

master server request failed

(NetBackup status code 149)

media block size changed prior to resume

(NetBackup status code 163)

media close error

(NetBackup status code 87)

media id is either expired or will exceed maximum mounts

(NetBackup status code 169)

media id is not in NetBackup volume pool

(NetBackup status code 178)

media id must be 6 or less characters

(NetBackup status code 171)

media id is not assigned to this host in the EMM database

(NetBackup status code 95)

Media Manager device daemon (ltid) is not active

(NetBackup status code 80)

Media Manager volume daemon (vmd) is not active

(NetBackup status code 81)

media manager detected image that was not in tar format

(NetBackup status code 92)

media manager found wrong tape in drive

(NetBackup status code 93)

media manager killed by signal

(NetBackup status code 82)

media manager received no data for backup image

(NetBackup status code 90)

media manager - system error occurred

(NetBackup status code 174)

media open error

(NetBackup status code 83)

media position error

(NetBackup status code 86)

media read error

(NetBackup status code 85)

media write error

(NetBackup status code 84)

Member already exists in server group

(NetBackup status code 409)

Member’s NetBackup version not compatible with Server Group

(NetBackup status code 407)

Member's server type not compatible with Server Group

(NetBackup status code 405)

multiple profiles exist

(NetBackup status code 305)

NB database backup failed, a path was not found or is inaccessible

(NetBackup status code 124)

NB database backup header is too large, too many paths specified

(NetBackup status code 126)

NB database recovery failed, a process has encountered an exceptional condition

(NetBackup status code 128)

NB image database contains no image fragments for requested backup id/copy number

(NetBackup status code 165)

NB-Java application server interface error: *Java exception*

(NetBackup status code 511)

NB-Java application server protocol error

(NetBackup status code 523)

NB-Java: bpjava-msvc is not compatible with this application version (*application_version*). You may try login to a different NetBackup host or exit the application. The remote NetBackup host will have to be configured with the same version of NetBackup as the host you started the application on.

(NetBackup status code 514)

NB-Java Configuration file (*file_name*) does not exist

(NetBackup status code 521)

NB-Java Configuration file (*file_name*) is not readable due to the following error: (*message*)

(NetBackup status code 522)

NDMP backup failure

(NetBackup status code 99)

network connection broken

(NetBackup status code 40)

network connection timed out

(NetBackup status code 41)

network read failed

(NetBackup status code 42)

network write failed

(NetBackup status code 44)

no active policies contain schedules of the requested type for this client

(NetBackup status code 198)

no active policies in the configuration database are of the correct client type

(NetBackup status code 246)

No authorization entry exists in the auth.conf file for username *username*. None of the NB-Java applications are available to you.

(NetBackup status code 502)

no BRMComm to join

(NetBackup status code 823)

no connection to reader

(NetBackup status code 611)

no drives available to start the reader process

(NetBackup status code 617)

no drives available to start the writer process

(NetBackup status code 634)

no entity was found

(NetBackup status code 227)

no files specified in the file list

(NetBackup status code 112)

no images duplicated

(NetBackup status code 308)

no images were found to synthesize

(NetBackup status code 607)

no images were successfully processed

(NetBackup status code 191)

no media ejected for the specified vault session

(NetBackup status code 327)

no media is defined for the requested NB database backup

(NetBackup status code 121)

no message was received from bptm

(NetBackup status code 629)

No ports available in range (*port_number*) through (*port_number*) per the NBJAVA_CLIENT_PORT_WINDOW configuration option

(NetBackup status code 518)

no profile was specified

(NetBackup status code 274)

no robot on which the media can be read

(NetBackup status code 606)

no schedules of the correct type exist in this policy

(NetBackup status code 240)

no storage units available for use

(NetBackup status code 213)

no target storage unit specified for the new job

(NetBackup status code 604)

no target storage unit was specified via command line

(NetBackup status code 655)

no vault session id was found

(NetBackup status code 269)

none of the files in the file list exist

(NetBackup status code 71)

none of the requested files were backed up

(NetBackup status code 2)

not all requested files were restored

(NetBackup status code 175)

number of media has exceeded the capacity of MAP

(NetBackup status code 291)

one or more errors detected during consolidated eject processing

(NetBackup status code 290)

operation not allowed during this time period

(NetBackup status code 199)

operation requested by an invalid server

(NetBackup status code 37)

operation would cause an illegal duplication

(NetBackup status code 242)

permission denied by client during rcmd
(NetBackup status code 55)

pipe close failed
(NetBackup status code 18)

pipe fgets call from bpcoord failed
(NetBackup status code 668)

premature eof encountered
(NetBackup status code 233)

problems encountered during setup of shared memory
(NetBackup status code 89)

process called but nothing to do
(NetBackup status code 296)

process was killed by a signal
(NetBackup status code 63)

profile already exists
(NetBackup status code 345)

query for list of component images failed
(NetBackup status code 671)

RB communication error
(NetBackup status code 903)

RB disk volume mount failed
(NetBackup status code 912)

RB internal error
(NetBackup status code 901)

RB invalid argument
(NetBackup status code 902)

RB max reallocation tries exceeded
(NetBackup status code 904)

RB media reservation not found

(NetBackup status code 914)

RB media server mismatch

(NetBackup status code 905)

RB operator denied mount request

(NetBackup status code 906)

RB user cancelled resource request

(NetBackup status code 907)

RB was reset

(NetBackup status code 908)

read from input socket failed

(NetBackup status code 636)

reader failed

(NetBackup status code 609)

received an error from bptm request to suspend media

(NetBackup status code 631)

received an error from bptm request to un-suspend media

(NetBackup status code 632)

received error notification for the job

(NetBackup status code 605)

report requested without eject being run

(NetBackup status code 309)

request attempted on a non reserved port

(NetBackup status code 45)

requested media id is in use, cannot process request

(NetBackup status code 97)

required or specified copy was not found

(NetBackup status code 147)

required value not set

(NetBackup status code 152)

resource request failed

(NetBackup status code 800)

retry nbrb request later

(NetBackup status code 900)

robot already exists

(NetBackup status code 343)

schedule windows overlap

(NetBackup status code 231)

scheduler found no backups due to run

(NetBackup status code 200)

send buffer is full

(NetBackup status code 670)

server backup restore manager’s network is unreachable

(NetBackup status code 203)

Server Group Active State is not valid

(NetBackup status code 403)

Server Group Already Exists

(NetBackup status code 401)

Server Group Already Exists with a different type

(NetBackup status code 402)

Server Group does not exist

(NetBackup status code 404)

Server Group is in use

(NetBackup status code 408)

Server Group Type is Invalid

(NetBackup status code 400)

server is not the master server
(NetBackup status code 153)

server name not found in the bp.conf file
(NetBackup status code 254)

server not allowed access
(NetBackup status code 46)

SERVER was not specified in /usr/openv/netbackup/bp.conf
(NetBackup status code 111)

Session id assignment failed
(NetBackup status code 263)

Session id file is empty or corrupt
(NetBackup status code 265)

Snapshot error encountered
(NetBackup status code 156)

socket close failed
(NetBackup status code 22)

Socket connection to the NB-Java user service has been broken. Please retry your last operation. Check the log file for more details.
(NetBackup status code 507)

socket open failed
(NetBackup status code 21)

socket read failed
(NetBackup status code 23)

socket write failed
(NetBackup status code 24)

specified device path does not exist
(NetBackup status code 122)

specified disk path is not a directory
(NetBackup status code 123)

specified file contains no valid entry

(NetBackup status code 326)

specified media or path does not contain a valid NB database backup header

(NetBackup status code 127)

specified policy does not exist

(NetBackup status code 639)

specified profile not found

(NetBackup status code 304)

specified report does not exist

(NetBackup status code 348)

specified schedule was not found

(NetBackup status code 640)

storage unit characteristics mismatched to request

(NetBackup status code 154)

storage unit query failed

(NetBackup status code 608)

suspend requested by administrator

(NetBackup status code 157)

system call failed

(NetBackup status code 11)

system error occurred

(NetBackup status code 130)

system error occurred while processing user command

(NetBackup status code 100)

tar did not find all the files to be restored

(NetBackup status code 185)

tar had an unexpected error

(NetBackup status code 184)

tar received an invalid archive
(NetBackup status code 183)

tar received an invalid argument
(NetBackup status code 181)

tar received an invalid file name
(NetBackup status code 182)

tar received no data
(NetBackup status code 186)

tar was successful
(NetBackup status code 180)

termination requested by administrator
(NetBackup status code 150)

termination requested by bpcoord
(NetBackup status code 665)

text exceeded allowed length
(NetBackup status code 225)

the archive failed to back up the requested files
(NetBackup status code 7)

the backup failed to back up the requested files
(NetBackup status code 6)

the catalog image .f file has been archived
(NetBackup status code 253)

the client is not in the configuration
(NetBackup status code 243)

the client type is incorrect in the configuration database
(NetBackup status code 72)

the database contains conflicting or erroneous entries
(NetBackup status code 238)

the entity already exists
(NetBackup status code 226)

the file list is incomplete
(NetBackup status code 249)

An extended error status has been encountered, check detailed status
(NetBackup status code 252)

the image was not created with TIR information
(NetBackup status code 250)

the library is not ready to eject volumes
(NetBackup status code 298)

The machine specified is not a member of the server group specified
(NetBackup status code 406)

the maximum number of jobs per client is set to 0
(NetBackup status code 194)

the requested operation was partially successful
(NetBackup status code 1)

the requested operation was successfully completed
(NetBackup status code 0)

the required storage unit is unavailable
(NetBackup status code 219)

the restore failed to recover the requested files
(NetBackup status code 5)

the server is not allowed to write to the client's filesystems
(NetBackup status code 189)

the specified container is not empty
(NetBackup status code 320)

the specified policy does not exist in the configuration database
(NetBackup status code 230)

the specified policy is not active

(NetBackup status code 247)

the specified policy is not of the correct client type

(NetBackup status code 245)

the specified client does not exist in an active policy within the configuration database

(NetBackup status code 236)

the specified client does not exist in the specified policy

(NetBackup status code 239)

the specified schedule does not exist in an active policy in the configuration database

(NetBackup status code 237)

the specified schedule does not exist in the specified policy

(NetBackup status code 197)

the specified schedule is the wrong type for this request

(NetBackup status code 241)

the TIR information is zero length

(NetBackup status code 251)

the vault session directory is either missing or inaccessible

(NetBackup status code 268)

there are no active policies in the configuration database

(NetBackup status code 248)

there are no volumes to eject

(NetBackup status code 280)

there is no available MAP for ejecting

(NetBackup status code 299)

there was a conflicting specification

(NetBackup status code 224)

third-party copy backup failure

(NetBackup status code 170)

this mpx group is unjoinable

(NetBackup status code 806)

timed out connecting to client

(NetBackup status code 54)

timed out connecting to server backup restore manager

(NetBackup status code 202)

timed out waiting for database information

(NetBackup status code 51)

timed out waiting for media manager to mount volume

(NetBackup status code 52)

timed out waiting for the client backup to start

(NetBackup status code 64)

tir info was pruned from the image file

(NetBackup status code 136)

unable to accept connection from the reader

(NetBackup status code 657)

unable to accept connection from the writer

(NetBackup status code 658)

unable to allocate new media for backup, storage unit has none available

(NetBackup status code 96)

unable to collect pre eject information from the API

(NetBackup status code 278)

unable to connect to bpcoord

(NetBackup status code 621)

unable to determine the status of rbak

(NetBackup status code 8)

unable to find policy/schedule for image using retention mapping

(NetBackup status code 325)

unable to get the address of the local listen socket

(NetBackup status code 646)

unable to issue the database query for policy

(NetBackup status code 651)

unable to issue the database query for policy information

(NetBackup status code 652)

unable to listen and register service via vnetd

(NetBackup status code 633)

unable to locate vault directory

(NetBackup status code 285)

unable to mount media because its in a DOWN drive or misplaced

(NetBackup status code 164)

unable to obtain process id, getpid failed

(NetBackup status code 270)

unable to open listen socket

(NetBackup status code 601)

unable to open pipe between bpsynth and bpcoord

(NetBackup status code 667)

unable to process request

(NetBackup status code 228)

unable to process request because the server resources are busy

(NetBackup status code 134)

unable to receive response from robot; robot not ready

(NetBackup status code 334)

unable to register handle with the reactor

(NetBackup status code 635)

unable to send a message to bpcoord

(NetBackup status code 653)

unable to send a message to the writer child process

(NetBackup status code 659)

unable to send a start command to a reader/writer process on media server

(NetBackup status code 624)

unable to send exit message to the BPXM reader

(NetBackup status code 661)

unable to send extent message to bpcoord

(NetBackup status code 650)

unable to send extent message to BPXM

(NetBackup status code 648)

unable to send start synth message to bpcoord

(NetBackup status code 656)

unable to start the writer on the media server

(NetBackup status code 645)

unexpected message received

(NetBackup status code 43)

unexpected message received from bpcoord

(NetBackup status code 643)

unexpected message received from bpsynth

(NetBackup status code 627)

unexpected message received from BPXM

(NetBackup status code 649)

unexpected message was received from bptm

(NetBackup status code 630)

unimplemented error code

(NetBackup status code 114)

unimplemented feature

(NetBackup status code 16)

unknown image referenced in the SYNTH CONTEXT message from BPXM

(NetBackup status code 662)

unsupported image format for the requested database query

(NetBackup status code 79)

Updating of Media Manager database failed

(NetBackup status code 310)

user id was not superuser

(NetBackup status code 140)

user is not validated to use the server

(NetBackup status code 132)

valid archive image produced, but no files deleted due to non-fatal problems

(NetBackup status code 3)

validation of synthetic image failed

(NetBackup status code 647)

vault already exists

(NetBackup status code 344)

vault catalog backup failed

(NetBackup status code 294)

vault configuration cache not initialized

(NetBackup status code 347)

vault configuration file format error

(NetBackup status code 339)

vault configuration file not found

(NetBackup status code 259)

vault configuration serialization failed

(NetBackup status code 341)

vault configuration tag not found

(NetBackup status code 340)

vault core error

(NetBackup status code 281)

vault duplication partially succeeded

(NetBackup status code 306)

Vault duplication was aborted by administrator request

(NetBackup status code 258)

vault eject failed

(NetBackup status code 287)

vault eject partially succeeded

(NetBackup status code 288)

vault eject timed out

(NetBackup status code 338)

vault internal error 261

(NetBackup status code 261)

vault internal error 262

(NetBackup status code 262)

vault internal error 286

(NetBackup status code 286)

vault XML version mismatch

(NetBackup status code 271)

vmchange api_eject command failed

(NetBackup status code 301)

vmchange eject verify not responding

(NetBackup status code 300)

VxSS access denied

(NetBackup status code 117)

VxSS authentication failed

(NetBackup status code 116)

VxSS authorization failed

(NetBackup status code 118)

VxSS authentication is requested but not allowed

(NetBackup status code 193)

VxSS authentication is required but not available

(NetBackup status code 192)

write on output socket failed

(NetBackup status code 637)

You are not authorized to use this application

(NetBackup status code 501)

zero extents in the synthetic image, cannot proceed

(NetBackup status code 664)

Chapter 6

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.

- Media Manager status codes
- Device configuration status codes
- Format optical status codes
- Device management status codes
- Robotic status codes
- Robotic error codes

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.

Note: The Symantec technical support site has a wealth of information that can help you solve NetBackup problems. Visit http://entsupport.symantec.com for comprehensive troubleshooting details.

Status codes

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.)

With the 6.0 version of NetBackup, the meaning of certain error codes changed. For any status codes that a 5.x media server issues, consult the corresponding 5.x version of the *Troubleshooting Guide*.

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 `install_path\Volmgr\ (`Windows).
3. Restart the daemons and services or run the command's verbose option, if available.

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.

Recommended action:

1. Check for other error messages in the command or the interface output to determine which system call failed.

See “Using debug logs” on page 358.

2 Check the system application log for error and warning messages.

3 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.
- On the Performance tab, set Virtual Memory to a higher value. (On Windows 2000, select Performance Options from the Advanced tab.)

4 Verify that all product binaries are properly installed.

5 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: must be root user to execute command

Explanation: A user or process that did not have root privileges (on UNIX) 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 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.

Recommended action:

1 Examine command output, debug logs, and system logs for a more detailed message on the error.
See “Using debug logs” on page 358.

2 Check the usage statement for expected usage and compare with the parameters being sent to start the new process.

3 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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. 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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. Ensure that the media ID, where requested, is not blank.
3. 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.

4. If the media is for optical disk, ensure that the media ID of the optical partner is specified and contains only valid characters.
5. If the media ID is for optical disk in a TLM robot, ensure that the format is as follows: “Axxxxxx” for the ID and “Bxxxxx” for the partner.
6. 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.
7. Ensure that the media ID is from 1 to 6 characters in length.
8. Ensure that a valid media and seed were specified.
9. 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.

Recommended action:

1. 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.
2. If using a command line interface directly, verify that a valid media type has been passed, according to `vmadd(1m)` command line documentation.
3. Ensure that an operation valid only for cleaning media has not been requested on a media ID that does not correspond to cleaning tape.
4. 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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 358.

2. Ensure that the bar code, where requested, is not blank.
3. 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.
4. Ensure that the number of characters in the bar code does not exceed the maximum that is allowed for the robot type.
5. 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 358.
- 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.

Recommended action:

- 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

Explanation: A requested operation encountered a case where the robot control host:

- Is not specified
- Is not valid for the given robot type
- Is not in an acceptable format
- Exceeds the allowed length of a robot control host name

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error
  See "Using debug logs" on page 358.
- 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

Explanation: 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

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error
  See "Using debug logs" on page 358.
- Specify a volume group where one is required to ensure that it contains the following:
  - 25 ASCII characters or less
  - No whitespace
  - 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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: 17

Message: invalid robot coord2

Explanation: A requested operation encountered a missing or an invalid robot coordinate 2 (used for the optical platter side). Or a move by volume group residence was attempted when the volume was not previously associated with a valid robot coordinate 2 (optical platter side).

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Specify a robot coordinate 2 value of zero (0) for non-optical media. Or specify either A or B to represent the platter side for optical media.

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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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; 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) 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) 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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) 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) or *`install_path`*`\NetBackup\var\global` folder (Windows):
  - `external_robotics.txt`
  - `external_densities.txt`
  - `external_drivetypes.txt`
  - `external_mediatypes.txt`
- Check the permissions on the nbpushdata working directory: `/usr/openv/tmp` (UNIX) or *`install_path`*`\tmp` (Windows).

Media Manager status code: 27

Message: database read record operation failed

Explanation: `nbpushdata` encountered a read error while reading 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 358.

- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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 358.

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 (or optical partner 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.

Recommended action:

- Examine the daemon and reqlib debug logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine the daemon and reqlib debug logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- 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 358.
- 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.

Recommended action:

- 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 358.

- Query or sort volume records by slot number to identify the volume entry with the duplicate robotic coordinate. (If you use optical disk, display the optical platter side.)
- 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.

Recommended action:

- 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 358.
- 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.

Recommended action:

- 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 358.
- 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.

Recommended action:

- 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 358.
- 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 "Media and device management programs and daemons" on page 640.
  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.

Recommended action:

- Examine command output (if available) and the daemon and reqlib debug logs for a more detailed message error.
  See "Using debug logs" on page 358.
- 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.

See “Media and device management programs and daemons” on page 640.

- 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.
  Perform “Resolving network communication problems” on page 36.

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.

Recommended action:

- 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 358.
- 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 programs and daemons” on page 640.
- 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.
  Perform “Resolving network communication problems” on page 36.

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.

Recommended action:

- 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 358.
- 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.

Recommended action:

- 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 358.

Media Manager status code: 48

Message: no entries deleted

Explanation: A delete volume(s) operation completed. No changes were made to the volume configuration.

Recommended action:

- 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 358.

Media Manager status code: 49

Message: no entries inserted

Explanation: An insert volume(s) operation completed. No volumes were added to the volume configuration.

Recommended action:

- 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 358.

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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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 or NetBackup Volume Manager service on Windows.)

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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 or NetBackup Volume Manager service on Windows.)

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- From catalog backups or another source if available, restore an earlier version of the database file: `/usr/openv/volmgr/database/volDB` (UNIX) 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 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.

Recommended action:

- 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 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 the NetBackup Volume Manager service on Windows.)

Recommended action:

- 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 358.

- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Robot inventory update, with the optical media format specified, must be initiated only on the host where the robotic control and optical 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- 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 358.

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.

Recommended action:

- 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 358.
- 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.

Recommended action:

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 358.
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 the NetBackup Volume Manager service on Windows.)

Recommended action:

- 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 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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 or NetBackup Volume Manager service on Windows; `oprd` is the operator request daemon or process.)

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.

- 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 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.

Recommended action:

- 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 358.
- Verify that the correct host names are defined in the configuration.
- Check the services file. On UNIX, 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) or NetBackup Volume Manager service (Windows).

Recommended action:

- 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 358.
- 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) or NetBackup Volume Manager service (Windows).

Recommended action:

- 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 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 358.

- 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: 77

Message: failed during tpformat

Explanation: When a request was made to format an optical platter, the request failed. Or the administrator terminated it.

- The optical volume format may have failed because a WORM (write-once, read many) platter cannot be reformatted.
- If the platter is already formatted: the format optical operation fails if the overwrite label option was not specified and the format operation is not interactive.
- If the administrator terminates the format operation after learning that the platter is already formatted, the format request returns with this status code.
- The format operation may have failed due to a device or a media problem.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 358.
- For any of the cases that are listed under Explanation, choose a format operation appropriate for the current state of the platter. Then retry the format as needed by using the `tpformat` command.

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.

Recommended action:

- Examine the daemon and reqlib debug logs for a more detailed message on the error.
  See “Using debug logs” on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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

Explanation: `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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.veritas.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 358.

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) 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.

Recommended action:

- 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, run `/usr/openv/volmgr/bin/vmd [-v]`. On Windows, start the NetBackup Volume Manager service in Services of the system Control Panel. (On Windows 2000, Services is in Administrative Tools of the 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 358.
- 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.

Recommended action:

- 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 358.

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, 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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 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) 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:

- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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. Optical volumes cannot be deleted unless both sides of the optical platter are unassigned.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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. For optical media, if no worthwhile data is on either side of the platter, unassign both of the volumes before attempting to delete them.

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. Or for optical media, the volume partner was already assigned.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
    - 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, or the volume partner was in a different volume pool for optical media.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.

- 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.

Recommended action:

- 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 358.
- 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
- Format optical platters
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

1. Examine the daemon debug log for a more detailed message on the system error.
   See "Using debug logs" on page 358.
2. Examine the permissions and available file system space for writing to the database: on UNIX, `/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

Explanation: 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

Recommended action:

- Examine the daemon and reqlib debug logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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. For optical media, the volume partner expiration date has expired.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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. (Or the maximum number that is allowed for the volume partner in the case of optical media.)

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- 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 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Use `vmrule` 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 358.

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.

Recommended action:

- 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 358.

- 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 (except HP-UX):

      ```
      /usr/openv/lib/libvopie.so
      /usr/openv/lib/libvnoauth.so
      ```

      UNIX (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: `/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:

      ```
      /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.

Recommended action:

- Examine the daemon and reqlib debug logs for a more detailed message on the error.
  See “Using debug logs” on page 358.
- 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.

Recommended action:

- 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 358.

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 is a possible scenario:

1. Host A reserves a shared drive.
2. Host A becomes unavailable for some time, unable to communicate with other hosts.
3. 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.

4. Some other host (such as Host A or Host C) reserves the drive.
5. 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 is a possible scenario:

1. Host A reserves a shared drive.
2. Host A becomes unavailable for some time, unable to communicate with other hosts.
3. 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.
4. 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 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

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: 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 358.
- 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) 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.

Recommended action:

- 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.

Recommended action:

- 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 358.

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 358.

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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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 358.

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.)

Recommended action:

- 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 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.)

Recommended action:

- 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 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- 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 <hoostname> -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.

Recommended action:

- 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 358.
- 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 (except HP-UX):
    ```
    /usr/openv/lib/libvopie.so
    /usr/openv/lib/libvnoauth.so
    ```
    UNIX (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: `/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:

```
/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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.

See "Using debug logs" on page 358.

- 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.

Recommended action:

- Ensure that the Veritas Security Services is installed and configured.

  For complete installation instructions please see the *Veritas Security Services Installation Guide.*
- Check that both parties have a valid certificate by examining the listed expiry date from a `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 2003 GMT
  Authentication method: Microsoft Windows
  Operation completed successfully.
  ```
- Shows an expiry date of September 19th, 2003. 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 please consult the *Veritas Security Services Administrator's 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.

  See the *Veritas Security Services Administrator's Guide* for more information on broker hierarchies and how to establish trust relationships between brokers.
- 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.

Recommended 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:

  ```
  17:19:27.653 [904.872] <2> GetAzinfo: Peer Cred Info.
  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.

Recommended action:

- 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 358.
- 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.

Recommended action:

- 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 358.
- 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 358.

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.

See “Using debug logs” on page 358.

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 358.

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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 358.
- Verify that Symantec 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 358.
- 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 `vmoprcmd` 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) or administrator privileges (on Windows) started the process. Or the EMM server name cannot be set.

Recommended action:

- If appropriate, give the user or the process administrator privileges (on Windows) or root privileges (on UNIX) 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

Explanation: The problem concerns one of the following files: `/usr/openv/share/device_mappings.txt` (UNIX) 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 Symantec support website at `www.veritas.com`.

Device configuration status code: 3

Message: Could not get hostname

Explanation: An attempt to look up the host name for this host failed.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.

- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine the daemon debug log and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- 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 358.

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.

Recommended action:

- 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 is 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.

Recommended action:

- 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.

Recommended action:

- 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 Symantec 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.

Recommended action:

- 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 358.
- 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.

Recommended action:

- 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. On UNIX hosts, refer to the appropriate chapter in the *NetBackup Device Configuration Guide*. Always use no-rewind device files for drives that are attached to UNIX 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: 20

Message: Duplicate device path names

Explanation: The same device path name was used for the optical drive character and volume header names.

Recommended action: Refer to the appropriate chapter in the *NetBackup Device Configuration Guide* to determine which optical drive names should be specified.

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.

Recommended action:

- 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: In the *NetBackup Device Configuration Guide*, check the Robot Attributes tables to determine valid media types for a given robot type. 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.

Recommended action:

- 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.

Recommended action:

- 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.

Recommended action:

- 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.

Recommended action:

- Examine the daemon debug log and command or interface output for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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 `www.veritas.com` 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) 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, 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.

Recommended action:

- 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 358.
- 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) 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 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Use the `-add -nh` option on the `tpconfig` command to add the NDMP host.

Device configuration status code: 63

Message: NDMP request failed

Explanation:

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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 358.

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.

Recommended action:

- 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 358.

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 358.

Device configuration status code: 70

Message: Unable to create NDMP session

Explanation: An error occurs while opening an NDMP connection to a NAS filer.

Recommended action:

- Examine debug logs for more information on the error.
  See "Using debug logs" on page 358.
- 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 358.

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 358.

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.

Recommended action:

- Examine debug logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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 358.

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 358.

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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.

- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Verify that adequate memory is available.

Device configuration status code: 80

Message: Multiple drive paths are not supported for optical drives

Explanation: The specified drive type in this operation is optical, which does not support multiple paths.

Recommended action: Check the `tpconfig` usage to ensure that the command is used properly.

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`.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.

See "Using debug logs" on page 358.

- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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

Recommended action:

- Verify that the user has the correct permissions to perform this operation.
- Verify that the VxSS settings are correct, under Host Properties in the NetBackup Administration Console.
  See the *NetBackup Administrator's Guide Volume I* for information on how to use the Veritas Security Subsystem (VxSS)

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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- 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 featured. 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.

Format optical status codes

These status codes appear in exit status and command output for the `tpformat` command, and in system or debug logs. Programs that call `tpformat`, such as media and device management user interfaces and the `vmoprcmd` command also present these codes.

Format optical status code: 0

Message: Success

Explanation: An optical volume format operation was successfully completed.

Recommended action: None.

Format optical status code: 1

Message: tpformat: Invalid usage

Explanation: The format optical disk command `tpformat` was ran with improper options or an incompatibility exists between components or versions of the product.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Check the `tpformat` usage statement and compare with the parameters being sent to start the new process.
- Verify that all Media Manager binaries are at a compatible version level.

Format optical status code: 2

Message: tpformat: Cannot set volume header

Explanation: The format optical disk command `tpformat` encountered a system, device, or media error while trying to write the optical volume header.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Verify integrity of the device and the media, and check the system device files for correctness according to the *NetBackup Device Configuration Guide*. Example problems are as follows:
  - Operating system error where exclusive access to the disk cannot be set.
  - Operating system error while attempting to format the disk.
  - Cannot determine the name of the disk.
  - Operating system was unable to set the geometry.
  - Could not write the volume table of contents.
  - Cannot determine SCSI passthrough path to the device.
  - Cannot read capacity of the optical platter.
  - Cannot seek to write the volume header.
  - Optical volume format is not supported on the targeted platform.

Format optical status code: 3

Message: tpformat: Cannot open

Explanation: The format optical disk command `tpformat` encountered a system, device, or media error while trying to open the optical disk device.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Verify integrity of the device and the media, and check the system device files for correctness according to the *NetBackup Device Configuration Guide*. Use the `tpformat -f` option if the media has not already been formatted into sectors.

Format optical status code: 4

Message: tpformat: Cannot read

Explanation: The format optical disk command `tpformat` encountered a system, device, or media error while trying to read the optical disk.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Verify the integrity of the device and media, and check the system device files for correctness according to the *NetBackup Device Configuration Guide*. Use the `tpformat -f` option if the media has not already been formatted into sectors.

Format optical status code: 5

Message: tpformat: Cannot seek

Explanation: The format optical disk command `tpformat` encountered a system, device, or media error while trying to seek on or determine characteristics of the optical disk.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Verify the integrity of the device and media, and check the system device files for correctness according to the *NetBackup Device Configuration Guide*.

Format optical status code: 6

Message: tpformat: Cannot write

Explanation: The format optical disk command `tpformat` encountered a system, device, or media error while trying to write the optical disk.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Verify the integrity of the device and media, and check the system device files for correctness according to the *NetBackup Device Configuration Guide*. Use the `tpformat -f` option if the media has not already been formatted into sectors.

Format optical status code: 7

Message: tpformat: Existing media ID

Explanation: The format optical disk command `tpformat` cannot format the optical disk because it has already been formatted.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Ensure that the device files and optical drive library address are correct. This error can occur if the device paths or drive address was incorrectly configured. Use the `tpformat -o` (overwrite) option if you want to reformat the optical platter. If the platter is WORM (write-once, read-many), it cannot be reformatted.

Format optical status code: 8

Message: tpformat: Must be root

Explanation: A non-root user ran the format optical disk command `tpformat`.

Recommended action: Run `tpformat` only as the root user.

Format optical status code: 9

Message: tpformat: Tape request failed

Explanation: The format optical disk command `tpformat` encountered a situation where the optical volume cannot be mounted.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Verify the integrity of the device and media, and check the system device files for correctness according to the *NetBackup Device Configuration Guide*. Investigate robotic errors and determine if the administrator cancels mount requests.

Format optical status code: 10

Message: tpformat: Invalid robot

Explanation: The format optical disk command `tpformat` cannot find a valid, specified robot in the device configuration.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Check the device configuration to see if a robot of type TLM (Tape Library Multimedia) or ODL (Optical Disk Library) is configured. Check that it matches the robot number that is passed on the `tpformat -r` option.

Format optical status code: 11

Message: tpformat: Command interrupted

Explanation: The format optical disk command `tpformat` was interrupted because the optical mount request was canceled or not accomplished within the required time interval.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Submit the request again and observe the Device Monitor for stand-alone optical mount requests. Service them as needed. Look for pending requests indicating reasons for the optical mount not being completed.

Format optical status code: 12

Message: tpformat: Skip

Explanation: The remaining optical format operations are skipped because an optical disk format operation failed.

Recommended action: Look in the user interface output for the cause of the initial optical disk format failure. Based on the provided error, resolve the situation. Use the `tpformat` command interface to format any remaining optical disks.

Format optical status code: 13

Message: tpformat: No media present in drive or robot slot

Explanation: The format optical disk command `tpformat` was interrupted. No media is present in the drive or robotic slot.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Submit the request again and observe the Device Monitor for stand-alone optical mount requests. Service them as needed and look for pending requests indicating reasons for the optical mount not being satisfied.

Format optical status code: 14

Message: tpformat: EMM error

Explanation: tpformat had a problem when it tried to communicate with EMM.

Recommended action:

- Make sure nbemm is running and that it responds to requests.
- Examine command output, debug logs, and system logs for a more detailed message on the error. See "Using debug logs" on page 358.

Format optical status code: 15

Message: tpformat: Can not retrieve Job ID from Job Manager

Explanation: The format optical disk command tpformat encountered an error while trying to get a job ID from the NetBackup Job Manager (nbjm).

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Verify that the NetBackup Job Manager is running on the master server.

Format optical status code: 16

Message: tpformat: Job Manager returned error: see activity monitor

Explanation: The format optical disk command tpformat encountered an error while communicating with the NetBackup Job Manager (nbjm). The details of this issue may be found in the Activity Monitor entry for this job.

Recommended action:

Examine command output, debug logs, and system logs for a more detailed message on the error.

See "Using debug logs" on page 358.

Format optical status code: 17

Message: tpformat: Request terminated because of volume pool mismatch

Explanation: The format optical disk command tpformat encountered an error while requesting media. The requested pool did not match the pool in which the media resides.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Verify the media is in the requested pool.

Format optical status code: 18

Message: tpformat: Invalid volume pool specified

Explanation: The format optical disk command tpformat encountered an error while requesting media. The requested pool does not exist.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- Use the NetBackup Administration Console or the vmpool command to verify that the requested pool exists.

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 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- On UNIX 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 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- On UNIX 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 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- On UNIX 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 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- On UNIX 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 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.

See “Using debug logs” on page 358.

- On UNIX 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 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 358.
- On UNIX 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 358.

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 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 or the NetBackup Device Manager service on Windows.)

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- On UNIX 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 or the NetBackup Device Manager service on Windows.)

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- On UNIX 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- 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 or the NetBackup Device Manager service on Windows). Or the `tpclean` command was called, but the user was not root (UNIX) or the administrator (Windows).

Recommended action: If appropriate, give the user or the process administrator privileges on Windows or root privileges on UNIX 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 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, 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 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.

Recommended action:

- If `ltid` is not running, start `ltid` and try the operation again. On UNIX, 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) 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, 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 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) 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.

Recommended action:

- 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: `ltid` made an attempt to obtain a message queue identifier that was used for internal message communications. (`ltid` is the Media Manager device daemon on UNIX 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- On UNIX 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: `ltid` made an attempt to obtain a semaphore that was used for arbitrating access to shared memory. (`ltid` is the Media Manager device daemon on UNIX 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- On UNIX 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: 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 `ltid`. (`ltid` is the Media Manager device daemon on UNIX or the NetBackup Device Manager service on Windows.)

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- On UNIX servers, gather the output of the `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.

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.

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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.) On an optical mount request, the optical disk drive character-device file was not a character-special device.

Recommended action:

- 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, recommended character device files for optical devices, 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. Refer to the appropriate chapter in 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.

Recommended action:

- 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.

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 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.

Recommended action:

- Determine which host serve as the drive's scan host: use `vmoprcmd` output or by checking the Device Monitor in the Administration Console.
- Ensure that `vmd` (the NetBackup Volume Manager daemon on UNIX 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 358.

- 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).

Recommended action:

- 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 `vmoprcmd` 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 358.
- 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 `ltid`, no robots of the expected type were found actively configured. (`ltid` is the Media Manager device daemon on UNIX 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: 54

Message: Block device name for optical disk is not a block device

Explanation: On an optical mount request, the configured optical disk drive block device file was not a block-special device.

Recommended action: Use only the recommended device files for optical devices. Check to ensure that the specified device names exist as the type of special file required.

Refer to the appropriate chapter in the *NetBackup Device Configuration Guide*.

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 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: 57

Message: Cannot assign due to media ID mismatch

Explanation: An attempt was made to assign an optical disk request to a volume that contained a different recorded media ID than was requested.

Recommended action: Refer to the `tpformat` man page to change recorded media IDs on optical platters.

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.

Recommended action:

- 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 358.

Device management status code: 60

Message: No robot daemon or robotics are unavailable

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 358.

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.

Recommended action:

1. Check integrity of the drive, drive path, and media.
2. 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 `tpreq` man page or command description for specifying the media access mode. The `tpreq` command is described in the *NetBackup Administrator's Guide, Volume II*, and in the *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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. Verify that `pbx_exchange` is running.
3. Run the `tpconfig -d` or `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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. Verify that the robotic hardware is functional.

Device management status code: 75

Message: LTI system error

Explanation: A system error occurred.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. A tpclean operation was attempted and Windows networking was not properly configured.
3. 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- 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 Administrator's Guide Volume I* for information on using the Veritas Security Subsystem (VxSS).

Device management status code: 78

Message: Unable to connect to the EMM server

Explanation: An attempt to retrieve or update information in EMM failed.

Recommended action:

- 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 358.

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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- Examine command output, debug logs, and system logs for a more detailed message on the error.
  See "Using debug logs" on page 358.
- 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.

Recommended action:

- 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.

Recommended action:

- 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

Explanation: 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 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.

Recommended action:

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) 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 or the NetBackup Device Manager service on Windows).

Robotic status code: 202

Message: Unable to sense robotic device

Explanation: 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.

Recommended action:

1. Check the configuration of the robot against the recommended configuration as indicated in the documentation for robot configuration.
2. Check the health of the robotic device by using a robot test utility, then close the test utility when finished.

3 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) 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 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.

Recommended action:

1 Stop any robot test utilities, since they have the lock on the robotic device when they are active, and can block other requests.

2 Check whether excessive hardware retries have delayed the completion of a robotic command.

3 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.

Recommended action:

1 Examine command output, debug logs, and system logs for a more detailed message on the error.
See “Using debug logs” on page 358.

2 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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. 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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. 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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. 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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. 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.
3. 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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. 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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. 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.

Recommended action:

1. Stop any robot test utilities, since they have the lock on the robotic device when they are active, and can block other requests.
2. Check to see whether the robotic device still functions.
3. Check whether excessive hardware or communication problems have delayed the completion of a robotic command.
4. 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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. 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 `ltid` was stopped and restarted after changes were last made to the device configuration. `ltid` is the Media Manager device daemon on UNIX 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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See “Using debug logs” on page 358.
2. 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 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.

Recommended action:

1. 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 358.
2. 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.

Recommended action:

1. 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.
2. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.

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.

Recommended action:

1. 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.
2. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.

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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. 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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Media Manager status codes" on page 358.
2. 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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. 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.

Recommended action:

1 Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 358.

2 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.

3 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.

Recommended action:

1 Examine command output, debug logs, and system logs for a more detailed message on the error.
  See “Using debug logs” on page 358.

2 Investigate the system log messages that are related to the error leading to the media mount failure.

3 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.

Recommended action:

1 Examine command output, debug logs, and system logs for a more detailed message on the error.
See "Using debug logs" on page 358.

2 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.

Recommended action:

1 Examine command output, debug logs, and system logs for a more detailed message on the error.
See "Using debug logs" on page 358.

2 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.

Recommended action:

1 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 358.

2 Check the system application log for error and warning messages.

3 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.

4 Verify that all product binaries are properly installed.

5 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.

Recommended action:

1 Examine command output, debug logs, and system logs for a more detailed message on the error.
See “Using debug logs” on page 358.

2 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 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) 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.

Recommended action:

1. Install the Shared Storage Option (SSO) license for mount requests to requeue when physical drive resources are not available.
2. 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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See “Using debug logs” on page 358.
2. 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.

Recommended action:

1. Verify that the user has the necessary permissions to perform this operation.
2. Verify that the VxSS settings are correct, under Host Properties in the NetBackup Administration Console. See the *NetBackup Administrator's Guide Volume I* for information on using the Veritas Security Subsystem (VxSS).

Robotic status code: 260

Message: Robot busy, robot diagnostics in progress

Explanation: The requested robot is running a robot diagnostic.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. 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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. 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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. 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 `ltid` starts.

Robot Error status code: 1

Message: You must be ROOT to start daemon

Explanation: A user other than root started a robotic daemon. This status applies to UNIX systems only.

Recommended action: Log on as the root user before starting robotic daemons. Allow robotic daemons to be started automatically as needed by `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 `ltid` message queue failed. This error indicates that `ltid` (the device daemon or NetBackup Device Manager service) may not be running.

Recommended action:

1. Start `ltid` so that shared memory can be initialized, allowing the robotic daemon/process to function.
2. 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 358.
3. On UNIX servers, gather the output of the `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 `ltid` maintains. (`ltid` is the Media Manager device daemon on UNIX or the NetBackup Device Manager service on Windows.)

Recommended action:

1 Examine command output, debug logs, and system logs for a more detailed message on the error.
See "Using debug logs" on page 358.

2 On UNIX servers, gather the output of the `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 `ltid` maintains. (`ltid` is the Media Manager device daemon on UNIX or the NetBackup Device Manager service on Windows.)

Recommended action:

1 Examine command output, debug logs, and system logs for a more detailed message on the error.
See "Using debug logs" on page 358.

2 On UNIX servers, gather the output of the `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 `ltid` (the Media Manager device daemon on UNIX 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 `ltid` (the Media Manager device daemon on UNIX 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 or the NetBackup Device Manager service on Windows.)

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See “Using debug logs” on page 358.
2. On UNIX 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 servers only).

Recommended action:

1. Restart the device daemon at a later time and investigate system problems that limit the number of processes.
2. Examine the system logs for a more detailed message on the error.
   See “Using debug logs” on page 358.

3. 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 358.

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.

Recommended action:

1. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.
2. 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.

Recommended action:

1. Make sure nbemm is running and responding to requests.
2. Examine command output, debug logs, and system logs for a more detailed message on the error.
   See "Using debug logs" on page 358.

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.

Recommended action:

1. Check product documentation for supported device configurations.
2. 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) or in the *`install_path`*`\NetBackup\share` folder (Windows).

Messages

This section lists Media Manager messages alphabetically. The status code type and number are included in parentheses after the message.

Refer to the appropriate section in this chapter for the status code with explanation and recommended action.

<NONE>

(Device Configuration status code 36)

A memory allocation attempt failed in the robotic daemon

(Robotic status code 240)

a scratch pool is already defined

(Media Manager status code 171)

A SCSI inquiry sent to the device has failed

(Device Configuration status code 16)

ADAMM GUID does not exist in database

(Media Manager status code 168)

ADAMM GUID is not unique in the database

(Media Manager status code 167)

Add Drive Name Rule request failed

(Device Configuration status code 82)

Adding this device would exceed the maximum allowed

(Device Configuration status code 40)

Adding this drive would exceed the maximum allowed

(Device Configuration status code 39)

another daemon already exists

(Media Manager status code 89)

Another device configuration is already in progress

(Device Configuration status code 90)

barcode does not exist in database

(Media Manager status code 78)

barcode label is unreadable

(Robotic status code 235)

barcode not unique in database

(Media Manager status code 36)

barcode tag is not unique in rule database

(Media Manager status code 122)

Block device name for optical disk is not a block device

(Device management status code 54)

cannot allocate requested memory

(Media Manager status code 18)

Cannot assign a robotically controlled device

(Device management status code 64)

Cannot assign due to media ID mismatch

(Device management status code 57)

cannot auto-eject this robot type

(Media Manager status code 51)

cannot auto-inject this robot type

(Media Manager status code 52)

Cannot change terminal mode

(Device Configuration status code 41)

cannot connect to robotic software daemon

(Media Manager status code 42)

cannot connect to vmd [on host *host name*]

(Media Manager status code 70)

Cannot create miscellaneous working repository

(Device Configuration status code 42)

cannot delete assigned volume

(Media Manager status code 92)

cannot delete one of the default volume pools

(Media Manager status code 118)

Cannot discover devices. See the Troubleshooting Guide for details.

(Device Configuration status code 44)

Cannot execute command, permission denied

(Device Configuration status code 1)

cannot get host name

(Media Manager status code 76)

Cannot move from media access port to slot

(Robotic status code 218)

Cannot move from slot to media access port

(Robotic status code 219)

cannot obtain daemon lockfile

(Media Manager status code 21)

Cannot open/create the media access port status file

(Robotic status code 243)

cannot perform operation on this host

(Media Manager status code 60)

Can not retrieve Job ID from Job Manager

(Device management status code 79)

Cannot stop device daemon with tapes assigned

(Device management status code 20)

cannot update database due to existing errors

(Media Manager status code 80)

Character device name for optical disk is not a character device

(Device management status code 38)

child process killed by signal

(Media Manager status code 63)

Cleaning/unknown media in drive

(Robotic status code 258)

Configuration has changed, robot daemons and ltid need restarting

(Robotic status code 262)

Control daemon connect or protocol error

(Robotic status code 224)

CORBA communication error

(Media Manager status code 195)

Could not get hostname

(Device Configuration status code 3)

Credentials already exist

(Device configuration status code 99)

Current version does not support remote device host

(Device Configuration status code 38)

current version does not support this configuration

(Media Manager status code 149)

daemon cannot obtain socket

(Media Manager status code 58)

daemon failed accepting connection

(Media Manager status code 59)

daemon resources are busy

(Media Manager status code 5)

daemon terminated

(Media Manager status code 7)

database open operation failed

(Media Manager status code 26)

database read operation read too few bytes

(Media Manager status code 28)

database read record operation failed

(Media Manager status code 27)

database server is down

(Media Manager status code 23 and Device Configuration status code 93)

database write record operation failed

(Media Manager status code 32)

Delete Drive Name Rule request failed

(Device Configuration status code 84)

device entry is not unique in global device database

(Media Manager status code 153)

device management error

(Media Manager status code 83)

Device path is already in use

(Device Configuration status code 22)

device test state file does not exist

(Media Manager status code 182)

Devices located in multiple domains

(Robot Error status code 16)

Disk Optimization feature is not licensed

(Device Configuration status code 94)

Door is open on cabinet

(Robotic status code 216)

Drive being assigned is either not NDMP or on the wrong NDMP client

(Device management status code 37)

Drive does not exist in robot

(Robotic status code 213)

Drive does not support pending request density

(Device management status code 17)

Drive index is in use by another drive

(Device Configuration status code 29)

Drive is currently assigned

(Device management status code 2)

Drive name does not exist

(Device Configuration status code 35)

Drive name is already in use by another drive

(Device Configuration status code 34)

Drive name rule has exceeded its maximum length of 48 characters

(Device Configuration status code 89)

Drive not available in library for mount request

(Device management status code 62)

Duplicate device path names

(Device Configuration status code 20)

EMM database error

(Media Manager status code 196)

EMM DB record not found

(Media Manager status code 194)

EMM error

(Robotic status code 261 and Robot Error status code 13)

EMM library call failed

(Device management status code 72)

error auto-generating volume group

(Media Manager status code 57)

Error in attaching the shared memory

(Robot Error status code 4)

Error in getting process Id

(Robot Error status code 5)

Error in getting semaphore

(Device management status code 32)

Error in getting shared memory

(Robot Error status code 3)

Error in IPC SHMAT call

(Device management status code 14)

Error in IPC SHMGET call

(Device management status code 13)

Error in MsgGet

(Device management status code 28)

Error in Receiving Daemon Message

(Device management status code 6)

Error in Receiving Operator Message

(Device management status code 4)

Error in Receiving User Message

(Device management status code 8)

Error in SEMAPHORE operation

(Device management status code 33)

Error in SEMAPHORE operation

(Robotic Error status code 9)

Error in Sending Daemon Message

(Device management status code 5)

Error in Sending Operator Message

(Device management status code 3)

Error in Sending User Message

(Device management status code 7)

Evaluation period expired. Go to www.symantec.com to order this product.

(Media Manager status code 165)

failed appending to pool database

(Media Manager status code 104)

failed appending to rule database

(Media Manager status code 121)

failed changing terminal characteristics

(Media Manager status code 45)

failed during tpformat

(Media Manager status code 77)

failed initiating child process

(Media Manager status code 88)

failed making the database directory

(Media Manager status code 25)

failed opening tmp output file

(Media Manager status code 86)

Failed reading drive or robot config file

(Device Configuration status code 13)

failed receiving from robotic software daemon

(Media Manager status code 44)

failed receiving from vmd

(Media Manager status code 72)

failed redirecting input to pipe

(Media Manager status code 62)

failed redirecting tmp output file

(Media Manager status code 87)

failed sending request to vmd

(Media Manager status code 69)

failed sending to robotic software daemon

(Media Manager status code 43)

failed sending to vmd

(Media Manager status code 71)

Failed to find an available slot to inject to

(Robotic status code 246)

failed to initialize a connection to the Enterprise Media Manager

(Media Manager status code 189)

File name already exists

(Device management status code 40)

File name does not exist

(Device management status code 25)

Fork failure occurred

(Robot Error status code 10)

generic EMM SQL error

(Media Manager status code 193)

global device database append operation failed

(Media Manager status code 155)

global device database host name is invalid

(Device Configuration status code 49)

global device database record not found

(Media Manager status code 152)

Host is not the scan host for this shared drive

(Device management status code 48)

incompatible database version

(Media Manager status code 146)

Incomplete robot information

(Device Configuration status code 24)

Incorrect tpreq access mode

(Device management status code 42)

internal database access failure

(Media Manager status code 169)

Internal NDMP error

(Device Configuration status code 57)

invalid barcode

(Media Manager status code 10)

invalid change type

(Media Manager status code 75)

invalid change-entry request

(Media Manager status code 50)

Invalid command code
(Robotic status code 207)

invalid command usage
(Media Manager status code 4)

invalid container id
(Media Manager status code 186)

invalid database host
(Media Manager status code 19)

invalid database version header
(Media Manager status code 56)

invalid description
(Media Manager status code 11)

Invalid device path name
(Device Configuration status code 19)

Invalid drive index
(Device Configuration status code 14)

invalid drive name
(Media Manager status code 129)

Invalid Drive Name Rule
(Device Configuration status code 86)

Invalid Drive Number
(Device management status code 23)

Invalid drive type for the robot
(Device Configuration status code 27)

Invalid Drive Type/Density
(Device management status code 1)

invalid EMM argument
(Media Manager status code 191)

invalid expiration date

(Media Manager status code 113)

Invalid host

(Device Configuration status code 88)

invalid host name

(Media Manager status code 136)

invalid maximum mounts

(Media Manager status code 114)

invalid media generation rule

(Media Manager status code 140)

invalid media ID for naming mode

(Media Manager status code 41)

invalid media ID

(Media Manager status code 8)

invalid media type

(Media Manager status code 9)

Invalid NDMP device

(Device Configuration status code 64)

Invalid NDMP hostname

(Device Configuration status code 55)

Invalid NDMP password

(Device Configuration status code 60)

invalid number of cleanings

(Media Manager status code 74)

invalid number of mounts

(Media Manager status code 141)

invalid offsite location

(Media Manager status code 142)

invalid offsite return date

(Media Manager status code 144)

invalid offsite sent date

(Media Manager status code 143)

invalid offsite session id

(Media Manager status code 148)

invalid offsite slot

(Media Manager status code 147)

Invalid Operator

(Device management status code 12)

invalid pool database entry

(Media Manager status code 102)

invalid protocol request

(Media Manager status code 6)

invalid query type

(Media Manager status code 73)

invalid robot coord1

(Media Manager status code 16)

invalid robot coord2

(Media Manager status code 17)

Invalid robot drive number for the robot type

(Device Configuration status code 28)

invalid robot host

(Media Manager status code 14)

Invalid robot number

(Device Configuration status code 15)

invalid robot number

(Media Manager status code 13)

Invalid robot type

(Device Configuration status code 18)

invalid robot type

(Media Manager status code 12)

invalid rule database entry

(Media Manager status code 119)

invalid scratch pool name

(Media Manager status code 173)

Invalid SCSI bus number for the robot

(Device Configuration status code 8)

Invalid SCSI logical unit number for the robot

(Device Configuration status code 10)

Invalid SCSI port number for the robot

(Device Configuration status code 7)

Invalid SCSI target for the robot

(Device Configuration status code 9)

Invalid Usage

(Device Configuration status code 11)

invalid volgroup

(Media Manager status code 15)

invalid volume move mode

(Media Manager status code 53)

Invalid volume pool specified

(Device management status code 65)

invalid volume pool

(Media Manager status code 90)

IPC Error: Daemon may not be running

(Device management status code 22)

IPC sequence error

(Device management status code 10)

Job Manager returned error: see activity monitor

(Device management status code 80)

List Drive Name Rule request failed

(Device Configuration status code 85)

LTI Daemon may not be running

(Robot Error status code 2)

LTI system error

(Device management status code 75)

Media access port already contains media

(Robotic status code 221)

Media access port does not contain media

(Robotic status code 220)

Media access port is available

(Robotic status code 250)

Media access port is in eject mode

(Robotic status code 253)

Media access port is in inject mode

(Robotic status code 252)

Media access port is unavailable

(Robotic status code 251)

media access port not available

(Media Manager status code 166)

Media does not exist in database

(Device management status code 83)

media generation rule already exists

(Media Manager status code 138)

media generation rule does not exist
(Media Manager status code 139)

media ID is not the specified media type
(Media Manager status code 95)

media ID not unique in database
(Media Manager status code 34)

media type and volume group mismatch
(Media Manager status code 101)

Mount canceled, device daemon is terminating
(Device management status code 56)

Multiple drive paths are not supported for optical drives
(Device Configuration status code 80)

must be root user to execute command
(Media Manager status code 3)

NDMP authorization error, verify username/password
(Device Configuration status code 74)

NDMP config_get_connection_type failed
(Device Configuration status code 76)

NDMP config_get_mover_type failed
(Device Configuration status code 75)

NDMP failed to verify host
(Device Configuration status code 58)

NDMP get_host_info failed
(Device Configuration status code 71)

NDMP get_server_info failed
(Device Configuration status code 72)

NDMP host does not exist
(Device Configuration status code 62)

NDMP host exists, use change option

(Device Configuration status code 61)

NDMP host not connected

(Device Configuration status code 69)

NDMP is not installed on platform

(Device Configuration status code 59)

NDMP request failed

(Device Configuration status code 63)

NDMP robot does not exist

(Device Configuration status code 66)

NDMP robot exists, use change option

(Device Configuration status code 65)

NetApp Disk Storage Unit feature is not licensed

(Device configuration status code 94)

NetBackup Snapshot client not licensed

(Device configuration status code 100)

network protocol error

(Media Manager status code 39)

No action pending for given mount index

(Device management status code 50)

no child process to wait for

(Media Manager status code 64)

No cleaning tape is defined in the device's robot or 0 cleanings remaining

(Device management status code 59)

No compatible device is registered at these SCSI coordinates

(Device Configuration status code 51)

No devices are configured on the robot

(Robot Error status code 6)

No drive available

(Device management status code 82)

no entries changed

(Media Manager status code 47)

no entries deleted

(Media Manager status code 48)

no entries inserted

(Media Manager status code 49)

No Error on operation, sideband data only

(Device management status code 84)

No media found in device or robot slot, please verify

(Device management status code 61)

No memory available

(Robot Error status code 8)

No mount pending for given mount index

(Device management status code 16)

no pools in the pool list

(Media Manager status code 112)

No robot daemon or robotics are unavailable

(Device management status code 60)

No robot is defined of this type

(Device management status code 52)

No robots are configured

(Robot Error status code 7)

<NONE>

(Device Configuration status code 36)

Not authorized by VxSS

(Robotic status code 259)

not authorized to connect to vmd

(Media Manager status code 126)

No valid license key for Disk Array configuration

(Device Configuration status code 97)

Only the administrative user can perform the requested operation

(Device management status code 19)

Open Storage feature is not licensed

(Device configuration status code 98)

operation not allowed on cleaning cartridge

(Media Manager status code 117)

Operator denied mount request

(Device management status code 55)

oprd request is not supported on the remote host

(Media Manager status code 137)

oprd returned abnormal status

(Media Manager status code 96)

Parameter is invalid

(Device management status code 39)

Physical drive is not available

(Robotic status code 245)

pool does not exist in pool database

(Media Manager status code 109)

poolname is not unique in pool database

(Media Manager status code 105)

pool not defined as a catalog backup pool

(Media Management status code 198)

pool not defined as a scratch pool

(Media Manager status code 172)

pool type change is not allowed for <CatalogBackup> pool

(Media Manager status code 22)

Process killed by parent

(Robotic status code 212)

Process killed by signal

(Robotic status code 211)

protocol error

(Media Manager status code 20)

registering this host would exceed the maximum allowed

(Media Manager status code 150)

request can only be performed on the Media and Device management Domain Server

(Media Manager status code 177)

request completed

(Media Manager status code 1)

Request has been queued (Cancel to clear message

(Device management status code 53)

Request terminated because host not validated for volume pool

(Device management status code 26)

Request terminated because media id is expired

(Device management status code 27)

Request terminated because *media id* will exceed maximum mount count

(Device management status code 30)

Request terminated because media is a cleaning tape

(Device management status code: 71)

Request terminated because media is unavailable (in DOWN drive, misplaced, write protected or unmountable

(Device management status code 35)

Request terminated because media is unmountable

(Device management status code 69)

Request terminated because media is write protected

(Device management status code 70)

Request terminated because mount requests are disabled

(Device management status code 63)

Request terminated because of volume pool mismatch

(Device management status code 66)

Request terminated by tpunmount call from another process

(Device management status code 36)

Requested drive could not be reserved

(Device management status code 24)

requested drive is already reserved by host

(Media Manager status code 145)

requested drive is already reserved

(Media Manager status code 130)

Requested drive is in an offline domain

(Robotic status code 238)

requested drive is not currently registered

(Media Manager status code 132)

requested drive is not currently reserved

(Media Manager status code 134)

requested drive is not registered for host

(Media Manager status code 131)

requested drive is not reserved by host

(Media Manager status code 133)

requested host is not currently registered

(Media Manager status code 135)

Requested operation is not supported by the robot

(Robotic status code 229)

Requested slot already has cartridge

(Robotic status code 217)

Requested slot contains the wrong tape

(Robotic status code 226)

Requested slot does not exist in robot

(Robotic status code 228)

Requested slot is empty

(Robotic status code 208)

Requested tape in other or non-configured drive

(Robotic status code 215)

Requested volume is in an offline domain

(Robotic status code 239)

Residence is not licensed for multihosted drive support

(Device Configuration status code 37)

Retry later

(Device management status code 81)

Robot busy, cannot perform operation

(Robotic status code 223)

Robot busy, inject operation in progress

(Robotic status code 255)

Robot busy, inventory operation in progress

(Robotic status code 254)

Robot busy, multiple eject operation in progress

(Robotic status code 256)

Robot busy, multiple inject operation in progress

(Robotic status code 257)

Robot busy, robot diagnostics in progress

(Robotic status code 260)

Robot denied access to the resource

(Robotic status code 234)

Robot drive number in use for this robot

(Device Configuration status code 25)

Robot hardware or communication error

(Robotic status code 225)

Robot has misplaced the media

(Robotic status code 236)

robot host and volume group mismatch

(Media Manager status code 82)

Robot/LTI protocol error

(Device management status code 76)

Robot media access port does not exist

(Robotic status code 242)

robot number and robot host mismatch

(Media Manager status code 61)

robot number and robot type mismatch

(Media Manager status code 54)

robot number and volume group mismatch

(Media Manager status code 55)

Robot number does not exist

(Device Configuration status code 31)

Robot number does not exist

(Robotic status code 214)

Robot number is already in use

(Device Configuration status code 21)

Robot number is in use by another robot

(Device Configuration status code 30)

Robot operation failed

(Device management status code 74)

robot type and volume group mismatch

(Media Manager status code 81)

Robot type must be controlled locally

(Device Configuration status code 33)

Robotic arm has no addressable holder

(Robotic status code 222)

Robotic daemon not licensed

(Robot Error status code 17)

Robotic dismount failure

(Robotic status code 206)

Robotic mount failure

(Robotic status code 205)

robotic volume position is already in use

(Media Manager status code 37)

RSM is not supported

(Device Configuration status code 48)

rule does not exist in rule database

(Media Manager status code 97)

Shared Storage Option (SSO) is not licensed

(Device Configuration status code 53)

specified robot is unknown to vmd

(Media Manager status code 79)

STATUS_SUCCESS

(Robotic status code 200)

Stopping device daemon with tapes assigned

(Device management status code 73)

Success

(Device Configuration status code 0)

Success

(Format optical status code 0)

System Error

(Device Configuration status code 87 and Media Manager status code 2)

System error occurred

(Robot Error status code 11)

System error occurred during robot operation

(Robotic status code 230)

Tape file path exceeds 255 character maximum

(Device management status code 49)

Tape needs to be write enabled

(Device management status code 46)

The device is not robotic, cannot perform cleaning

(Device management status code 58)

The device_mappings file has invalid license info

(Device Configuration status code 2)

The device name is not valid, no device responded

(Device Configuration status code 52)

The drive is DOWN

(Device management status code 15)

The drive is not ready or inoperable

(Device management status code 21)

The drive serial number already exists in the device database

(Device Configuration status code 91)

The eject command was aborted by the user

(Robotic status code 244)

The EMM server failed to process the request

(Device Configuration status code 78)

the global device database device name is invalid

(Media Manager status code 162)

the global device database device type is invalid

(Media Manager status code 160)

the media is allocated for use

(Media Management status code 199)

the operation requested has failed

(Media Manager status code 163)

the query with time failed because a limit was reached

(Media Manager status code 184)

The requested operation is not valid for the specified Disk Type

(Device Configuration status code 95)

the request sent to the Device Allocator has failed

(Media Manager status code 190)

the robotic daemon returned an invalid volume GUID

(Media Manager status code 164)

the robotic library is full and may still have media in its map

(Media Manager status code 185)

The specified Disk Array Host is not configured in NetBackup

(Device Configuration status code 96)

the specified pool is not empty

(Media Manager status code 111)

This is a drive path operation, use the -drpath option

(Device Configuration status code 81)

this machine is not the database host

(Media Manager status code 84)

This robot type does not support multiple media types

(Device Configuration status code 17)

Timeout waiting for robotic command

(Robotic status code 203)

too many volumes in volume group

(Media Manager status code 68)

tpformat: Cannot open

(Format optical status code 3)

tpformat: Cannot read

(Format optical status code 4)

tpformat: Can not retrieve Job ID from Job Manager

(Format optical status code 15)

tpformat: Cannot seek

(Format optical status code 5)

tpformat: Cannot set volume header

(Format optical status code 2)

tpformat: Cannot write

(Format optical status code 6)

tpformat: Command interrupted

(Format optical status code 11)

tpformat: EMM error

(Format optical status code 14)

tpformat: Existing media ID

(Format optical status code 7)

tpformat: Invalid robot

(Format optical status code 10)

tpformat: Invalid usage

(Format optical status code 1)

tpformat: Invalid volume pool specified

(Format optical status code 18)

tpformat: Job Manager returned error: see activity monitor

(Format optical status code 16)

tpformat: Must be root

(Format optical status code 8)

tpformat: No media present in drive or robot slot

(Format optical status code 13)

tpformat: Request terminated because of volume pool mismatch

(Format optical status code 17)

tpformat: Skip

(Format optical status code 12)

tpformat: Tape request failed

(Format optical status code 9)

Unable to allocate memory for this process

(Device configuration status code 79)

Unable to connect to NDMP host verify hostname

(Device configuration status code 67)

Unable to connect to the EMM server

(Device configuration status code 77 and Device management status code 78)

Unable to create NDMP session

(Device configuration status code 70)

unable to find any records in the device test database

(Media Manager status code 176)

unable to generate a unique media id

(Media Manager status code 127)

Unable to initialize robot

(Robotic status code 204)

Unable to open drive

(Robotic status code 209)

Unable to open robotic path

(Robotic status code 201)

unable to open the device test state file

(Media Manager status code 175)

Unable to process NDMP message

(Device configuration status code 68)

Unable to SCSI unload drive

(Robotic status code 210)

unable to send exit status

(Media Manager status code 67)

Unable to sense robotic device

(Robotic status code 202)

unexpected data from robotic software daemon

(Media Manager status code 46)

unexpected data received

(Media Manager status code 40)

Unknown drive name

(Device management status code 41)

unknown EMM error code

(Media Manager status code 192)

Unsupported NDMP version

(Device configuration status code 73)

Update Drive Name Rule request failed

(Device configuration status code 83)

Usage error in creating child process

(Robot Error status code 12)

volume daemon fork failed

(Media Manager status code 85)

volume does not exist in database

(Media Manager status code 35)

volume group does not exist

(Media Manager status code 65)

volume has exceeded maximum mounts

(Media Manager status code 116)

volume has passed expiration date

(Media Manager status code 115)

volume is already assigned

(Media Manager status code 93)

Volume is in home slot

(Robotic status code 249)

Volume is in library, but not in drive domain

(Robotic status code 233)

Volume is in use

(Robotic status code 237)

volume is not in specified pool

(Media Manager status code 94)

Volume not found in library

(Robotic status code 232)

VxSS Access Denied

(Media Manager status code 188, Device management status code 77, and Device configuration status code 92)

VxSS authentication failed

(Media Manager status code 187)

You do not have permission to create the file

(Device management status code 44)

You must be administrator to execute

(Robot Error status code 14)

You must be ROOT to start daemon

(Robot Error status code 1)

Chapter 7

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.

Caution: Before attempting any of the disaster recovery procedures in this chapter, Symantec recommends that you contact technical support.

This chapter provides information about installing NetBackup and, if necessary, recovering NetBackup catalogs after a system disk failure. Symantec assumes that you are recovering to the original system disk or one configured exactly like it.

Caution: If you reinstall NetBackup and recover its catalogs on a system disk to a different partition or on a system disk that is partitioned differently due to internal configuration information, NetBackup may not function properly. Symantec recommends that you set up a replacement disk with identical partitioning to that of the failed disk and that you reinstall NetBackup on the same partition on which it was originally installed.

Note: Specific procedures for replacing a failed disk, building partitions and logical volumes, and reinstalling the operating system 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

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 records that are critical to users and the organization. It is equally important 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, without which it is impossible to restore the client to its original configuration. If you are using a NetBackup exclude list for a client, do not specify any Windows system files in that list.

It is not a good idea to omit executables and other application files. It is tempting to save tape by excluding these easy-to-reinstall files. However, backing up the entire application ensures that it will be restored to its exact configuration. For example, if you have applied software updates/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. For a complete description of BMR backup and recovery procedures, 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 will verify that all of the media needed to restore critical policies are available.

Full backup after catalog recovery

If the configuration contains Windows clients that have their incremental backup configuration set to **Perform Incrementals Based on Archive Bit**, Symantec recommends running a full backup of these clients as soon as possible after a catalog recovery. This will reset the archive bit on files that were backed up with an incremental backup after the time of 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 any subsequent incremental backup.

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 is occurring, providing improved support for environments in which continual backup activity is typical. Symantec recommends use of the online catalog backup rather than the offline catalog backup.

Online catalog backup disaster recovery files

Symantec 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 machine. 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 perform the recovery on a system other than the one that originally made the backups, the system you use should be identical to the original system. For example, if the system performing the recovery does not include NetBackup servers with names that are identical to those on the system where the backups were made, the automated recovery may not succeed.

Online catalog disaster recovery information E-mail

Symantec recommends configuring the online catalog backup policy to e-mail a copy of the disaster recovery information to a NetBackup administrator in your organization as part of every catalog backup. Do not save the disaster recovery information e-mails to the local machine. Catalog recovery from an online catalog backup with neither the disaster recovery image file nor the disaster recovery information e-mail available becomes exceedingly complex, time consuming, and requires assistance.

You may tailor the disaster recovery e-mail process by providing a customized mail script. See the Reference Topics chapter of the *NetBackup Administrator's Guide, Volume II*, for more detail.

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. An example is tape media whose images have all expired after the catalog backup that the recovery was done from and the tape designated for and possibly re-used. Another example is 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 play a part in determining the time required to recover the catalog. Careful planning and testing should be done in order to determine the catalog backup methods that will result in the desired catalog recovery time.

Master and media server backups

While the NetBackup catalog backup protects your NetBackup configuration and catalog data, you should also set up backup schedules for the master and media servers in your NetBackup installation. This ensures that the operating system, device configuration, and other applications on these servers are protected.

The procedures that follow for recovering a master or media server when the system disk has been lost, assume that the master and media 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

The following section describes the procedures for three different types of disk recovery for UNIX:

- Master server disk recovery procedures
- Media server disk recovery procedures
- Client disk recovery procedures

Note: Disk-based images residing on SharedDisk, 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 *NetBackup Administrator's Guide, Volume I.*

NOTE: when the disk image is imported, NetBackup does not recover the original catalog entry for the image. A new catalog entry is created.

Recovering the master server disk

The procedure in this section explains how to recover data if the system disk fails on a UNIX NetBackup master server. 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 lets you recover the root partition without risking a crash due to overwriting files being used by the operating system during the restore.

Note: 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/or NetBackup catalog relocation utilities may need to be used to accomplish this.

Note: NetBackup Bare Metal Restore (BMR) protects client systems by backing them up with a policy configured for BMR protection. See the *Bare Metal Restore System Administrator's Guide* that describes backup and recovery procedures.

Recovering the master server when root is intact

The following procedure recovers the master server by first reloading the operating system, then restoring NetBackup, and finally restoring all other files.

1. Verify that the operating system is working, 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 are recovering. Refer to the *NetBackup Installation Guide for UNIX* for instructions on installing NetBackup software.
3. Install any NetBackup patches that had been previously installed. See the documentation that was included with the patch software.
4. If changes had been made to any of the default catalog directories that would be reflected in the NetBackup catalog backups, recreate those directories prior to 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. This might involve the following:
   - Installing and configuring the robotic software for the devices required to 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 the recovery scenario involves having to 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 might involve the following:

- Manually loading the required media into a standalone recovery device.
- Using the NetBackup utilities such as `robtest` and/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. Refer to one of the following sections, depending on how catalogs were backed up.

- "Catalog recovery from an online backup" on page 540
- "Catalog recovery from offline backup" on page 566

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.

Note: If your configuration includes an 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.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 root 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 lets you recover the root partition without risking a crash due to overwriting files that are being used by the operating system during the restore.

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, if applicable, its catalogs and databases resided on the original disk. By default, they reside under the `/usr/openv` directory.
3. Verify that the operating system is working, 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 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 changes had been made to any of the default catalog directories that would be reflected in the NetBackup catalog backups, recreate those directories prior to the catalog recovery. For example:
   - 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. This might involve the following:
   - Installing and configuring the robotic software for the devices required to 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, 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* manual.
- Updating the device mapping files. See the *NetBackup Administrator's Guide, Volume II*.

8 If the recovery scenario involves having to restore from policy or catalog backups that were done to media, the appropriate media may need to be configured in NetBackup. See the *NetBackup Administrator’s Guide, Volume I*. Configuring the media might involve the following:

- Manually loading the required media into a standalone recovery device.
- Using NetBackup utilities such as `robtest` and/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).

9 Recover the NetBackup catalogs to the alternate disk. Refer to one of the following sections, depending on how catalogs were backed up.

- “Catalog recovery from an online backup” on page 540
- “Catalog recovery from offline backup” on page 566

The NetBackup catalogs can be recovered only to the same directory structure from which they were backed up (alternate path recovery is not allowed).

10 Start the NetBackup Backup, Archive, and Restore interface (or the `bp` command) and restore the latest backed up version of all files to the disk you are recovering.

Note: You will be restoring these files from the backup of the master server (not from the NetBackup catalog backup). Be sure to specify the disk you are recovering as the alternate recovery location.

Caution: Do not restore files to the `/usr/openv/var`, `/usr/openv/db/data`, or `/usr/openv/volmgr/database` directories (or relocated locations) or directories containing NetBackup database data. This data was recovered to the alternate disk in step 9 and will be 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 are recovering. These are the catalogs recovered in step 9.

13 Make the recovered disk the boot disk again and reboot the system.

14 Start and test the copy of NetBackup on the disk that you have recovered.

Note: 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

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.

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 the following Recovering the Client Disk section).

Recovering the client disk

Note: NetBackup Bare Metal Restore (BMR) protects client systems by backing them up with a policy configured for BMR protection. For a complete description of BMR backup and recovery procedures, see the *Bare Metal Restore 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 below.

The following is the procedure for recovering 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 boot from this disk. After restoring the system, restore root to its original partition. This lets you recover the root partition without risking a crash due to overwriting files being used by the operating system during the restore. The procedure is similar to that for the master server, except that recovering the NetBackup catalogs is not necessary. (See "Recovering the master server disk" on page 532.)
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

Note: Disk-based images residing on SharedDisk, 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 *NetBackup Administrator's Guide, Volume I.*

NOTE: when the disk image is imported, NetBackup does not recover the original catalog entry for the image. A new catalog entry is created.

Recovering the master server disk

The procedure in this section explains how to recover data if one or more disk partitions are lost on a Windows NetBackup master server. Two scenarios are covered:

- Windows is intact and not corrupted. The system still boots 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. This is a total recovery. These Windows recovery procedures assume that the NetBackup master disk was running a supported version of the Microsoft Windows operating system and that the defective hardware has been replaced.

Note: 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 prior to the catalog recovery.

Recovering 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* for instructions on installing NetBackup software.
5. Install any NetBackup patches that had been previously installed. See the documentation that was included with the patch software.
6. If changes had been made to any of the default catalog directories that would be reflected in the NetBackup catalog backups, recreate those directories prior to 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 device(s) must be configured. This might involve the following:

   - Installing and configuring the robotic software for the devices required to 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, 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*.

8. If the recovery scenario involves having to restore from policy or catalog backups that were done to media, the appropriate media may need to be configured in NetBackup. See the *NetBackup Administrator’s Guide, Volume I*. Configuring the media might involve the following:

   - Manually loading the required media into a standalone recovery device.
   - Using NetBackup utilities such as `robtest` and/or vendor specific robotic control software to load media into the required recovery device(s).
   - 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).

9. Recover the NetBackup catalogs as described in one of the following sections, depending on how the catalogs were backed up:

   - “Catalog recovery from an online backup” on page 540
   - “Catalog recovery from offline backup” on page 566

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
    ```

Note: If your configuration includes an EMM server that is separate from the master server, start NetBackup on the EMM server before starting NetBackup on the master server.

Caution: 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 will 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 Restore all other files:

a Start the NetBackup Administration interface on the master server.

b Start the Backup, Archive, and Restore utility.

c Browse for restores and select only the partitions that were lost. It is especially important to select the system directory (typically `C:\Winnt`). This ensures that all registry files are restored.

d Deselect the `install_path\NetBackup\db`, `install_path\NetBackupDB`, `install_path\NetBackup\var`, and `install_path\Volmgr\database` directories (see the caution above).

e If reinstalling Windows, select the **Overwrite existing files** option. This ensures that existing files are replaced with the backups.

f Start the restore.

12 Reboot the system.
This 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

The following procedures assumes that all disk partitions in Windows are lost.

1 Install a minimal Windows operating system (perform the Express install). Be certain to do the following:

- 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 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 you are recovering. Refer to the *NetBackup Installation Guide for Windows* for instructions on installing NetBackup software. 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 changes had been made to any of the default catalog directories that would be reflected in the NetBackup catalog backups, recreate those directories prior to 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. This might involve the following:
   - Installing and configuring the robotic software for the devices required to 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 you do not need a robot (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 the recovery scenario involves having to 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 might involve the following:

- Manually loading the required media into a standalone recovery device.
- Using NetBackup utilities such as `robtest` and/or vendor specific robotic control software to load media into the required recovery device(s).
- 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).

10 Recover the NetBackup catalogs as described in one of the following sections, depending on how the catalogs were backed up:

- "Catalog recovery from an online backup" on page 540
- "Catalog recovery from offline backup" on page 566

11 When catalog recovery is complete, stop and restart the NetBackup services. You can 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
```

Note: 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.

Caution: 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 will leave the catalogs 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 10 and should not be restored in step 12.

12 Restore all other files:

- **a** Start the NetBackup Administration interface on the master server.
- **b** Start the Backup, Archive, and Restore client interface.
- **c** Browse for restores and select only the partitions that were lost. It is especially important to select the system directory (typically C:\Winnt). This ensures that all registry files are restored.
- **d** 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 above).
- **e** If reinstalling Windows, select the **Overwrite existing files** option. This ensures that existing files are replaced with the backups.
- **f** Start the restore.

13 Reboot the system.

This 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

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.

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 Client Disk Recovery that follows).

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.

Note: NetBackup Bare Metal Restore (BMR) protects client systems by backing them up with a policy configured for BMR protection. For a complete description of BMR backup and recovery procedures, 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 below.

This procedure assumes that the Windows operating system and NetBackup are reinstalled in order to boot the system and perform a restore. It also assumes:

- 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. This is the server from which you will be requesting the restore.
- The backups included the directory where the operating system, and therefore the registry, resided.
  If the backups excluded any files that resided in the above 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 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.
- 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, be certain to:
    - 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 and 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 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 enables NetBackup to start logging to the `bpinetd` debug log.

8. Use the NetBackup Backup, Archive, and Restore interface to restore the system 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. Refer to the online help or the *NetBackup Backup, Archive, and Restore Getting Started Guide* for instructions.

Note: 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. Reboot 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 section explains how to recover a catalog that was backed up using the online, hot catalog backup method described in the *NetBackup Administrator's Guide, Volume I.*

The online catalog backup method was introduced in NetBackup 6.0. If the catalog was not backed up using the online method, refer to "Catalog recovery from offline backup" on page 566.

This procedure can be standalone or part of a larger disk recovery procedure (see"Disk recovery procedures for UNIX" on page 525 or "Disk recovery procedures for Windows" on page 531).

Note: When any online catalog backup recovery attempt that involves media completes, NetBackup changes the state of the media containing the catalog backup to frozen. This prevents any subsequent accidental overwriting of 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. To unfreeze the media, refer to "Unfreezing online catalog recovery media" on page 565.

Note: You must have root (administrative) privileges to perform these procedures.

There are two methods of recovering the catalog from an online, hot backup:

- Recovering the entire catalog
  This is the recommended method for recovering the entire catalog and will recover 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

The entire catalog can be recovered by using the Catalog Recovery Wizard or the text-based `bprecover -wizard` command.

Caution: Do not run any client backups before recovering the NetBackup catalog.

Note: The Catalog Recovery Wizard screens that appear when performing these procedures are very similar for UNIX and Windows platforms. Only the Windows screens are shown in text in the following procedures.

Recovering the entire catalog using the Catalog Recovery Wizard

Do the following to recover the entire catalog using the Catalog Recovery Wizard. You must have root (administrative) privileges.

1 Start NetBackup by entering the following:

Note: 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.

UNIX:

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

Windows:

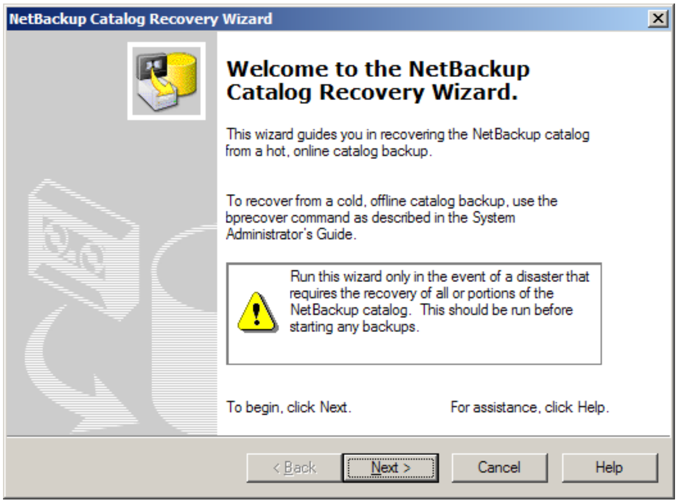
```
install_path\NetBackup\
bin\bpup
```

The NetBackup Administration Console appears.

2 If the necessary devices are not already configured, configure them in NetBackup.

3 Make available to NetBackup the media containing the catalog backup.

4 Click **Recover the Catalogs** on the NetBackup Administration Console to start the Catalog Recovery Wizard.



NetBackup Catalog Recovery Wizard

Welcome to the NetBackup Catalog Recovery Wizard.

This wizard guides you in recovering the NetBackup catalog from a hot, online catalog backup.

To recover from a cold, offline catalog backup, use the bprecover command as described in the System Administrator's Guide.

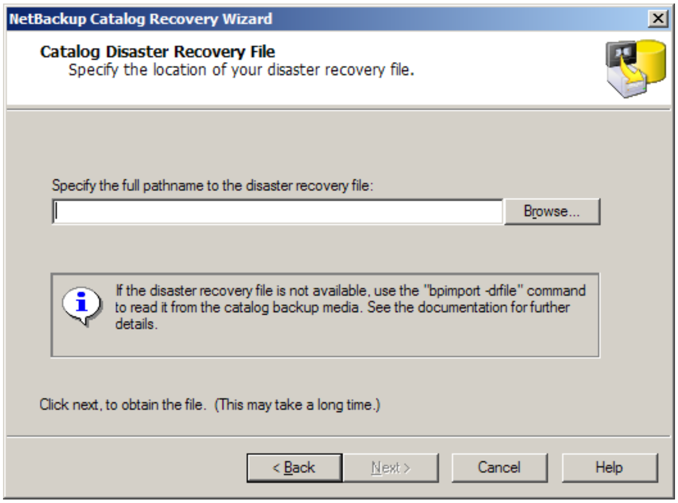
Run this wizard only in the event of a disaster that requires the recovery of all or portions of the NetBackup catalog. This should be run before starting any backups.

To begin, click Next.

For assistance, click Help.

The **Welcome** screen appears.

5 Click **Next** on the Welcome screen to display the **Catalog Disaster Recovery File** screen.



NetBackup Catalog Recovery Wizard

Catalog Disaster Recovery File
Specify the location of your disaster recovery file.

Specify the full pathname to the disaster recovery file:

If the disaster recovery file is not available, use the "bpimport -drfile" command to read it from the catalog backup media. See the documentation for further details.

Click next, to obtain the file. (This may take a long time.)

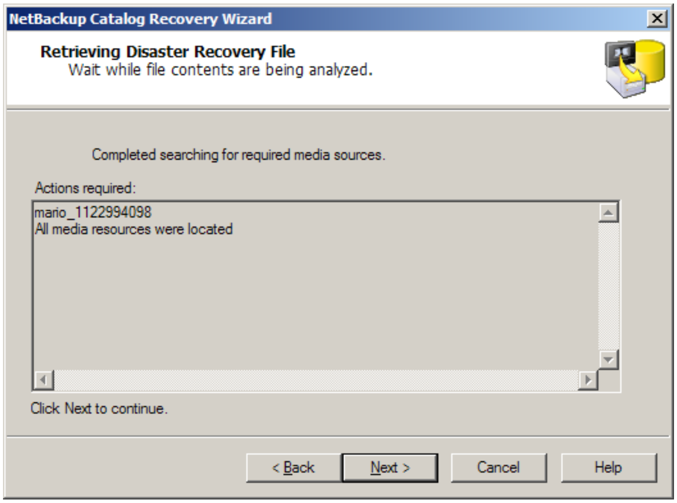
This wizard relies on the disaster recovery information generated during the online catalog backup. Part of configuring the online catalog backup included indicating where the disaster recovery information file was to be stored and/or sent.

In most cases, you would specify the most recent disaster recovery information file available, unless some form of corruption 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 followed by the incremental.)

Indicate where the disaster recovery file is stored by entering the fully qualified path to the disaster recovery file.

For more information on the e-mail that is sent and the attached disaster recovery file, see “Recovering the catalog without the disaster recovery file” on page 559.

6 The wizard waits while NetBackup searches for the necessary media sources, then informs you whether or not the necessary backup ID of the disaster recovery image was located.



NetBackup Catalog Recovery Wizard

Retrieving Disaster Recovery File

Wait while file contents are being analyzed.

Completed searching for required media sources.

Actions required:

```
mario_1122994098
All media resources were located
```

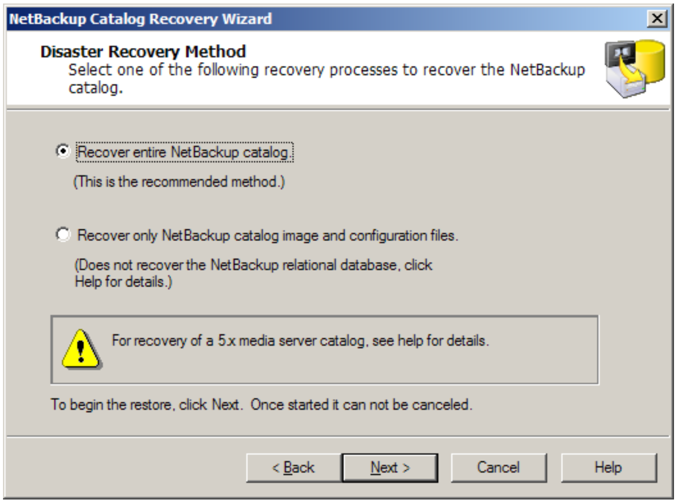
Click Next to continue.

Or, if the media was not located, the wizard lists which media is needed to update the database.

Follow the wizard instructions to insert the media indicated and run an inventory to update the NetBackup database. The information displayed on this screen depends on whether the recovery is from a full backup or an incremental backup.

Note: If an online catalog backup policy included both full and incremental backups, the disaster recovery e-mail may indicate either a full or an incremental backup for recovery. Recovering from an incremental backup will completely recover the entire catalog because it references information from the last full backup. It is not necessary to first recover the last full catalog backup, then subsequent incremental backups.

7 When the required media sources are all found, click **Next** to display the **Disaster Recovery Method** screen. The **Recover entire NetBackup catalog** radio button is selected.



NetBackup Catalog Recovery Wizard

Disaster Recovery Method
Select one of the following recovery processes to recover the NetBackup catalog.

● Recover entire NetBackup catalog.
(This is the recommended method.)

○ Recover only NetBackup catalog image and configuration files.
(Does not recover the NetBackup relational database, click Help for details.)

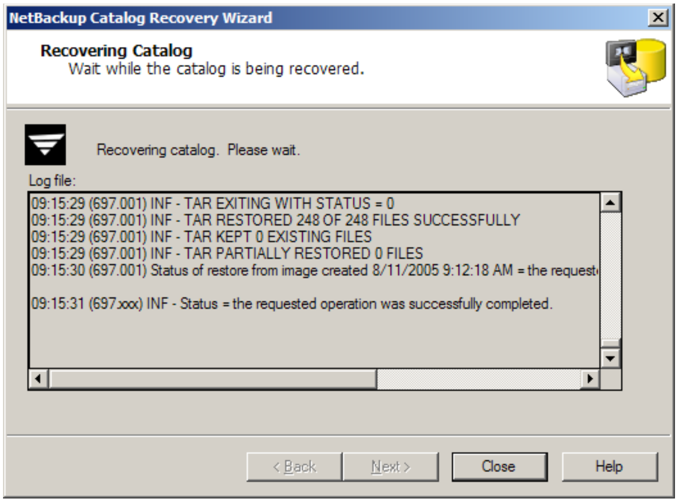
For recovery of a 5.x media server catalog, see help for details.

To begin the restore, click Next. Once started it can not be canceled.

8 With the **Recover entire NetBackup catalog** radio button selected, click **Next** to initiate the recovery of the entire NetBackup catalog. This wizard cannot be used to recover the catalog on NetBackup 5.x or earlier media servers.

NetBackup restores the entire NetBackup relational database, which includes the NBDB database (including the EMM database), the BMR database (if applicable), and the NetBackup policy files, backup image files, and other configuration files. If the EMM server is located on a remote machine, the NBDB database will be recovered on the remote machine.

9 The wizard displays the recovery progress.


NetBackup Catalog Recovery Wizard
Recovering Catalog
Wait while the catalog is being recovered.
Recovering catalog. Please wait.
Log file:
< Back
Next >
Close
Help

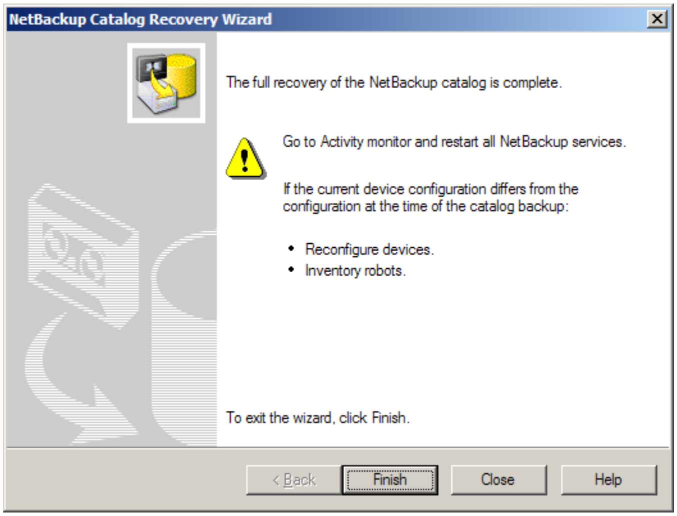
```
09:15:29 (697.001) INF - TAR EXITING WITH STATUS = 0
09:15:29 (697.001) INF - TAR RESTORED 248 OF 248 FILES SUCCESSFULLY
09:15:29 (697.001) INF - TAR KEPT 0 EXISTING FILES
09:15:29 (697.001) INF - TAR PARTIALLY RESTORED 0 FILES
09:15:30 (697.001) Status of restore from image created 8/11/2005 9:12:18 AM = the request

09:15:31 (697.xxx) INF - Status = the requested operation was successfully completed.
```

If the recovery is not successful, consult the log file messages for an indication of the problem.

10 The final screen announces that the full recovery is complete, that each image file is restored to the proper image directory, and that the NetBackup relational databases (NBDB and optionally BMRDB) have been restored and recovered.

Note: If this is part of a server recovery procedure, complete the remaining steps in the appropriate Server Disk Recovery procedure earlier in this chapter.


NetBackup Catalog Recovery Wizard

The full recovery of the NetBackup catalog is complete.

Go to Activity monitor and restart all NetBackup services.

If the current device configuration differs from the configuration at the time of the catalog backup:

- Reconfigure devices.
- Inventory robots.

To exit the wizard, click Finish.

11 NetBackup will not run scheduled backup jobs until NetBackup is stopped and restarted. Prior to restarting NetBackup, protect media that contains any backups that were successfully performed after the catalog backup that was just used to recover the catalog. This could include:

- importing the backups from the backup media into the catalog
- write protecting the media
- ejecting the media and setting it aside
- freezing the media

12 You can manually submit backup jobs prior to stopping and restarting NetBackup. Be aware that if you have not protected the media containing backups done after the catalog backup, the media may be overwritten.

13 Stop and restart NetBackup on all the servers.

UNIX:

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

Windows:

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

If a remote EMM server is being utilized, start NetBackup on it prior to starting NetBackup on the master server.

Note: If you have recovered from removable media, that media is now frozen. To unfreeze, go to "Unfreezing online catalog recovery media" on page 565.

Recovering the entire catalog using bprecover -wizard

The `bprecover -wizard` command is an alternate way to recover an entire catalog backed up using the online catalog backup method. This method does not require the NetBackup Administration Console. The basic steps are the same as those documented under "Recovering the entire catalog using the Catalog Recovery Wizard" on page 541.

Note: You must have root (administrative) privileges to perform this procedure.

1 Start NetBackup by entering the following:

Note: 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.

UNIX:

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

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 will not run scheduled backup jobs until NetBackup is stopped and restarted. Prior to restarting NetBackup, protect media that contains any backups that were successfully performed after the catalog backup that was just used to recover the catalog. This could include:

- 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.

UNIX:

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

Windows:

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

If a remote EMM server is being utilized, start NetBackup on it prior to starting 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, see “Recovering NetBackup relational database files” on page 577.

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 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 allows for the complete restoration of all backup images via 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 can be done in either of the following ways:

- Using the Catalog Recovery Wizard
- Using the `bprecover -wizard` command

During a manual recovery, the wizard recovers only NetBackup policy files, NetBackup backup image files, and other NetBackup configuration files, but does not recover the NBDB (includes EMM) or BMR databases.

If the backup recovered from is an incremental catalog backup and no catalog backup images exist in the catalog, only the NetBackup policy, backup image, and configuration files 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 that you can restore the remaining 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
```

Following is a list of the files that will be recovered in a manual recovery (an asterisk indicates multiple files within that folder):

Table 7-1 Files Recovered by Recovery of Catalog Image Files

UNIX	Windows
/usr/openv/netbackup/bp.conf	*install_path*\NetBackup\db\*
/usr/openv/netbackup/db/*	*install_path*\NetBackup\vault\sessions\*
/usr/openv/netbackup/vault/sessions*	*install_path*\NetBackup\var\*
/usr/openv/var/*	*install_path*\Volmgr\database\*
/usr/openv/volmgr/database/*	*install_path*\Volmgr\vm.conf
/usr/openv/volmgr/vm.conf	

Table 7-2 Files *Not* Recovered by Recovery of Catalog Image Files

NetBackup relational database (ASA) files:

`NBDB.db`
`NBDB.log`
`EMM_DATA.db`
`EMM_INDEX.db`
`BMRDB.db`
`BMRDB.log`
`BMR_DATA.db`
`BMR_INDEX.db`
`vxdbms.conf`
■ *`install_path`*`\NetBackupDB\conf\server.conf` (Windows only)
■ *`install_path`*`\NETBACKUP\DB\conf\databases.conf` (Windows only)
To recover these files, see “Recovering NetBackup relational database files” on page 577.

Recovering the catalog image files using the Catalog Recovery Wizard

You must have root (administrative) privileges to perform this procedure.

1 Start NetBackup by entering the following:

Note: If your configuration includes an EMM server that is separate from the master server, start NetBackup on the EMM server before starting NetBackup on the master server.

UNIX:

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

Windows:

`install_path``\NetBackup\bin\bpup`

2 Click **Recover the Catalogs** in the NetBackup Administration Console to start the Catalog Recovery Wizard.

Caution: Do not run any client backups before recovering the NetBackup catalog.

3 This wizard relies on the disaster recovery information generated during the online, hot catalog backup. Part of configuring the catalog backup included indicating where the disaster recovery information was to be stored and/or sent.

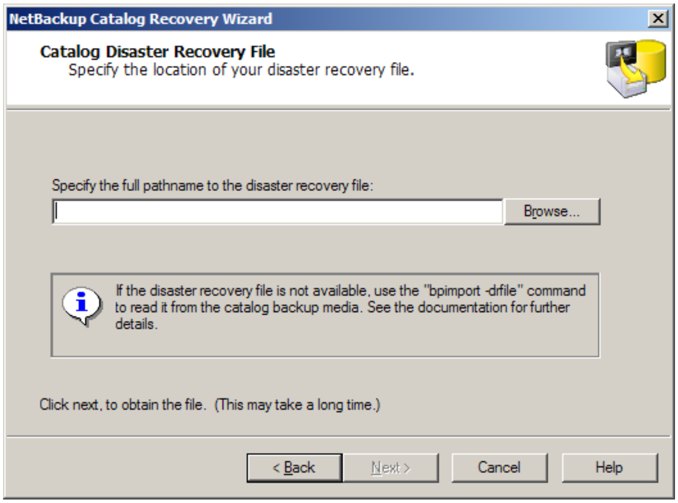
Indicate where the disaster recovery file is stored by entering the fully qualified path to the disaster recovery file.
For example:

```
/net/lex/Cat_DR/CatBk_1119304246_INCR
```

Note: Specify the most recent disaster recovery file available, unless there is a reason to restore from an earlier state.

Note: Be sure to note whether the disaster recovery file is based on a full (`*_FULL`) or an incremental (`*_INCR`) catalog backup. For more information on the e-mail that is sent and the attached disaster recovery file, see "Recovering the catalog without the disaster recovery file" on page 559.

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. Or, if the media was not located, the wizard lists which media is needed to update the database.


NetBackup Catalog Recovery Wizard

Catalog Disaster Recovery File
Specify the location of your disaster recovery file.

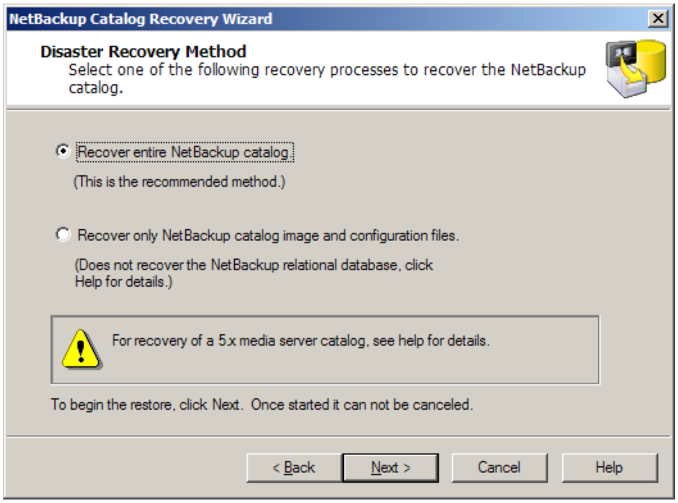
Specify the full pathname to the disaster recovery file:

If the disaster recovery file is not available, use the "bpimport -drfile" command to read it from the catalog backup media. See the documentation for further details.

Click next, to obtain the file. (This may take a long time.)

Follow the wizard instructions to insert the media indicated 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 button and click **Next**.



NetBackup Catalog Recovery Wizard

Disaster Recovery Method
Select one of the following recovery processes to recover the NetBackup catalog.

● Recover entire NetBackup catalog.
(This is the recommended method.)

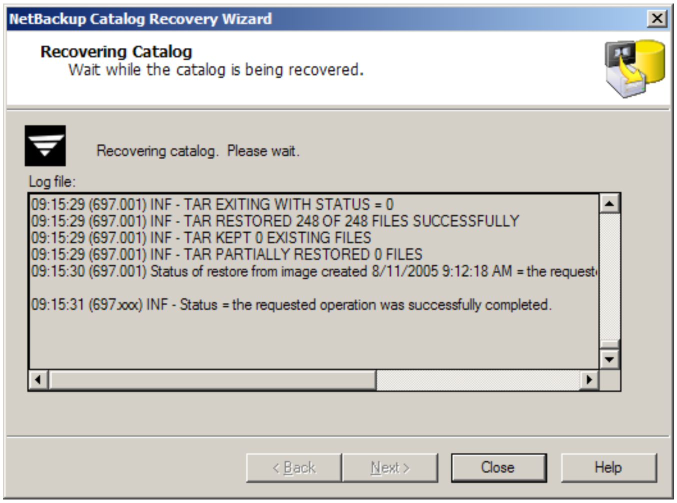
○ Recover only NetBackup catalog image and configuration files.
(Does not recover the NetBackup relational database, click Help for details.)

For recovery of a 5.x media server catalog, see help for details.

To begin the restore, click Next. Once started it can not be canceled.

Note: This wizard cannot be used to recover the catalog on NetBackup 5.x or earlier media servers.

6 The wizard displays the recovery progress and announces when the catalog has been recovered.



NetBackup Catalog Recovery Wizard

Recovering Catalog
Wait while the catalog is being recovered.

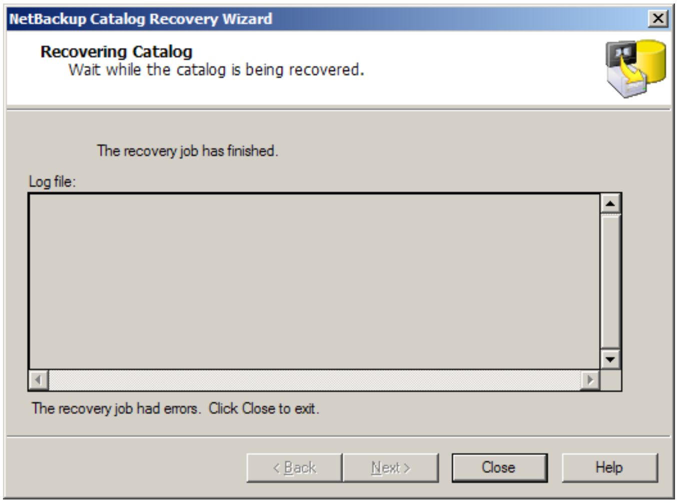
Recovering catalog. Please wait.

Log file:

```
09:15:29 (697.001) INF - TAR EXITING WITH STATUS = 0
09:15:29 (697.001) INF - TAR RESTORED 248 OF 248 FILES SUCCESSFULLY
09:15:29 (697.001) INF - TAR KEPT 0 EXISTING FILES
09:15:29 (697.001) INF - TAR PARTIALLY RESTORED 0 FILES
09:15:30 (697.001) Status of restore from image created 8/11/2005 9:12:18 AM = the request

09:15:31 (697.xxx) INF - Status = the requested operation was successfully completed.
```

If the recovery is not successful, consult the log file messages for an indication of the problem.



NetBackup Catalog Recovery Wizard

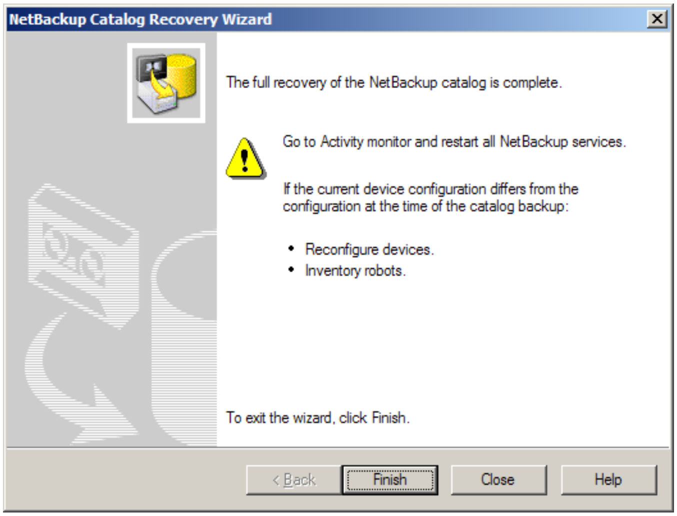
Recovering Catalog
Wait while the catalog is being recovered.

The recovery job has finished.

Log file:

The recovery job had errors. Click Close to exit.

7 The final screen indicates that the catalog backup images have been recovered.



NetBackup Catalog Recovery Wizard

The full recovery of the NetBackup catalog is complete.

Go to Activity monitor and restart all NetBackup services.

If the current device configuration differs from the configuration at the time of the catalog backup:

- Reconfigure devices.
- Inventory robots.

To exit the wizard, click Finish.

Note: You can now recover the NetBackup database if necessary.

8 NetBackup will not run scheduled backup jobs until NetBackup is stopped and restarted. Prior to restarting NetBackup, protect media that contains

any backups that were successfully performed after the catalog backup that was just used to recover the catalog. This could include:

- 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.

UNIX:

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

Windows:

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

If a remote EMM server is being utilized, start NetBackup on it prior to starting NetBackup on the master server.

Recovering the catalog image file using bprecover -wizard

You must have root (administrative) privileges to perform this procedure.

1 Start NetBackup by entering the following:

Note: 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.

UNIX:

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

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 was 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
```

Note: You can now recover the NetBackup database if necessary.

6 NetBackup will not run scheduled backup jobs until NetBackup is stopped and restarted. Prior to restarting NetBackup, protect media that contains any backups that were successfully performed after the catalog backup that was just used to recover the catalog. This could include:

- 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.

UNIX:

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

Windows:

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

If a remote EMM server is being utilized, start NetBackup on it prior to starting 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 the following steps. The relational database files are listed under “Files Not Recovered by Recovery of Catalog Image Files” on page 551.

Note: The full procedure is necessary only if the NBDB database has been corrupted and a temporary database must be created to restore from the catalog backup. If the NBDB database is available and the Sybase ASA server is running, then you need only perform 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.

1 If NetBackup is running, stop it.

UNIX:

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

Windows:

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

2 Change databases.conf so Sybase ASA does not attempt to automatically start them when the server is started.

UNIX:

```
/usr/openv/db/bin/nbdb_admin -auto_start NONE
```

Windows:

```
install_path\NetBackup\bin\nbdb_admin -auto_start NONE
```

3 Start the Sybase ASA server.

UNIX:

```
/usr/openv/netbackup/bin/nbdbms_start_stop start
```

Windows:

```
install_path\NetBackup\bin\bpup -e ASANYs_VERITAS_NB
```

4 **Re-create an empty database.**

UNIX:

```
/usr/openv/db/bin/create_nbdb -drop
```

Windows:

```
install_path\NetBackup\bin\create_nbdb -db_server
VERITAS_NB_servername -drop
```

5 Stop and restart NetBackup.

UNIX:

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

Windows:

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

6 Run tpext:

UNIX:

```
/usr/openv/volmgr/bin/tpext
```

Windows:

```
install_path\Volmgr\bin\tpext
```

7 If you have used the `nbdb_move` command to relocate NetBackup database files, re-create the directories where the files were located at the time of the catalog backup. The default location is:

UNIX:

```
/usr/openv/db/data
```

Windows:

```
install_path\NetBackupDB\data
```

8 Start the device manager:

UNIX:

```
/usr/openv/volmgr/bin/ltid -v
```

Windows: start the device manager service.

9 Configure the necessary recovery device in NetBackup.

10 Make available to NetBackup the media that contains the catalog backup. Inventory the robot or add the media for standalone drives.

11 For online catalog recovery, run the following command on the master server:

UNIX:

```
/usr/openv/netbackup/bin/admincmd/bprecover -r -nbdb
```

Windows: start the device manager service.

```
install_path\NetBackup\bin\admincmd\bprecover -r -nbdb
```

12 Stop and restart NetBackup.

UNIX:

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

Windows:

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

If a remote EMM server is being utilized, start NetBackup on it prior to starting NetBackup on the master server.

Recovering NetBackup access management components

If you have configured NetBackup Access Control (NBAC), your authentication and authorization configuration information is automatically backed up by the online, hot catalog backup.

Both the Operate and Configure permission sets are required on the catalog object in order to successfully backup 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 and configured prior to running the actual catalog recovery wizard or `bprecover` command.

2 Recover the NetBackup catalog from the online catalog backup using the recovery wizard or bprecover command. Authentication and authorization data will *not* be copied back to the hosts from which it was backed up; instead, it will be copied to a staging area for use in step 4.

3 Shut down the authentication and authorization services/daemons.

4 Run "`bprecover -r -vxss -p <policy name>`", supplying the name of the online catalog backup policy. This will recover 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/daemons.

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

With the online, hot catalog backup, it is possible to create multiple copies of the catalog backup, either by specifying multiple copies when the backup is originally done or by duplicating the catalog backup later. To recover the catalog from a copy, refer to "Recovering the catalog without the disaster recovery file" on page 559.

Recovering the catalog without the disaster recovery file

If the disaster recovery file has been lost, consult the e-mail that was sent to the administrator when the catalog was backed up. In addition to writing the Disaster Recovery file to the location you specify in the catalog backup policy, the Disaster Recovery file is also appended to the backup stream itself. To recover the catalog from an online catalog backup when you no longer have the Disaster Recovery file, use the following procedure.

1 The e-mail will identify the media that contains the Disaster Recovery file, as well as the media that was used to backup 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 will recover all disaster recovery files from the specified media id (which can be either a tape media id or the fully qualified location of a disk storage unit) and place them in the specified directory.

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.

5 Continue with the normal catalog recovery procedure by running the NetBackup Recovery Wizard or `bprecover` command, providing the Disaster Recovery file location when prompted.

Note: The recovery instructions that are sent when the catalog backup is completed, or when a catalog backup image is duplicated, are the most current instructions for recovering your catalog. Please refer to the e-mail as your primary source for recovery instructions.

The following is an example of a Disaster Recovery e-mail. Note that the name of the online catalog backup policy is CatalogBackup and the name of the Disaster Recovery file written to is `/storage/DR/CatalogBackup_1123605764_FULL`. The file name itself indicates if the backup was full or not.

```
Server
    ant

Date
    Tue Aug  9 11:41:48 2005

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 2005, retain a copy of the attached file, and the
media  or files listed below:

Catalog Recovery Media
        Media Server                Disk image path
```

```
      * ant
     /storage/DiskUnit1/ant_1123605764_C1_TIR
      * ant
     /storage/DiskUnit1/ant_1123605764_C1_F1
      * ant
     /storage/DiskUnit1/ant_1123605713_C1_F1

DR file written to
    /storage/DR/CatalogBackup_1123605764_FULL

* - Primary Media


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:
        bpimport -create_db_info [-server name] -id
/storage/DiskUnit1
    5. Go to the following directory to find the DR image file
       CatalogBackup_1123605764_FULL:
       /usr/openv/netbackup/db/images/ant/1123000000/tmp
    6. Delete the other files in the directory.
    7. Open CatalogBackup_1123605764_FULL file and find the
BACKUP_ID
    (for example: ant_1123605764).
    8. Run:
        bpimport [-server name] -backupid ant_1123605764
    9. Run:
        bprestore -T -w [-L progress_log] -C ant -t 35 -p
CatalogBackup -X -s 1123605764 -e 1123605764 /
    10. Run the BAR user interface to restore the remaining image
database
    if the DR image is a result of an incremental backup.
    11. To recover the NetBackup relational database, run:
        bprecover -r -nbdb
    12. Stop and Start NetBackup
    13. Configure the devices if any device has changed since the
last
    backup.
    14. To make sure the volume information is updated, inventory
the media
    to update the NetBackup database.
```

User-directed online catalog recovery from the CLI

This procedure is used to recover the catalog manually through the command line interface (CLI) without a Phase 1 import when the Disaster Recovery (DR) file is available. You must have root (administrative) privileges to perform this procedure.

Note: Use this procedure only if you want to restore the minimal NetBackup catalog information that will allow you to begin recovering critical data.

1. Verify the location of the Disaster Recovery Files created from Full and Incremental Hot Catalog backups. The Disaster Recover files can be stored in a specified path of the file system on the master server and in e-mail attachments to the NetBackup administrator.
2. Set up each master and media server in the same configuration as used during the last Catalog Backup. The master and media servers have the

same name, NetBackup version, operating system patch level, and path to Storage Devices as the backed up Catalog Configuration.

Configure any devices and volumes you may need for the recovery.

3 Locate the latest DR image file corresponding to the backup that will be used for recovery. Open the file in an editor and find values for the following:

- *master_server* – use the exact name specified in NetBackup configuration for the Master Server
- *media_server* – the location of the robot or disk storage unit used for catalog backup.
- *timestamp* – the 4 most significant digits in the DR filename and six zeros attached.
- *media* – the media where the catalog backup 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:

```
/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 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.

   a Open the Backup, Archive, and Restore client interface for NetBackup. Select NBU-Catalog as the policy type. Set the source and destination clients to your master server.

   b Search the backups and restore all files located in:

   ```
   install_path/netbackup/db/images/master_server
   ```

   c Verify that all files are restored successfully on the master server.

9 Restore your critical data via the Backup, Archive, and Restore client interface or the command line.

   a Restore the catalog backup images for each media server which requires data recovery.

   b 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:

   ```
   install_path/netbackup/db/images
   ```

   and restore the images for each configured media server. Verify 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 used to back up the desired data. Select the desired files from the Backup, Archive, and Restore client interface and restore them.

11 Recover the NetBackup relational database. To do this, run:

   ```
   bprecover -r -nbdb
   ```

   This command will restore NetBackup media usage information, ensure that media containing backups are not overwritten, and restore the storage unit configuration.

   If it is not possible to recover the NetBackup relational database because you are recovering to a configuration that is not identical to the configuration on which the catalog was backed up, you must import each piece of backup media.

12 If your catalog recovery media is on tape, freeze the media containing the catalog backup used for recovery. This protects the media from being reused:

   ```
   bpmedia -freeze -m media -h master_server
   ```

   Run `bpmedialist` to verify the media is frozen.

13 Recover your policies and configuration data on each master server and media server.

Note: Before recovering NetBackup policy files, you should ensure that you have recovered all of your critical data, or protected the media containing your critical data. When policy information is recovered, NetBackup will begin running scheduled jobs, and they 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 and destination clients to your server, starting with the master server.

Restore all files backed up by the hot catalog backup on each server.

14 Stop and restart the NetBackup services.

Restoring files from an online catalog backup

Since the online catalog backup uses the standard backup format, you may recover specific files from an online catalog backup using the NetBackup Backup, Archive, and Restore user interface. Symantec recommends that you restore catalog files to an alternate location, since restoring catalog files directly to their original location may cause inconsistencies in the NetBackup catalog or cause NetBackup to fail.

When restoring files from an online catalog backup from the NetBackup Backup, Archive and Restore user interface, be aware of the following:

- 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

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.

   a Identify the associated catalog backup parent image file by viewing the PARENT_IMAGE_ID value.

   b Identify the media that the catalog backup was written to by viewing the second to last field in the DR_MEDIA_REC line(s).

   c Save the catalog backup parent image file identified in step a.

   d Relocate or remove all other image files relating 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 relating to the catalog backup policy.

3 On the master server, for each media identified in step 1b, run the following:

```
bpimport -create_db_info -server server_name -id media_id
```

4 On the master server, run the following:

```
bpimport
```

5 On the master server, for each media identified in step 1b, run the following:

```
bpmedia -unfreeze -m media_id -h server_name
```

Catalog recovery from offline backup

If the catalog was backed up using the offline, cold catalog backup method, use the procedures in this section to recover it. A disaster recovery situation may involve recovering the entire NetBackup environment or only a portion of the catalog.

The NetBackup catalogs contain critical information and must be recovered before any other backups.

Master servers contain the following catalog files:

UNIX:

```
/usr/openv/netbackup/db
/usr/openv/volmgr/database
/usr/openv/var
```

Windows:

```
install_path\NetBackup\db
install_path\NetBackup\var
install_path\Volmgr\database
```

The offline, cold catalog backup will also back up the data contained in the NetBackup relational database NBDB and BMRDB, if applicable. The host and location of these files can be configured. The offline, cold catalog backup will automatically back up this data from the correct host and location.

5.x Media servers have the following NetBackup catalog files:

UNIX:

```
/usr/openv/netbackup/db/media
/usr/openv/volmgr/database
/usr/openv/volmgr/var
```

Windows:

```
install_path\Netbackup\db\media
install_path\Netbackup\var
```

```
    install_path\Volmgr\database
```

To recover the catalog from an offline, cold catalog backup, use the `bprecover` command (you must have root privileges):

UNIX:

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

Windows:

```
    install_path\NetBackup\bin\admincmd\bprecover
```

The topics in this section explain how to use `bprecover` to recover NetBackup catalogs from offline, cold catalog backups. Also, see the description of the `bprecover` command in the *NetBackup Commands* manual.

Note: The following discussions assume that NetBackup has been reinstalled, if required. See "Disk recovery procedures for UNIX" on page 525 or "Disk recovery procedures for Windows" on page 531.

Identifying the most recent catalog backup

Caution: Before you can recover the NetBackup catalogs, you must know which media ID contains their latest backups. Without this media ID, you cannot accurately recover the catalogs and the only option is to import all lost backup records into the NetBackup catalogs. See the *NetBackup Administrator's Guide, Volume I*.

The best way to track media IDs for catalog backups is to configure e-mail notifications with the **Administrator E-mail Address Global** attribute. This attribute causes NetBackup to list the status and media ID in an e-mail to the administrator each time a catalog backup occurs. You can check the e-mail to determine the last media ID used.

If you know the media IDs that were used but are not sure what media contains the most recent backup, use the `-l` option of `bprecover` to list the backups on each media ID. This information includes the date and time that the media was written.

Example 1: List by using a raw device

Assume the catalog backup was written to tape, but the NetBackup media management function was lost, so it cannot control the drive.

Note: UNIX: If the `/dev` file for the device you will use for listing the catalog information is lost in the failure, you must create the special device file path for that device before using `bprecover`. See the *NetBackup Device Configuration Guide* for information on creating this path.

In this case, insert the media in an appropriate drive. Assume the raw-device path is `/dev/rmt/hc2d4` (UNIX) or `\\.\Tape1` (Windows). Then, execute the following command on the NetBackup server that has the drive.

UNIX:

```
bprecover -l -tpath /dev/rmt/hc2d4
Offline Catalog Backup Information from /dev/rmt/hc2d4
Created:      03/30/93 11:31:34
Server:       bphost
Block size:   32768
        Path
        ----
IMAGE1 /usr/openv/netbackup/db
IMAGE2 /usr/openv/volmgr/database
IMAGE3 /usr/openv/var
```

Windows:

```
bprecover -l -tpath \\.\Tape1
Offline Catalog Backup Information from \\.\Tape1

Created:      03/31/97 11:31:34
Server:       bphost
Block Size:   32768

         Path
         ----
IMAGE1 D:\apps\VERITAS\NetBackup\db
IMAGE2 D:\apps\VERITAS\Volmgr\database
```

Example 2: List by using a media and device management controlled drive

UNIX:

Assume Media and Device Management is intact and the backup was written to an 8mm tape with media ID JBL29. Insert the tape into an appropriate drive. Then, execute the following `bprecover` command on the NetBackup server that has the drive (the Media Manager device daemon, `ltid`, must be active).

```
bprecover -l -m JBL29 -d 8mm
Offline Catalog Backup Information from JBL29
Created:      04/02/93 05:50:51
Server:       bphost
Block size:   32768
        Path
        ----
IMAGE1 /usr/openv/netbackup/db
IMAGE2 /usr/openv/volmgr/database
IMAGE3 /usr/openv/var
```

Windows:

Assume Media and Device Management part of the catalogs is intact and the backup was to a dlt tape with media ID 000001. Insert the tape into an appropriate drive. Then, execute the following `bprecover` command on the NetBackup server that has the drive (the NetBackup Device Manager Service must be active).

```
bprecover -l -m 000001 -d dlt
Offline Catalog Backup Information from 000001

Created:      03/31/97 05:50:51
Server:       bphost
Block size:   32768

          Path
          ----
IMAGE1 D:\apps\VERITAS\Netbackup\db
IMAGE2 D:\apps\VERITAS\Volmgr\database
IMAGE3 D:\apps\VERITAS\NetBackup\var
```

Example 3: List disk path

UNIX:

Assume the catalog backup was done to disk path `/disk1/bpbackup` and this disk has not failed. Assuming NetBackup is installed and operating, execute the following `bprecover` command to list the backup information.

```
bprecover -l -dpath /usr/nb_datua/catalog/data/data1
Offline Catalog Backup Information from
/usr/nbu_data/catalog/data/data1

Created:      04/18/05 10:24:29
Server:       nocturna
            Path
            ----
IMAGE1      nocturna:/usr/openv/netbackup/db
IMAGE2      nocturna:/usr/openv/volmgr/database
IMAGE3      nocturna:/usr/openv/var
IMAGE4      clearwater:/usr/openv/netbackup/db
IMAGE5      clearwater:/usr/openv/volmgr/database
IMAGE6      clearwater:/usr/openv/var
IMAGE7      nocturna:/usr/openv/db/data/NBDB.db
IMAGE8      nocturna:/usr/openv/db/data/EMM_DATA.db
IMAGE9      nocturna:/usr/openv/db/data/EMM_INDEX.db
IMAGE10     nocturna:/usr/openv/db/data/vxdbms.conf
IMAGE11     nocturna:/usr/openv/var/global/server.conf
```

```
   IMAGE12     nocturna:/usr/openv/var/global/databases.conf
```

Windows:

Assume the catalog backup was done to disk path `D:\apps\dbbackup` and this disk has not failed. Execute the following `bprecover` command to list the backup information.

```
bprecover -l -dpath D:\apps\dbbackup
Offline Catalog Backup Information from D:\apps\dbbackup

Created:      03/31/97 11:31:34
Server:       bphost
Block size:   32768

         Path
         ----
IMAGE1 D:\apps\VERITAS\NetBackup\db
IMAGE2 D:\apps\VERITAS\NetBackup\var
IMAGE3 D:\apps\VERITAS\Volmgr\database
```

Example 4: Media server

UNIX:

Assume the master server is a UNIX system with no tape drives and the media server is a supported Windows system with a 4mm tape drive. The catalog backup was written to the 4mm tape drive on the Windows media server.

Here, we mount the media in the appropriate drive (assume the raw device path is `\\.\Tape0`) and execute the following `bprecover` command on the media server.

```
bprecover -l -tpath \\.\Tape0
Offline Catalog Backup Information from \\.\Tape0

Created:      03/31/97 11:31:34
Server:       nbmedia
Block Size:   32768

         Path
         ----
IMAGE1 nbmaster:/usr/openv/netbackup/db
IMAGE2 nbmaster:/usr/openv/volmgr/database
IMAGE3 nbmaster:/usr/openv/var
IMAGE4 nbmedia:C:\VERITAS\NetBackup\db\media
IMAGE5 nbmedia:C:\VERITAS\NetBackup\var
IMAGE6 nbmedia:C:\VERITAS\Volmgr\database
```

NetBackup catalog recovery procedures

The following procedures explain how to recover the NetBackup catalogs from an offline, cold catalog backup when all or part of the catalogs are lost. The method required to recover the catalogs depends on the following factors:

- The type of media containing the backup of the NetBackup catalogs (tape, optical, or magnetic disk).
- Whether all or only some of the catalogs need to be recovered.

Before starting

- The host name of the master and EMM servers become an integral part of the NetBackup catalog and as such, part of the catalog backup information. During any catalog recovery procedure, the same host name (either short or fully qualified) that was used for the catalog backups must be used during catalog recovery.
- Reinstall the NetBackup software (if necessary) as explained in the appropriate server or client disk recovery section of this chapter.
- UNIX: If you had created symbolic links to the catalog locations, be sure to manually recreate those links before starting the recovery.
- If you have used the `nbdb_move` command to relocate portions of the NetBackup relational database, be sure to recreate these locations.
- Find the tape that has the latest catalog backups.
- Ensure that the disk where you are restoring the catalogs contains the directory where the catalogs resided.
  This is required because the `bprecover` command always restores the NetBackup catalogs to the path from which they were backed up (alternate-path restores are not allowed).

Recovering the entire catalog

Use the following procedure to recover the entire catalog by using a disk or tape drive configured under Media and Device Management control.

Note: If this disk has failed, you must resort to backups of this disk that were backed up to another server. If you have not backed up the NetBackup catalogs to another server, you must use the NetBackup Import feature to re-add the image information to the catalogs. See the *NetBackup Administrator's Guide, Volume I,* for instructions.

Note: You must have root (administrative) privileges to perform this procedure.

1 On the master server, do the following.
UNIX:

a. Stop the NetBackup Monitor Service.

   ```
   nbsvcmon -terminate
   ```

b. Stop the NetBackup request daemon `bprd` by using the Terminate Request Daemon command on the `bpadm` **Special Actions** menu.

c. Stop the NetBackup database manager daemon `bpdbm` by entering:

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

d. Stop the Media Manager device daemon (`ltid`) by entering:

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

e. Stop the NetBackup Volume Manager (vmd) by entering:

   ```
   /usr/openv/volmgr/bin/vmctrldbm -t
   ```

Windows:

Stop the following services if they are running, by using the NetBackup Activity Monitor or the Services application in the Windows Control Panel.

- NetBackup Service Monitor service
- NetBackup Request Manager service
- NetBackup Policy Execution Manager service
- NetBackup Device Manager service
- NetBackup Volume Manager service

2 On the media server (if not same host as master server) enter the following.

UNIX:

Enter the following commands in the order shown.

```
/usr/openv/netbackup/bin/nbsvcmon -terminate
/usr/openv/volmgr/bin/stopltid
/usr/openv/volmgr/bin/vmctrldbm -t
```

Windows:

Stop the following services if they are running, by using the NetBackup Activity Monitor or the Services application in the Windows Control Panel.

- NetBackup Service Monitor service
- NetBackup Device Manager service
- NetBackup Volume Manager service

3 TAPE DRIVE: Insert the tape with the catalog backup into an appropriate drive.

If the tape is not in the drive, the Device Monitor displays a mount request when the recovery begins. If this occurs, insert the tape and use the Device Monitor to assign the drive to the request.

4 Run the following to verify that the correct offline catalog backup media is loaded in the drive:

```
bprecover -l -tpath device_path
```

5. On the NetBackup server where the drive for the recovery is attached, execute the appropriate `bprecover` command depending on whether you are using tape or disk:

   ```
   bprecover -r ALL -tpath device_path<tape drive>
   bprecover -r ALL -dpath device_path<disk drive>
   ```

   or one of the following if you want to select which items you want to recover:

   ```
   bprecover -r -tpath device_path<tape drive>
   bprecover -r -dpath device_path<disk drive>
   ```

   and answer `y` to all prompts.

Note: If the device and media for the recovery are configured in NetBackup and you did not enter `stopltid` or `vmctrldbm -t` (UNIX) or stop the Device Manager and Volume Manager services (Windows), you can omit the device path:

```
bprecover -r ALL -m media_ID -d density
```

Example 1

Assume the drive is attached to the NetBackup server you are recovering and the backup is on an 8mm tape that has media ID JBL29. To recover the entire catalog from the tape:

```
bprecover -r ALL -m JBL29 -d 8mm
```

UNIX output: `Recovering shark:/usr/openv/netbackup/db`
Windows output:`Recovering shark:D:\VERITAS\NetBackup\db`

Example 2

If the drive attaches to another NetBackup server, execute `bprecover` on the server where the drive attaches and specify the destination server with the `-dhost` option.

Caution: Use the `dhost` option with EXTREME caution, since it can overwrite existing catalogs on the destination host. If you unintentionally overwrite the wrong catalogs, you can recover by moving existing catalogs to a temporary directory on the destination host.

```
bprecover -r ALL -m JBL29 -d 8mm -dhost server_name
```

UNIX output: `Recover shark:/usr/openv/netbackup/db`
Windows output:`Recover shark:D:\VERITAS\NetBackup\db to host stud`

6. NetBackup will not run scheduled backup jobs until NetBackup is stopped and restarted. Prior to restarting NetBackup, protect media that contains

any backups that were successfully performed after the catalog backup that was just used to recover the catalog. This could include:

- 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 After recovering the catalog, start the following:
UNIX:

- `nbsvcmon` (NetBackup Monitor Service)
- `bprd` (NetBackup request daemon)
- `bpdbm` (NetBackup database manager daemon)
- `ltid` (Media Manager device daemon)
- `vmd` (NetBackup Volume Manager daemon)

Use the following commands (`initbprd` starts `bpdbm` and `ltid` starts `vmd`).

```
/usr/openv/netbackup/bin/initbprd
/usr/openv/volmgr/bin/ltid
```

Windows:

After recovering the catalog, use the NetBackup Activity Monitor or the Services application in the Windows Control Panel to start the following services.

- NetBackup Request Manager Service
- NetBackup Database Manager Service
- NetBackup Device Manager Service
- NetBackup Volume Manager Service

8 On all NetBackup servers: stop and restart all NetBackup daemons/services. If a remote EMM server is being utilized, start NetBackup on it prior to starting NetBackup on the master server. You can use the **Activity Monitor** in the NetBackup Administration Console, or the following commands:

Note: If your configuration includes an EMM server that is separate from the master server, start NetBackup on the EMM server before starting NetBackup on the master server.

UNIX:

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

Windows:

Use the Windows Management Console for Services, or the following:

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

Recovering catalog image files

If the NetBackup relational database catalogs are intact but some or all of the catalog backup images need to be recovered, do the following:

Note: You must have root (administrative) privileges to perform this procedure.

1. Stop daemons/services and insert and verify the media as described under "Recovering the entire catalog" on page 571.
2. On the NetBackup server where the drive for the recovery is attached, execute the `bprecover` command in one of the following ways:
   - To select the catalog images that you want recovered, enter the following:

     ```
     bprecover -r -tpath device_path
     ```

     and answer `y` to the prompts identifying the catalog images to be recovered.
   - If the device and media for the recovery are configured in NetBackup and you did not enter `stopltid` or `vmctrldbm -t` (UNIX) or stop the Device Manager and Volume Manager services (Windows), you can omit the device path and enter `bprecover` as follows:

     ```
     bprecover -r -m media_ID -d density
     ```

     and answer `y` to the prompts identifying the catalog images to be recovered.
   - If you want to recover a specific image and know its image number, enter the following:

     ```
     bprecover -r -tpath image_number
     ```

   Example 1

   Assume you are restoring the catalogs to disk 1 and the 8mm tape has media ID JBL29. To recover the desired NetBackup parts of the catalogs on the tape, execute the following command:

   ```
   bprecover -r -m JBL29 -d 8mm
   ```

Enter `y` for the prompts identifying catalog images or other files you want to restore. For example:

```
Recover nocturna:/usr/openv/netbackup/db y/n (n)? y
Recovering nocturna:/usr/openv/netbackup/db
Recover nocturna:/usr/openv/volmgr/database y/n (n)? y
Recovering nocturna:/usr/openv/volmgr/database
Recover nocturna:/usr/openv/var y/n (n)? y
Recovering nocturna:/usr/openv/var
Recover nocturna:/usr/openv/db/data/NBDB.db y/n (n)? n
```

```
Recover nocturna:/usr/openv/db/data/EMM_DATA.db y/n (n)? n
Recover nocturna:/usr/openv/db/data/vxdbms.conf y/n (n)? n
Recover nocturna:/usr/openv/var/global/server.conf y/n (n)? y
Recovering nocturna:/usr/openv/var/global/server.conf
Recover nocturna:/usr/openv/var/global/databases.conf y/n (n)? y
Recovering nocturna:/usr/openv/var/global/databases.conf
```

Example 2

If the drive attaches to another NetBackup server, execute `bprecover` on the server where the drive attaches and specify the server with the `-dhost` option (see caution below). You will be recovering the NetBackup part of the catalogs from image 1 of the tape.

```
bprecover -r 1 -m JBL29 -d 8mm -dhost server_name
```

Caution: Use the `dhost` option with EXTREME caution, since it can overwrite existing catalogs on the destination host. To permit recovery in case you unintentionally overwrite the wrong catalogs, you can move existing catalogs to a temporary directory on the destination host.

---

3 NetBackup will not run scheduled backup jobs until NetBackup is stopped and restarted. Prior to restarting NetBackup, protect media that contains any backups that were successfully performed after the catalog backup that was just used to recover the catalog. This could include:

- importing the backups from the backup media into the catalog
- write protecting the media
- ejecting the media and setting it aside
- freezing the media

4 On all NetBackup servers: stop and restart all NetBackup daemons/services. You can use the **Activity Monitor** in the NetBackup Administration Console, or the following.

Note: If your configuration includes an EMM server that is separate from the master server, start NetBackup on the EMM server before starting NetBackup on the master server.

UNIX:

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

`Windows:`

Use the Windows Management Console for Services, or the following:

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

Recovering NetBackup relational database files

If the NetBackup relational database files need to be recovered, do the following. These files are listed under "Files Not Recovered by Recovery of Catalog Image Files" on page 551.

Note: If the configuration was lost for the device that you plan to use for the recovery, reinstall the device as explained in your operating system documentation.

Note: This procedure is intended to be used when the NBDB database has been corrupted and a temporary database must be created to restore from the catalog backup. However, if the NBDB database is available and the Sybase ASA server is running, then skip steps 1-6 and start the following procedure on step 7 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.

---

1. If NetBackup is running, stop it.

   UNIX:

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

   Windows:

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

2. Change databases.cnf so Sybase ASA does not attempt to automatically start them when the server is started.

   UNIX:

   ```
   /usr/openv/db/bin/nbdb_admin -auto_start NONE
   ```

   Windows:

   ```
   install_path\VERITAS\NetBackup\bin\nbdb_admin -auto_start NONE
   ```

3. Start the Sybase ASA server.

   UNIX:

   ```
   /usr/openv/netbackup/bin/nbdbms_start_stop start
   ```

   Windows:

   ```
   install_path\NetBackup\bin\bpup -e ASANYs_VERITAS_NB
   ```

4. **Re-create an empty database.**

   UNIX:

   ```
   /usr/openv/db/bin/create_nbdb -drop
   ```

   Windows:

```
install_path\Netbackup\bin\create_nbdb -db_server
VERITAS_NB_servername -drop
```

5 Stop and restart NetBackup.

UNIX:

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

Windows:

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

6 Run `tpext` by entering the following command:

UNIX:

```
/usr/openv/volmgr/bin/tpext
```

Windows:

```
install_path\Volmgr\bin\tpext
```

7 If you have used the nbdb_move utility to relocate NetBackup database files, re-create the directories where the files were located at the time of the catalog backup. The default location is:

UNIX:

```
/usr/openv/db/data
```

Windows:

```
install_path\NetBackupDB\data
```

8 Configure the necessary recovery device in NetBackup.

9 Make available to NetBackup the media that contains the catalog backup. Use the appropriate robtest utility, or load the media in the standalone drive.

10 On the master server, do the following.

UNIX:

Enter the following commands in the order shown.

```
/usr/openv/netbackup/bin/nbsvcmon -terminate
/usr/openv/netbackup/bin/bpadm <to stop the bprd service>
/usr/openv/netbackup/bin/bpdbm -terminate
/usr/openv/volmgr/bin/stopltid
/usr/openv/volmgr/bin/vmctrldbm -t
```

Windows:

Use the NetBackup Activity Monitor or the Services application in the Windows Control Panel to stop the following services:

- Service Monitor
- Policy Execution Manager
- Request Manager
- Device Manager
- Volume Manager

11 Enter the following:

UNIX:

```
/usr/openv/netbackup/bin/bprecover -r -tpath device_path
```

Windows:

```
install_path\NetBackup\bin\admincmd\bprecover -r -tpath
device_path
```

Note: Select only the NBDB.db, EMM_DATA.db, EMM_INDEX.db, NBDB.log, vxdbms.conf catalog, server.conf, and databases.conf catalog components to restore. If BMRDB is also on the server, select the BMRDB database files as well.

12 Stop and restart NetBackup.

UNIX:

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

Windows:

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

If a remote EMM server is being utilized, start NetBackup on it prior to starting NetBackup on the master server.

Recovering catalogs from an NDMP-attached tape drive

If the latest NetBackup catalog backup is on a tape that is directly attached to a Network Data Management Protocol (NDMP) host and the NetBackup catalog files are lost, you must recover the catalog from the tape drive attached to the NDMP host.

The procedure for recovering the catalog from an NDMP-attached tape drive is the same as for recovering the catalog from any other tape device. Use the Device Configuration Wizard to configure the NDMP-attached tape drive. For help with this wizard, refer to the *NetBackup for NDMP Guide*.

Note: You must have root (administrative) privileges to perform this procedure.

If you do not use the Device Configuration Wizard, there are a few configuration items that you need to pay attention to:

- Authorize access to the NDMP host by entering the following command:

  ```
  install_path\Volmgr\bin\tpconfig -add -nh ndmp_host -user_id
  username
  ```

  For more information on authorizing access to the NDMP host, refer to the *NetBackup for NDMP System Administrator's Guide* or the man page for `tpconfig`.

- If you are configuring the tape drive as a standalone drive, and you are using the `-tpath` option on the `bprecover` command, include the NDMP host in the `tpath` as in the following:

  ```
  bprecover -r all -tpath ndmp_host:tape_device_name
  ```

For examples of tape device names for particular NAS vendors, refer to the Veritas document on NAS appliance information. For instructions on accessing this document, refer to “NDMP Information on the Web” in the *NetBackup for NDMP System Administrator’s Guide*.

Recovering NetBackup access management components

If you have configured NetBackup Access Control (NBAC), you can configure the offline, cold catalog backup to also back up your NetBackup authentication and authorization data (see Access Management in the *NetBackup Security and Encryption Guide*).

Both the Operate and Configure permission sets are required on the catalog object in order to successfully back up and recover NBAC authentication and authorization data.

To recover the NetBackup catalog from an offline catalog backup when NetBackup Access Control is configured:

1. Shut down authentication and authorization services/daemons.
2. Recover the NetBackup catalog from the cold backup using the `bprecover` command. No special parameters are required. VxSS data will be copied back to the hosts from which it was backed up.

Note: If the master server is a UNIX machine and the NetBackup master server configuration file (`/usr/openv/netbackup/bp.conf`) was included in the cold catalog backup, do not recover it at this time.

3. Start up authentication and authorization services/daemons.
4. Configure NetBackup to use NBAC.

Note: If the master server is a UNIX machine and the NetBackup master server configuration file (`/usr/openv/netbackup/bp.conf`) was included in the cold catalog backup, you can configure NetBackup to use NBAC by recovering the configuration file, rather than by configuring NetBackup to use NBAC via the user interface.

5. Restart NetBackup.

5.x media server catalog recovery

A 5.x media server's catalog backup contains catalog paths that include catalog information that must be restored as part of a disaster recovery.

1. Install the same version of NetBackup 5.x software and patches.
2. Create identical catalog directory paths or locations that were in place at the time of the catalog backup.
3. Do one of the following:
   - **Offline, Cold Catalog Backup Recovery** – Beyond ensuring that the 5.x media server catalog paths are configured and part of an offline backup, there are no additional steps required to recover a 5.x media server catalog from an offline catalog backup. The 5.x media server catalog paths are recovered just like 6.5 media server catalog paths.
   - **Online, Hot Catalog Backup Recovery** – Recovery of a 5.x media server catalog from an online catalog backup requires an additional command be run after the completion of the online catalog recovery. After the successful completion of either the Catalog Recovery wizard or the `bprecover -wizard` command, run the following command line to recover the 5.x media server catalogs.

     ```
     bprecover -r ALL -5x -p <policy name>
     ```

     The following is an example of the output generated:

```
Offline Catalog Backup Information from 0087L2
Created: 07/14/05 18:22:23
Server: stud
Block size: 32768
Path
----
IMAGE1 stud:C:\Program Files\VERITAS\NetBackup\db
IMAGE2 stud:C:\Program Files\VERITAS\Volmgr\database
IMAGE3 stud:C:\Program Files\VERITAS\NetBackup\var\auth
IMAGE4 stud:C:\Program Files\VERITAS\NetBackup\var\global
IMAGE5 stud:C:\Program Files\VERITAS\NetBackup\var\license.txt
IMAGE6 yellowcat:/usr/openv/netbackup/db
IMAGE7 yellowcat:/usr/openv/volmgr/database
IMAGE8 yellowcat:/usr/openv/netbackup/bp.conf
IMAGE9 yellowcat:/usr/openv/var/auth
IMAGE10 yellowcat:/usr/openv/var/vxss
IMAGE11 yellowcat:/usr/openv/var/license.txt
IMAGE12 stud:C:\Program Files\VERITAS\NetBackupDB\data\NBDB.db
IMAGE13 stud:C:\Program Files\VERITAS\NetBackupDB\data\EMM_DATA.db
IMAGE14 stud:C:\Program Files\VERITAS\NetBackupDB\data\vxdbms.conf
IMAGE15 stud:C:\Program Files\VERITAS\NetbackupDB\conf\server.conf
IMAGE16 stud:C:\Program
Files\VERITAS\NetbackupDB\conf\databases.conf
IMAGE17 stud:C:\Program Files\VERITAS\NetBackupDB\data\NBDB.log
```

```
C:\Program Files\VERITAS\NetBackup\bin\admincmd>bprecover -r -m
0087L2 -d
hcart2

Recover stud:C:\Program Files\VERITAS\NetBackup\db y/n (n)? y
Recovering
stud:C:\Program Files\VERITAS\NetBackup\db Recover stud:C:\Program
Files\VERITAS\Volmgr\database y/n (n)? y Recovering stud:C:\Program
Files\VERITAS\Volmgr\database Recover stud:C:\Program
Files\VERITAS\NetBackup\var\auth y/n (n)? y Recovering
stud:C:\Program
Files\VERITAS\NetBackup\var\auth Recover stud:C:\Program
Files\VERITAS\NetBackup\var\global y/n (n)? y Recovering
stud:C:\Program
Files\VERITAS\NetBackup\var\global
Recover stud:C:\Program Files\VERITAS\NetBackup\var\license.txt y/n
(n)? y
Recovering stud:C:\Program Files\VERITAS\NetBackup\var\license.txt
Recover yellowcat:/usr/openv/netbackup/db y/n (n)? y
Recovering yellowcat:/usr/openv/netbackup/db
Recover yellowcat:/usr/openv/volmgr/database y/n (n)? y Recovering
yellowcat:/usr/openv/volmgr/database
Recover yellowcat:/usr/openv/netbackup/bp.conf y/n (n)? y Recovering
yellowcat:/usr/openv/netbackup/bp.conf
Recover yellowcat:/usr/openv/var/auth y/n (n)? y
Recovering yellowcat:/usr/openv/var/auth
Recover yellowcat:/usr/openv/var/vxss y/n (n)? y
Recovering yellowcat:/usr/openv/var/vxss
Recover yellowcat:/usr/openv/var/license.txt y/n (n)? y Recovering
yellowcat:/usr/openv/var/license.txt

The following files are normally recovered as a group.
Use caution when recovering individual files only.
If the main system database file (NBDB.db) is chosen,
the remaining database files are recovered by default.

Recover stud:C:\Program Files\VERITAS\NetBackupDB\data\NBDB.db y/n
(n)? y
Recovering stud:C:\Program Files\VERITAS\NetBackupDB\data\NBDB.db
Recover stud:C:\Program Files\VERITAS\NetBackupDB\data\EMM_DATA.db
y/n (y)? y
Recovering stud:C:\Program
Files\VERITAS\NetBackupDB\data\EMM_DATA.db
Recover stud:C:\Program Files\VERITAS\NetBackupDB\data\vxdbms.conf
y/n (y)? y
Recovering stud:C:\Program
Files\VERITAS\NetBackupDB\data\vxdbms.conf
Recover stud:C:\Program Files\VERITAS\NetbackupDB\conf\server.conf
y/n (y)? y
Recovering stud:C:\Program
Files\VERITAS\NetbackupDB\conf\server.conf
```

```
Recover stud:C:\Program
Files\VERITAS\NetbackupDB\conf\databases.conf y/n (y)?
y Recovering stud:C:\Program
Files\VERITAS\NetbackupDB\conf\databases.conf
Recover stud:C:\Program Files\VERITAS\NetBackupDB\data\NBDB.log y/n
(y)? y
Recovering stud:C:\Program Files\VERITAS\NetBackupDB\data\NBDB.log
```

Functional overview

This appendix provides a functional overview of NetBackup for both UNIX and Windows. The discussions include descriptions of important services or daemons and programs, and the sequence in which they execute during typical operations. The databases and the directory structure of the installed software are also described.

It is assumed that you are already familiar with the overviews in the first chapter of the *NetBackup Administrator's Guide, Volume I.*

There are two main sections in this appendix:

- Backup and restore functional description
- Media and device management functional description
  This section contains a description of the Shared Storage Option (SSO).

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 functional description

This section explains the operation of NetBackup during backup and restores and contains the following discussions:

- Startup process
- Backup and archive processes
- Restore processes
- NetBackup directories and files
- NetBackup programs and daemons
- NetBackup catalogs

Startup process

When the NetBackup master server boots up, a script automatically starts all services, daemons, and programs required by NetBackup. (The start-up commands 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. See "Media and device management functional description" on page 631 for more details.

For information about SAN client and Fibre Transport startup processes, see the *NetBackup Shared Storage Guide*.

Note: There are no daemons or programs that you must explicitly start. 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.[1]

Note that all NetBackup processes can be started manually by running the following:

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

[1] An NLM is similar to a service; NLM stands for NetWare Loadable Module.

Backup and archive processes

The backup and archive processes vary depending on the type of client. The following explains the basic variations, and also describes the synthetic backup process. There is also a description of how NetBackup operates when backing up its catalogs.

Job scheduling

Starting with NetBackup 6.0, the scheduler process bpsched is replaced by the following new services.

- **nbpem** service (Policy Execution Manager): creates a persistent job worklist, starts each job when it is due (no wakeup interval), and sets a timer for the next due job.
- **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.
- **nbrb** service (Resource Broker): allocates resources in response to requests from nbjm. nbrb acquires physical resources from nbemm (the Enterprise Media Manager service), and 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.

Master server: responsible for running jobs as configured in NetBackup policies. The nbpem and nbjm services run only on the master server.

EMM server: allocates resources for one or more master servers. The EMM server is the repository for all device configuration information. The nbemm and nbrb services run only on the EMM server.

> **nbemm** service: centralizes resource selection. nbemm maintains devices, media, and storage units in a relational database. Prior to NetBackup 6.0, resource selection was handled by bpsched, bptm, ltid, and the robotic device daemons.

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). Once started, these operations are all similar to the extent that the same daemons and programs execute on the server. Each type of backup, however, is started differently.

Three ways to start a backup

- Scheduled backup operations begin when the `nbpem` service detects that a job is due. `nbpem` checks the policy configurations for scheduled client backups that are due.
- Immediate manual backups begin if the administrator chooses the manual backup option in the NetBackup Administration Console or runs the `bpbackup` command with the `-i` option. This causes `bprd` to contact `nbpem`, which then processes the policy, client, and schedule 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 (or the `bpbackup` or `bparchive` commands). This invokes the client's `bpbackup` or `bparchive` program, which sends a request to the request daemon `bprd` on the master server. When `bprd` receives the user request, it contacts `nbpem`, which checks the policy configurations for schedules and by default 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. See the *NetBackup Administrator's Guide, Volume I I,* for a description of the UNIX `BPBACKUP_POLICY` and `BPBACKUP_SCHED` options in bp.conf and the Windows equivalents.

Description of backup

The following steps refer to the diagram "Backup or archive to tape, optical, or disk" on page 591.

Note: PBX must be running in order for NetBackup to operate (PBX is not shown in the diagram). See "Resolving PBX problems" on page 65 for more information on PBX.

1 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:

2 Gets the policy list from bpdbm.

3 Builds a work list of all scheduled jobs.

4 Computes the due time for each job.

5 Sorts the work list in order of due time.

6 Submits to nbjm all jobs that are currently due.

7 Sets a wakeup timer for the next due job.

8 When the job finishes, re-computes the due time of the next job and repeats at step 5.

Next, the job manager service (nbjm) does the following:

9 Issues a single request (with a request ID) to `nbrb`, for all resources required by a job. `nbrb` gets the storage unit, tape drive, and media id information from `nbemm` and allocates client and policy resources. `nbrb` returns to `nbjm` an allocation sequence containing one allocation for each resource (each allocation contains a unique ID). `nbrb` also returns allocation data for the specific resource type. `nbrb` also returns the request ID along with the allocations so that `nbjm` can correlate the response with the right request (and job).

Note that `nbrb` allocates all resources included in a request. If the resources are temporarily unavailable the request will be queued in `nbrb`. If the resource cannot be allocated, `nbrb` fails the request.

10 `nbjm` starts the backup by using the client daemon `bpcd` to start the backup and restore manager `bpbrm`. For normal backup (not snapshots), `nbjm` starts `bpbrm` on the media server, which may or may not be the same system as the master server.

Next, the backup and restore manager (bpbrm) does the following:

11 Starts `bptm`.

12 Starts the actual backup (or archive) by using the client daemon `bpcd` to start the backup and archive program `bpbkar` on the client.

Next, the backup and archive manager (bpbkar) does the following:

13 Sends information about files within the image to `bpbrm`, which directs the file information to the NetBackup file database. The information is sent by means of `bpdbm` on the master server.

14 Transmits the backup image to `bptm`. This is accomplished in one of two ways, depending on the following:

- Whether the media server is backing up itself (`bptm` and `bpbkar` are on the same host).

- Whether the media server is backing up a client that resides on a different host.

If the media server is backing up itself, bpbkar stores the image block-by-block in shared memory on the media server. If the media server is backing up a client on a different host, the bptm process on the server creates a child process of itself. The child receives the image from the client by means of socket communications and then stores the image block-by-block in shared memory on the server.[2]

Next, the backup manager for tape or disk does the following:

15 The bptm or bpdm process on the server takes the image from shared memory and directs it to the storage media.

- If the storage media is tape, bptm requests information for the first media and drive to use, by exchanging information with nbjm. bptm sends mount requests for specific media and drives to the NetBackup Device Manager (ltid), which causes the media to be mounted on the appropriate devices.

  If, during the backup, a tape span is required, bptm again exchanges information with nbjm to release the correct tape and to get another one. nbjm exchanges information with nbrb to accomplish this.

- For SharedDisk, AdvancedDisk, and OpenStorage: bptm requests the volume from nbjm, which passes the request to nbemm to choose the volume and media server to use. nbemm calls nbrmms on the media server that was chosen to mount the volume. If a span is required, the same steps are used to mount the volume as described in the previous bullet.

  For BasicDisk: bpdm writes the images to the path configured in the disk storage unit. The system disk manager controls the actual writing of data.

In the case of an archive, bpbrm deletes the files from the client disk after the files have been successfully backed up.

Next, the job manager service (nbjm) does the following:

16 Receives completion status of the job from bpbrm.

17 Releases resources to nbrb and returns status to nbpem.

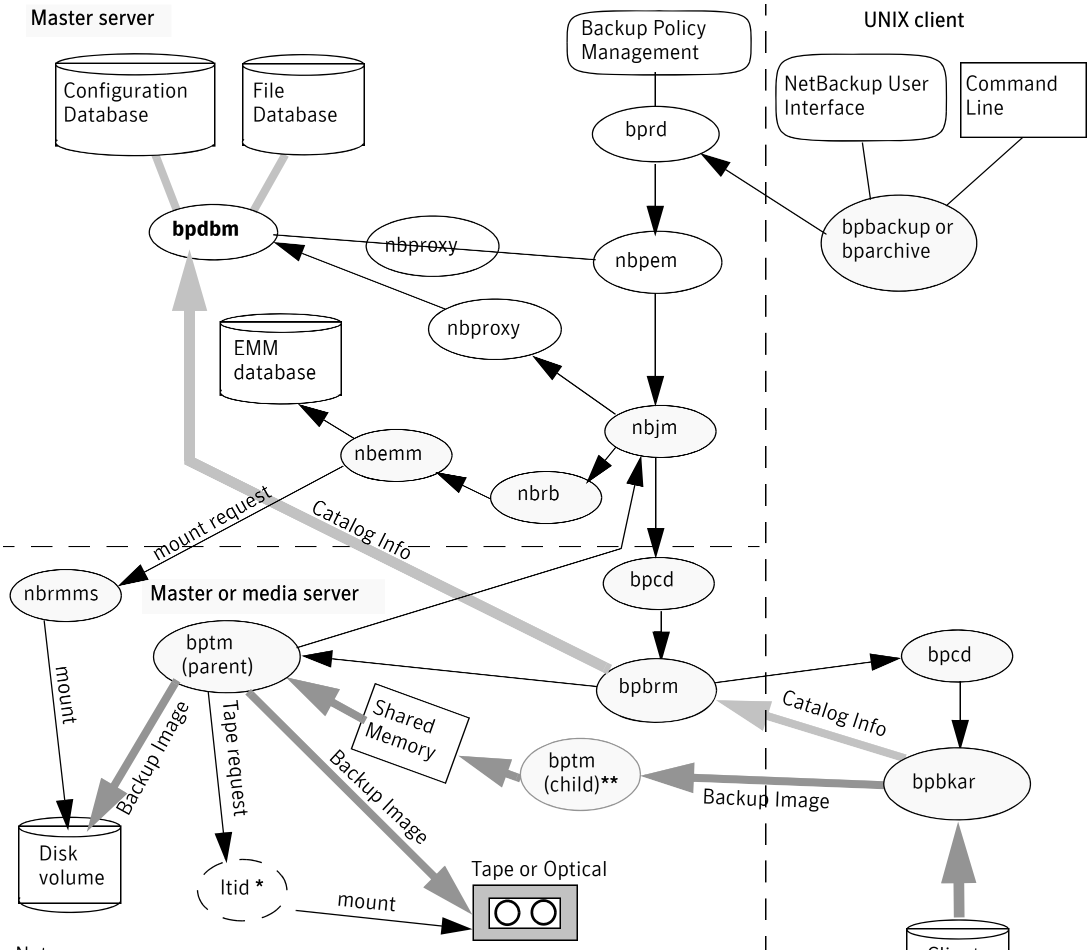
[2] You can use the NOSHM file to force a media server that is backing up itself to create a child process and use socket communications, as though the client is on a different host. For more information on the NOSHM file, see the *NetBackup Backup Planning and Performance Tuning Guide*.

Backup to tape or disk

The overall backup process is shown below.

Note: PBX must be running for NetBackup to operate (PBX is not shown in the diagram). See “Resolving PBX problems” on page 65.

Figure A-1 Backup or archive to tape, optical, or disk



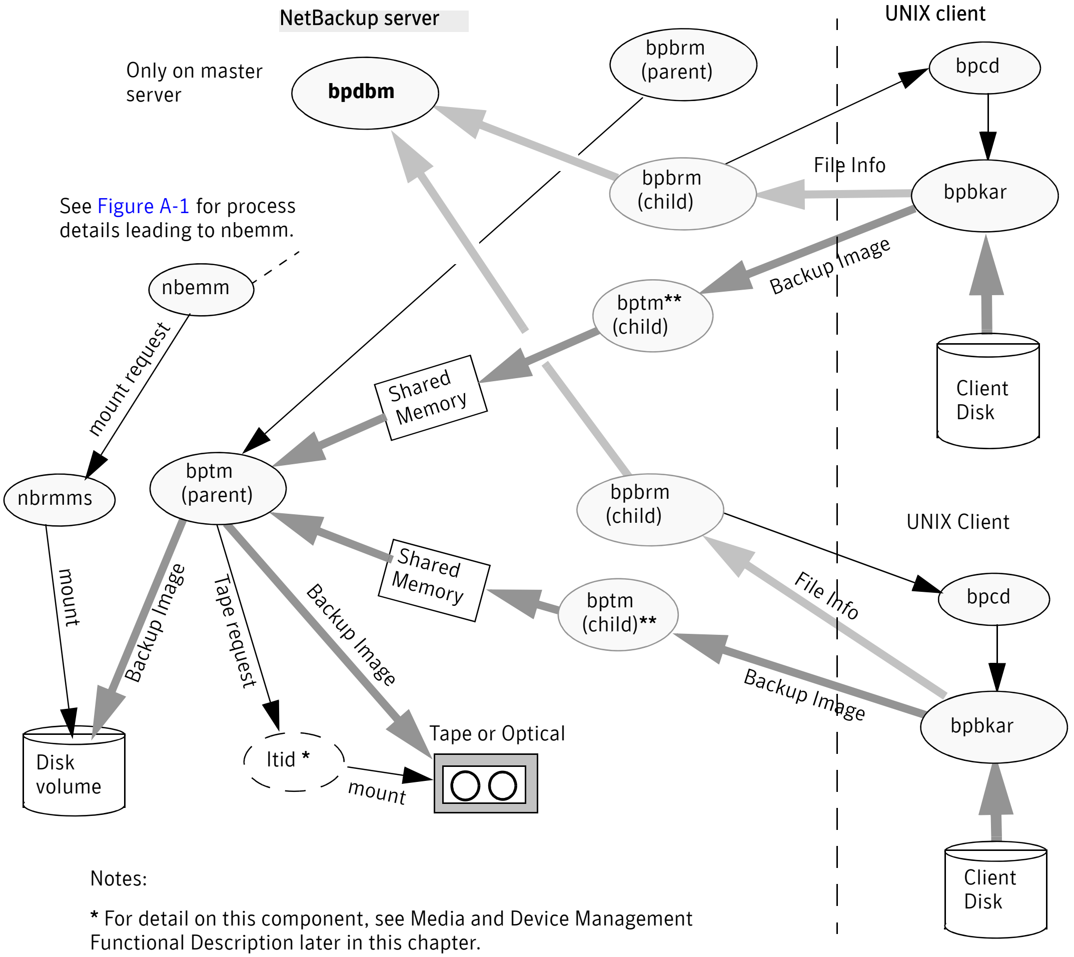
Notes:

* For detail on these components, see the Media and Device Management Functional Description later in this chapter. ltid is for tape backup only.
** If the media server is backing up itself (server and client on same host), there is no bptm child: bpbkar sends the data directly to shared memory.

Backup with multiple data streams

For multiplexed backups, the process is essentially the same except that a separate bpbrm 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 figure “Multiplexed backups example (two streams)” shows multiplexing images from two clients. The other client and server processes are the same as shown in the diagram “Backup or archive to tape, optical, or disk” on page 591. (See the note on PBX on previous page.)

Figure A-2 Multiplexed backups example (two streams)



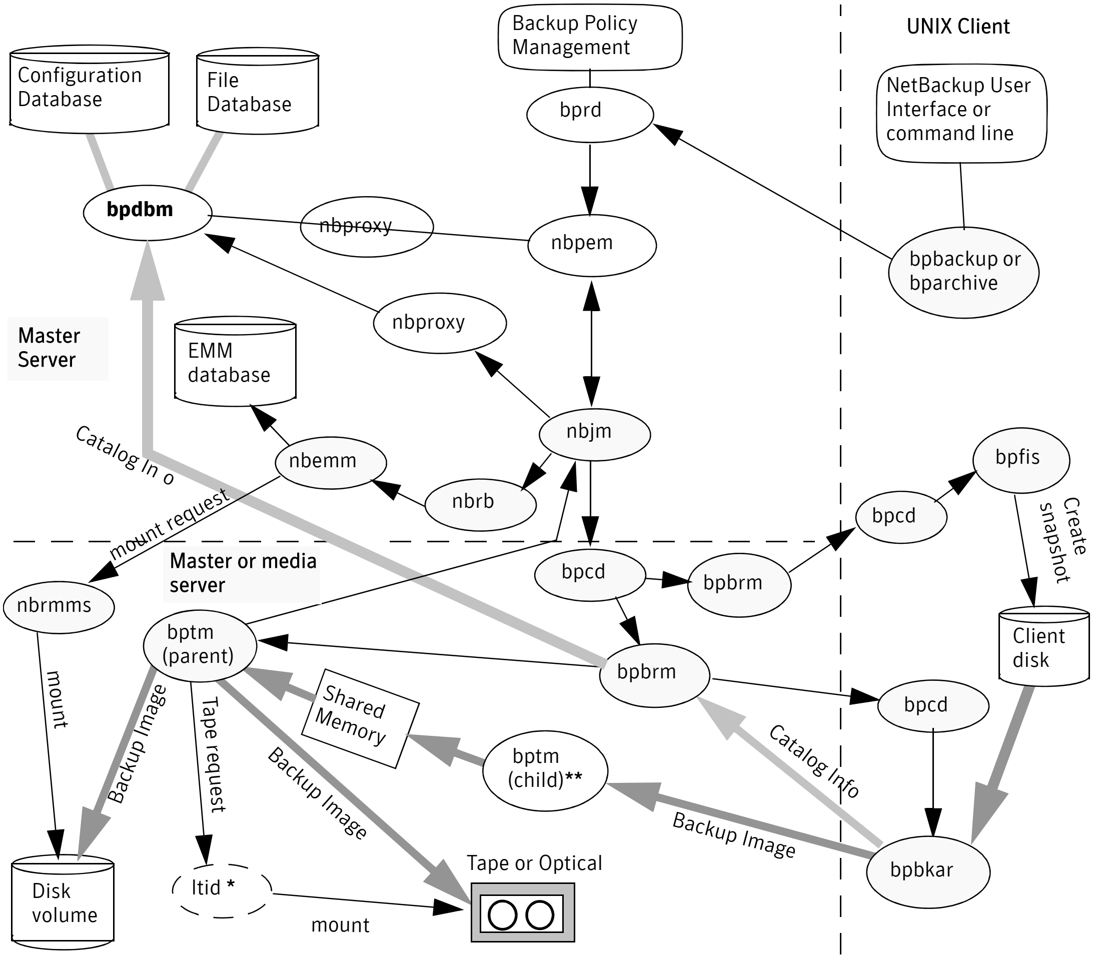
Notes:

* For detail on this component, see 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/Windows open file backups

The overall snapshot backup process is shown below. (See the note on PBX under "Backup to tape or disk" on page 591.)

Figure A-3 Snapshot backup, and Windows open file backup using multiple data streams



Notes:

* For detail on these components, see the Media and Device Management Functional Description later in this chapter.
** If the media server is backing up itself (server and client on same host), there is no bptm child: bpbkar sends the data directly to shared memory.

Description of snapshot backup

With the exception of Windows open file backups that do not use multiple data streams, all snapshots are created by a separate parent job, followed by a child job that backs up the snapshot.

The basic processing steps for snapshot creation and backup are the following (this includes Windows open file backups that employ multiple data streams):

1. The NetBackup master server or primary client initiates the backup, causing the NetBackup request daemon `bprd` to submit a backup request to the Policy Execution Manager `nbpem`. `nbpem` processes the policy configurations.
2. `nbpem` (through `nbjm`) starts a parent job to create the snapshot. This job is separate from the job that will back up the snapshot.
3. `nbjm` starts an instance of `bpbrm` through `bpcd` on the media server, and `bpbrm` starts `bpfis` through `bpcd` on the client.
4. `bpfis` creates a snapshot of the client's data by means of a snapshot method.
5. When finished, `bpfis` 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`.
6. `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.
7. `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.
8. `bpbrm` starts the process `bptm` (parent) on the media server.
9. The next step depends on whether the media server is backing up itself (`bptm` and `bpbkar` are on the same host) or the media server is backing up a client that resides on a different host. If the media server is backing up itself, `bpbkar` stores the snapshot-based image block by block in shared memory on the media server. If the media server is backing up a client that resides on a different host, the `bptm` process 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.
10. The original `bptm` process then takes the backup image from shared memory and sends it to the storage device (disk or tape). For information on how the tape request is issued, refer to "Media and device management process" on page 633.

11 bptm sends backup completion status to bpbrm, which passes it to nbjm.

12 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.

Note: For more information on snapshot backups involving Snapshot Client, refer to 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.

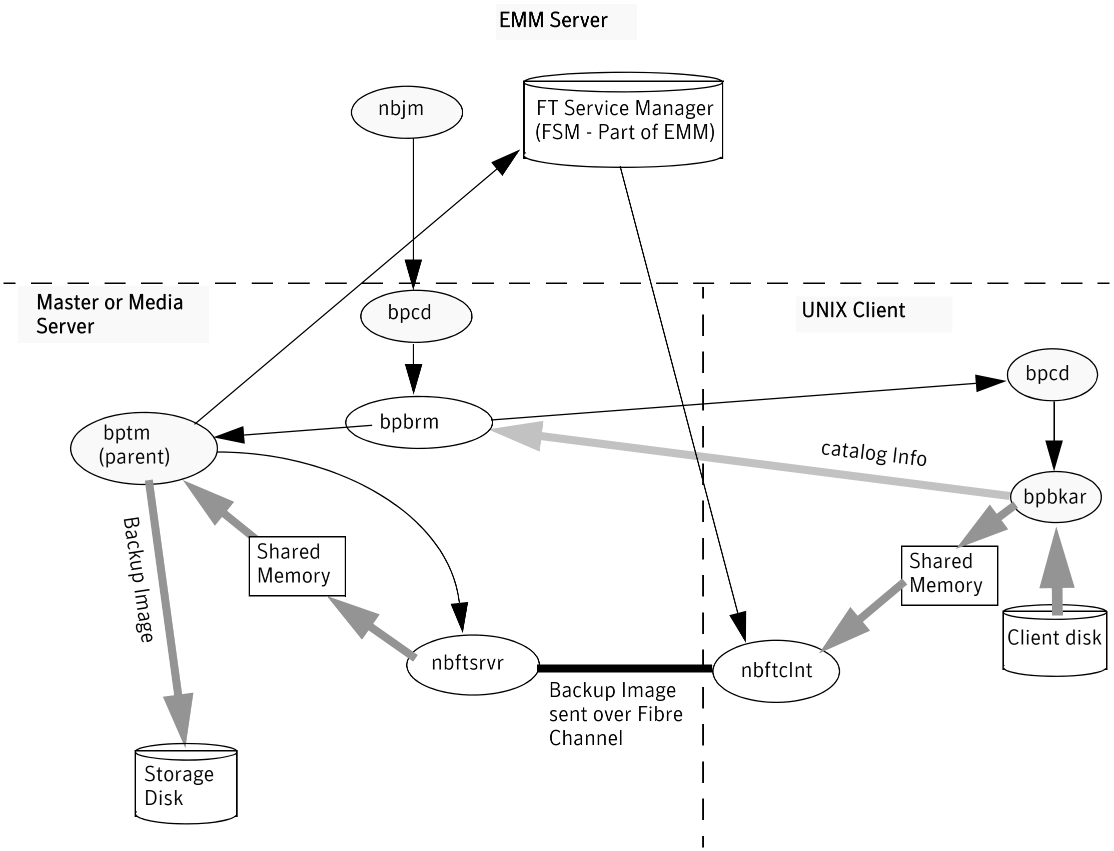
FT Service Manager

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.

Backup process overview

The initial stages of a backup are the same as shown in figures "Backup or archive to tape, optical, or disk" on page 591. The following diagram shows the server and client components that are unique to SAN client backup over Fibre Channel.

Figure A-4 SAN client backup over Fibre Transport



The process flow for a SAN Client backup is as follows. See the first few steps under "Description of backup" on page 588 for the initial actions common to all backups.

1 When 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.

2 nbjm starts the backup by means of the client daemon bpcd, which starts the backup and restore manager bpbrm.

3 bpbrm starts bptm. bptm does the following:

   a Requests SAN Client information from nbjm.

   b Sends a backup request to the FT server process (nbftsrvr).

c 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 (BID).

4 bpbrm starts bpbkar by means of bpcd. bpbkar does the following:

a Reads shared memory information from the BID file (waits for the file to exist and become valid).

b Sends information about files in the image to bpbrm.

c Writes file data to tar, optionally compresses it, then writes the data to the shared buffer.

d When the buffer is full or the job is done, sets buffer flag.

5 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.

6 nbftsrvr waits for data from nbftclnt; the data is written to the shared memory buffer. When the transfer completes, nbftsrvr sets the buffer flag.

7 bptm waits for the shared memory buffer flag to be set, writes data from the shared memory buffer to the storage device, and clears the buffer flag.

8 At the end of the job:

a bpbkar informs bpbrm and bptm that the job is complete.

b bptm sends bpbrm the final status of the data write.

c bptm directs nbftclnt to close the fibre channel connection.

d nbftclnt closes the fibre channel connection and deletes the BID file.

Backups and archives - Windows

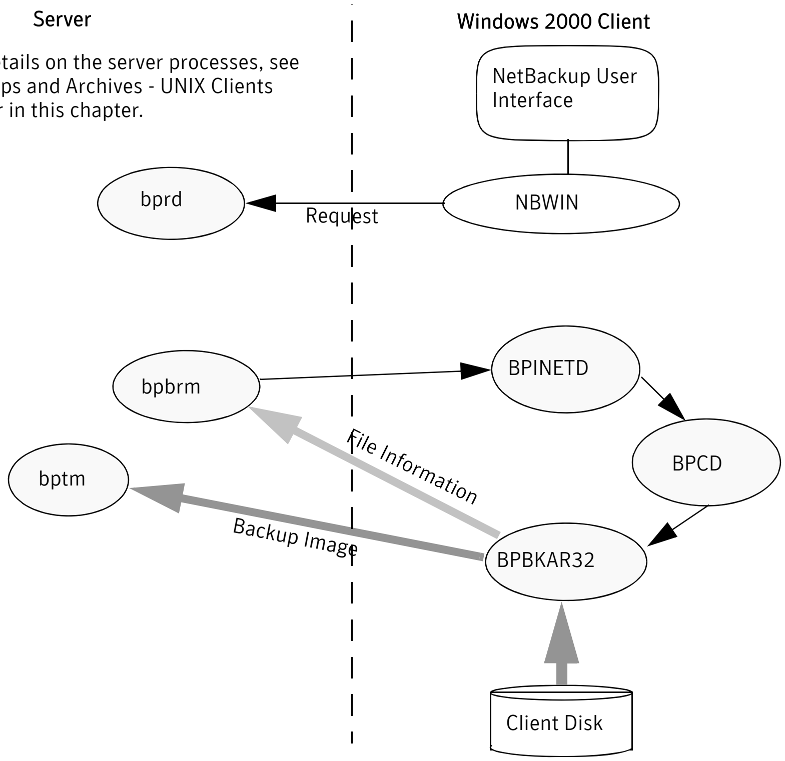
NetBackup supports the same types of operations on Windows clients as it does for UNIX clients.

The next figure shows the Windows client processes. In this figure:

- `NBWIN` is the user interface program on the client. The `bpbackup` and `bparchive` functions 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:

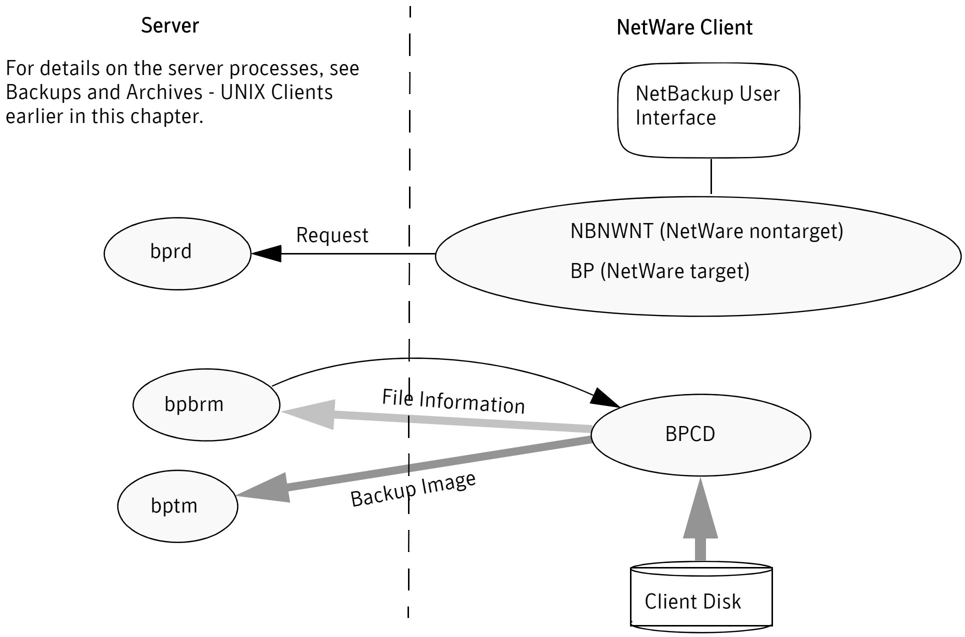
- Raw partition backups are not supported.
- NetBackup for NetWare does not support archiving.

The next figure shows the NetWare client processes. In this figure:

- 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 bpbackup, bparchive, 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


Server
For details on the server processes, see Backups and Archives - UNIX Clients earlier in this chapter.
NetWare Client
NetBackup User Interface
bprd
Request
NBNWNT (NetWare nontarget)
BP (NetWare target)
bpbrm
File Information
BPCD
bptm
Backup Image
Client Disk

Synthetic backups

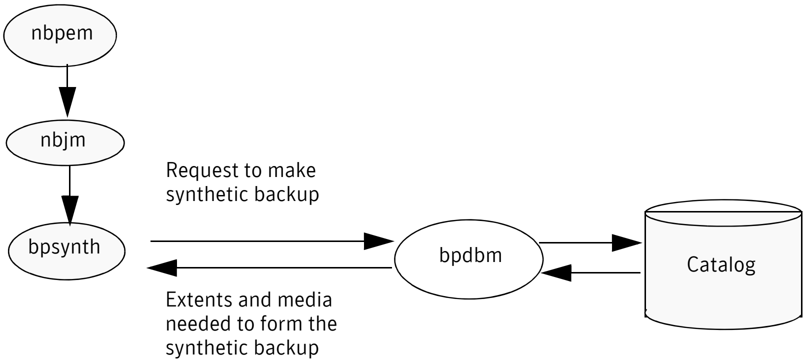
Note: There is no such thing as a synthetic archive.

The term “traditional backup” describes the familiar NetBackup process which 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 using only previously created backup images, called component images.

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 created through the traditional process. The new synthetic full image is a backup of the client that is as current as the last incremental. The synthetic image is created by copying the most current version of each file from the most recent component image containing 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 files that have been deleted from the client file system from appearing in the synthetic backup.

Like a traditional backup, a synthetic backup is typically initiated by nbpem. nbpem submits to nbjm a request to start the synthetic backup job. nbjm starts bpsynth. bpsynth controls the creation of the synthetic backup image and controls the reading of the files needed from the component images. bpsynth executes on the master server. If a directory named bpsynth exists in the debug log directory, additional debug log messages are written to a log file in that directory.

Figure A-7 Synthetic backup -- preparation phase


nbpem
nbjm
bpsynth
Request to make synthetic backup
Extents and media needed to form the synthetic backup
bpdbm
Catalog

bpsynth makes a synthetic image in several phases:

1. Prepare catalog information and extents
2. Obtain resources
3. Copy data
4. Validate the image

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 and 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.

Obtain resources

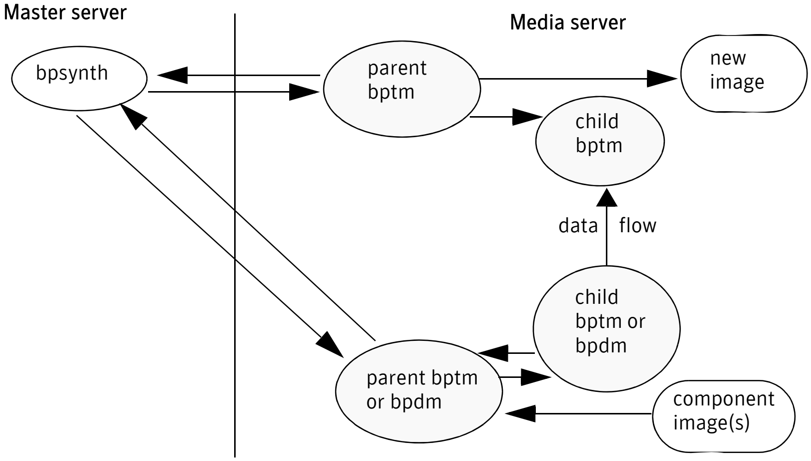
In phase 2, bpsynth obtains write resources (storage unit, drive, and media) for the new image. It also reserves all the read media containing component images and obtains the drive for the first media to be read.

Note: When the component images reside on BasicDisk or NearStore, no resource reservation is done.

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` (for tape) or `bpdm` (for 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 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.

The parent bptm writer process notifies bpsynth when the synthetic image is complete.

Validate the image

In phase 4, the bpsynth process validates the image. The new image is now visible to NetBackup and can be used like any other full or cumulative incremental backup.

Synthetic backup requires:

- That True Image Restore (TIR) with move detection be selected for each component image.
- That the component images are made with NBU 5.0 or later clients, or that they are synthetic images.
- That the component images use the binary catalog format, not the ASCII catalog format as may have been used in 5.x images.

NetBackup catalog backups

Two types of catalog backup are available (these are covered in greater detail in the *NetBackup Administrator's Guide, Volume I*).

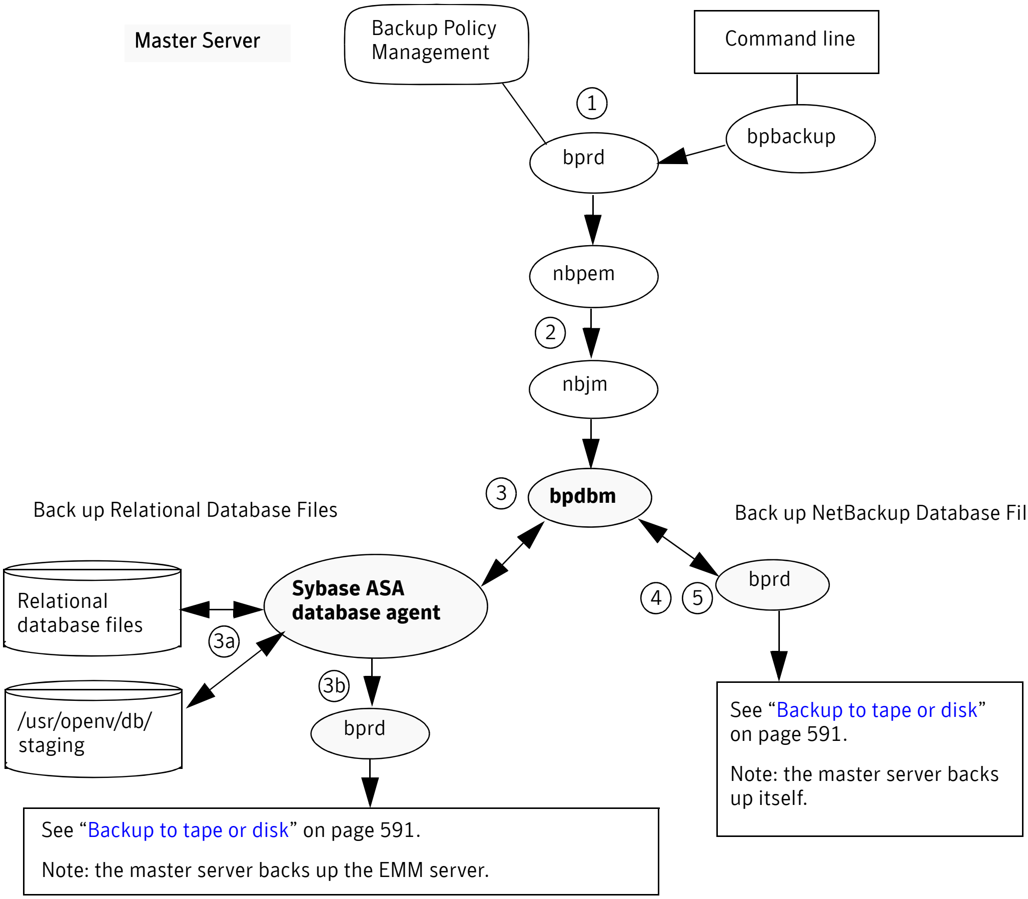
- Online, hot catalog backup. This type of catalog backup is policy-based, with all of the scheduling flexibility of a regular backup policy. This backup type is designed for highly active NetBackup environments where other backup activity is usually taking place. The catalog backup is performed online, meaning that the catalog is not shut down. See "Hot catalog backup process" on page 602 for more details.
- Offline, cold catalog backup. This type of catalog backup is for NetBackup environments in which there are periods when little or no backup activity is occurring. It is considered an offline, cold backup because it should not be run when regular backup activity is taking place. This type of catalog backup must fit on a single tape. See "Cold catalog backup process" on page 605 for more details.

You can use an option in the Administration Console to start a manual backup of the NetBackup catalogs or configure a NetBackup policy to automatically back up its catalogs.

Hot catalog backup process

The hot catalog backup process is shown as follows.

Figure A-9 Hot catalog backup: Overview


Master Server
Backup Policy Management
Command line
1
bpbackup
bprd
nbpem
2
nbjm
3
bpdbm
Back up Relational Database Files
Back up NetBackup Database Files
Relational database files
Sybase ASA database agent
3a
/usr/openv/db/ staging
3b
bprd
4
5
bprd

See "Backup to tape or disk" on page 591.

Note: the master server backs up the EMM server.

See "Backup to tape or disk" on page 591.

Note: the master server backs up 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`).

The steps in a hot catalog backup are as follows:

1. The backup is initiated by either a manual backup or by a catalog backup policy.
2. nbpem submits a parent job to nbjm; nbjm sends a request to bpdbm.
3. bpdbm handles the backup of the relational database files, in two steps:
   - a The Sybase ASA 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.
   - b Once the files are in the staging area, the Sybase ASA database agent backs them up in the same manner as is used for an ordinary backup. For the process, see "Backup to tape or disk" on page 591.
4. If there are any pre-6.0 media servers, NetBackup copies their NetBackup database files to the 6.5 master server.
5. NetBackup backs up the database files that are in `/usr/openv/netbackup/db`, other important NetBackup files, and the pre-6.0 files (if any) that were copied to the master server. For the process, see "Backup to tape or disk" on page 591.
6. NetBackup creates the disaster recovery file, and emails it to the administrator if the email option was selected in the policy.

Logs

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).

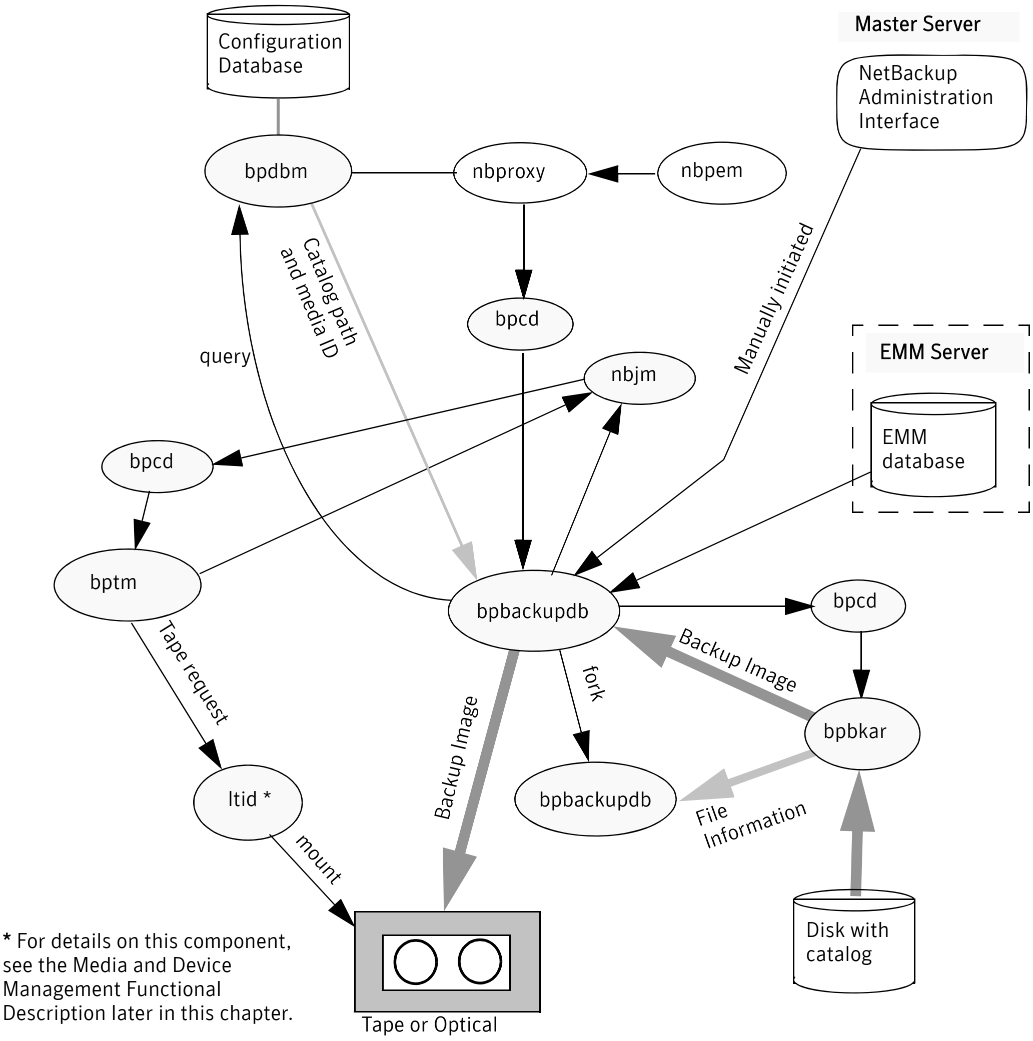
For messages pertaining only to the relational database files, see the progress log file in:

- `/usr/openv/netbackup/logs/user_ops/dbext/logs` (UNIX)
- *`install_path`*`\NetBackup\logs\user_ops\dbext\logs` (Windows)

Cold catalog backup process

The cold catalog backup process is shown below. (See the note on PBX under “Backup to tape or disk” on page 591.)

Figure A-10 Cold catalog backup



* For details on this component, see the Media and Device Management Functional Description later in this chapter.

If configured for a cold catalog backup, nbpem initiates automatic database backup (bpbackupdb) in either of the following cases:

- After a scheduled backup session that creates at least one backup image.
- After a scheduled, user-directed, or manual backup or archive session that creates at least one backup or archive image.

Once started, bpbackupdb does the following:

1 bpbackupdb queries bpdbm for the catalog paths to back up and the media ID to use for the backup. The NetBackup relational database files are included in the list of paths automatically.

2 bpbackupdb suspends nbemm and nbrb, and shuts down the NetBackup relational database, NBDB.

3 bpbackupdb sends a request to nbjm. After getting the specified media resource and drive resource from nbrb, nbjm starts bptm. bptm exchanges information with nbjm to determine the media and drive to load. This information is sent to ltid, which causes the media to be loaded in the specified drive.
The tape and optical manager (bptm) recognizes the request as being for a catalog backup. bptm checks the catalog to ensure that the media ID is not used for regular backups.

4 bpbackupdb starts the actual backup by using bpcd to start the backup/archive program, bpbkar.
If the catalog is on the master server, bpbackupdb starts the backup/archive program bpbkar on the master server. If the catalog is on a media server, bpbackupdb starts bpbkar on the media server.
The bpbkar program transmits file information and the backup image to separate bpbackupdb processes as shown in the figure "Cold catalog backup."

   - The original bpbackupdb process receives the backup image and sends it to the backup device.
   - A second bpbackupdb process checks the file information to ensure that the proper files are being backed up.

5 bpbackupdb resumes nbemm and nbrb, and starts up the NetBackup relational database, NBDB.

Note the following about cold catalog backups:

- The entire catalog backup must fit on a single tape. The bpbackupdb process is unable to span tapes and there is no mechanism for specifying multiple tapes for a NetBackup catalog backup.
- If any part of the catalog backup fails, then NetBackup discards the entire backup. This is done because you must have a backup of *all* the catalogs to be certain that you have a consistent catalog.

- The relational database used by the EMM server and NetBackup Resource Broker is taken offline. No operation that uses nbemm or nbrb is possible during this time, such as most backup and restore operations.
- If the Bare Metal Restore (BMR) option is being used, the relational database used by BMR, BMRDB, is included in the backup and is shut down during the cold catalog backup.

Restore processes

NetBackup restore operations, like backups, can vary according to client type. The following explains the basic variations.

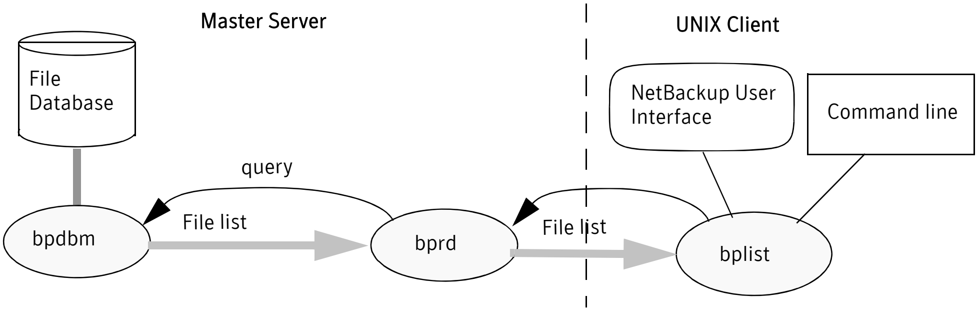
Restores - UNIX clients

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 is used by the NetBackup user interface programs.

`bplist` obtains the file list by sending a query to the request daemon, `bprd`, on the master server (see the graphic below, "List operation - UNIX client"). The request daemon, in turn, queries `bpdbm` for the information and transmits it to `bplist` on the client.

Figure A-11 List operation - UNIX client



With reference to "Restore from tape or optical (UNIX)" on page 609 or "Restore from disk" on page 610, the following are the processing steps in a restore:

1 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/restore manager (`bpbrm`).

Note: To restore Backup Exec images, bpbrm will invoke mtfrd instead of tar on the clients. The server processes are the same as those used for NetBackup restores.

2 If the disk or tape device on which the data resides attaches to the master server, then bprd starts the backup and restore manager on the master server. If the disk or tape unit connects to a media server, bprd starts the backup and restore manager on the media server.

3 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.

4 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 SharedDisk, 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.

5 When the allocation is granted to it, bptm starts retrieving data. bptm stores the image block-by-block in shared memory.

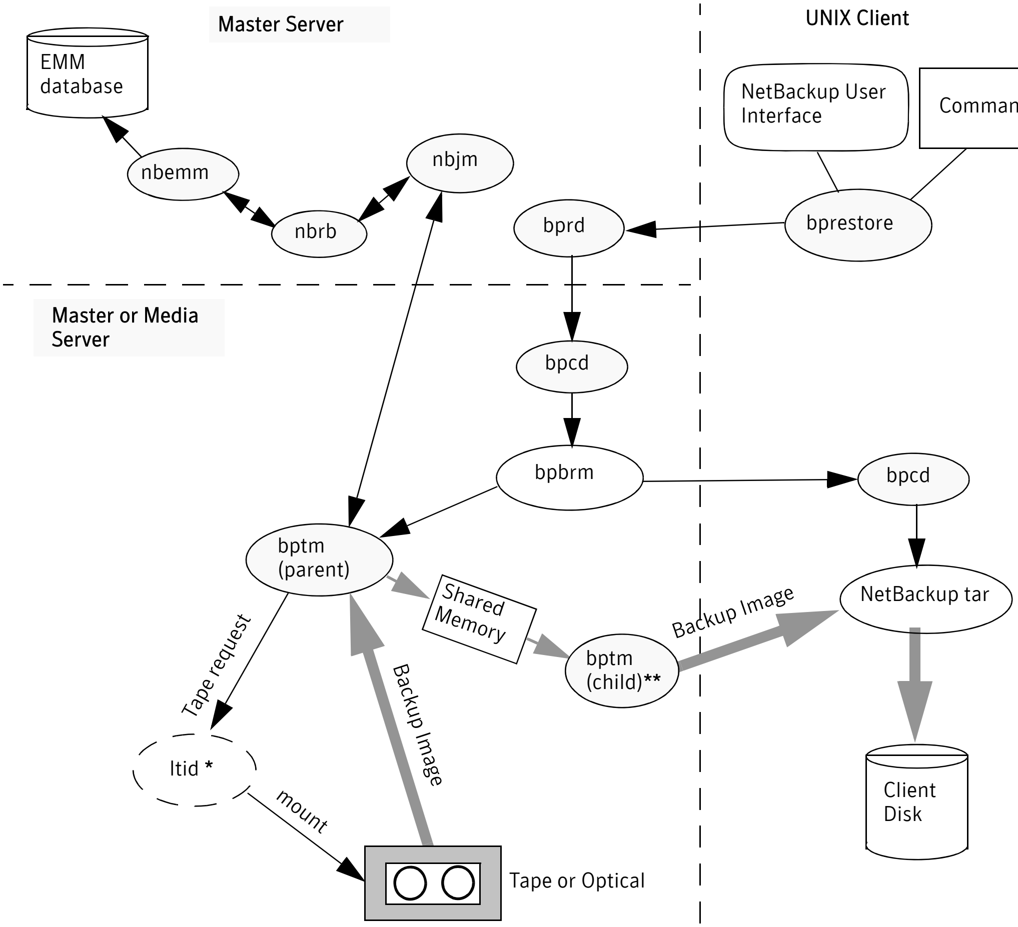
6 bptm directs the image to the client in one of two ways. If the server is restoring itself (server and client are on the same host), tar reads the data directly from shared memory. If the server is restoring a client that resides on a different host, a child bptm process is created which transmits 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.

7 The NetBackup tar program writes the data on the client disk.

Note: PBX must be running for NetBackup to operate (PBX is not shown in the next diagram). See "Resolving PBX problems" on page 65.

Figure A-12 Restore from tape or optical (UNIX)

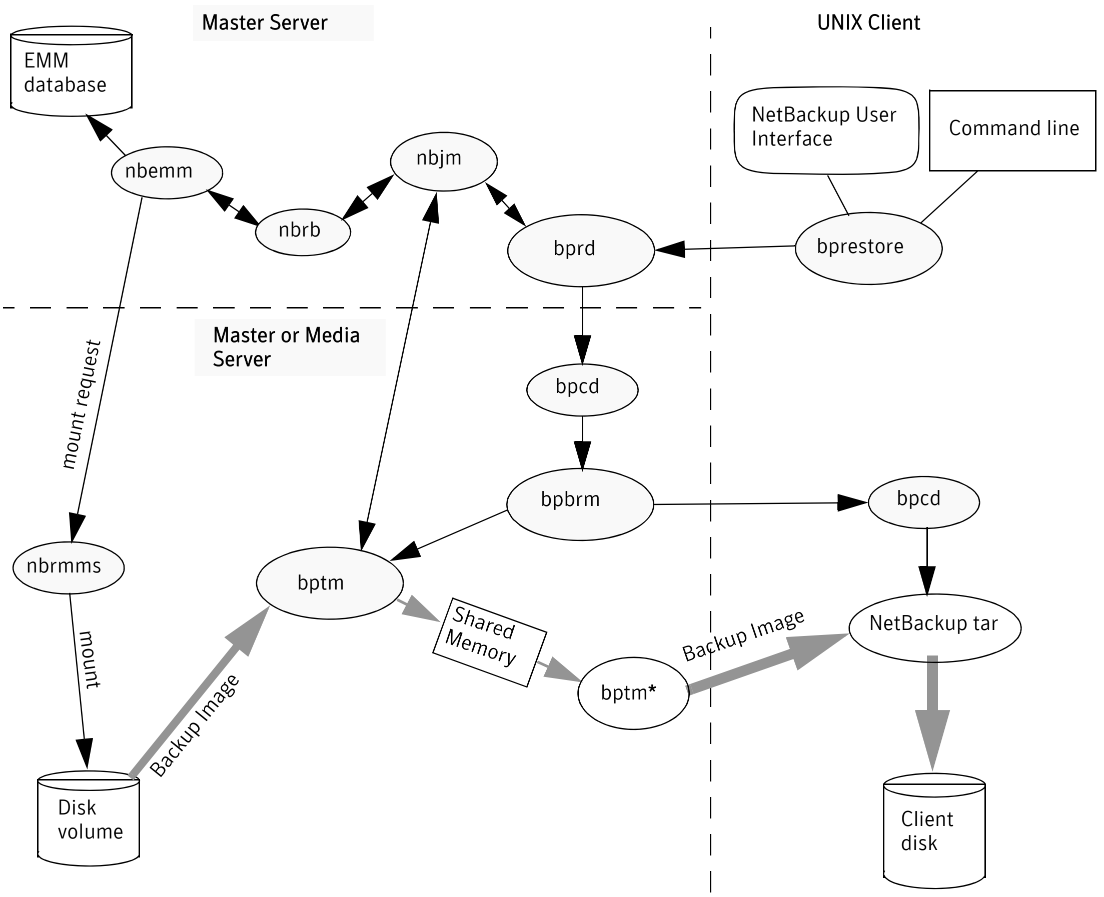


Notes:

* For detail on this component, see Media and Device Management Functional Description later in this chapter.

** 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.

Figure A-13 Restore from disk



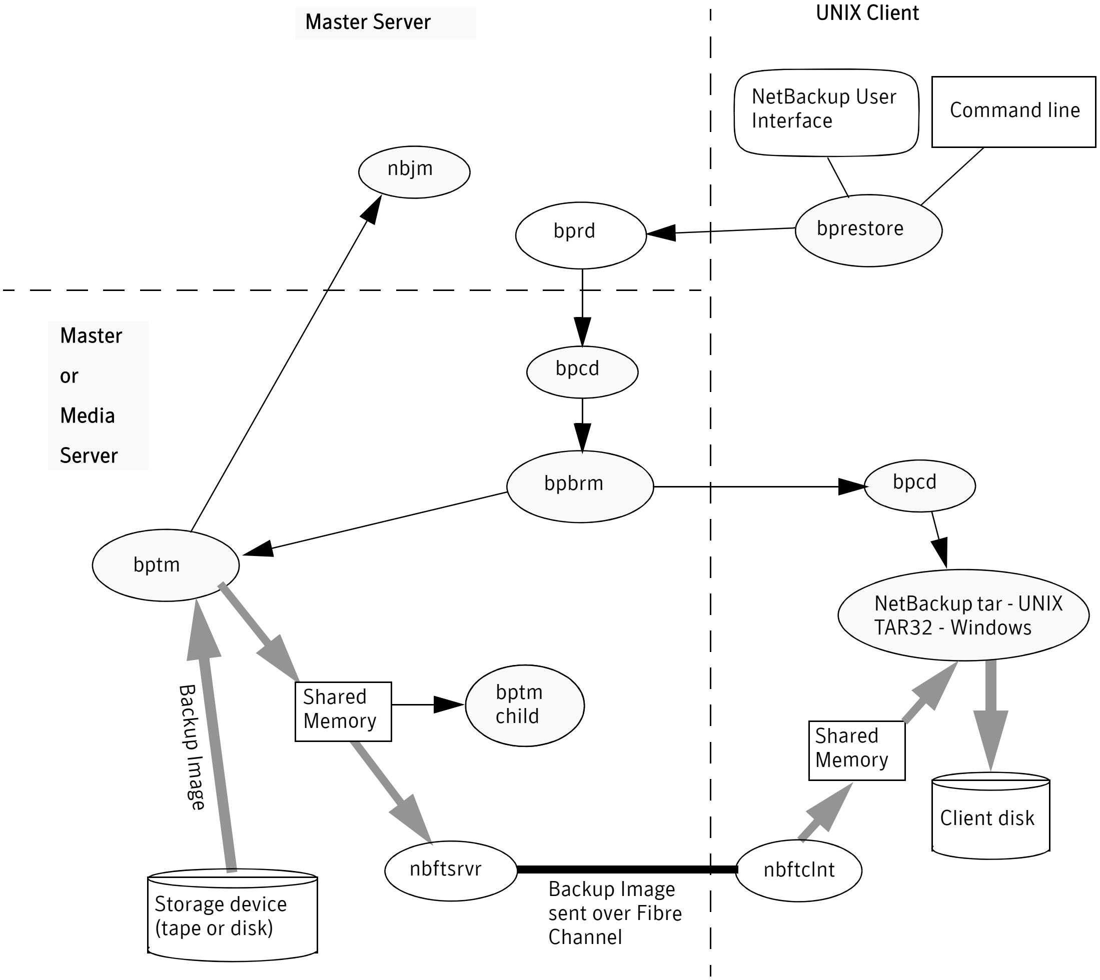
Notes:

* 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.

Restores - SAN client (UNIX or Windows)

The following diagram shows the server and client components involved in a restore of a SAN client over Fibre Channel.

Figure A-14 SAN client restore with Fibre Transport



The process flow for a SAN Client restore is as follows. See the first two steps under “Restores - UNIX clients” on page 607 for the initial actions common to restores.

1 bpbrm starts bptm and provides bptm with the backup ID and the shmfat (shared memory) flag.

2 bptm does the following:

   a Requests SAN Client information from nbjm.

   b Sends a restore request to the FT server process (nbftsrvr).

   c Sends a restore request to the FT Client process on the client (nbftclnt). nbftclnt opens a fibre channel connection to nbftsrvr on the media server, allocates shared memory, and writes shared memory information to the backup ID file (BID).

3 bpbrm starts tar by means of bpcd and provides tar with the backup ID, socket information, and the shmfat (shared memory) flag.

4 bptm does the following:

   a Reads the image from the storage device.

   b Creates a bptm child process, which filters the backup image so that only the files selected for the restore are sent to the client.

   c Writes the image data to the shared buffer on the server.

   d When buffer is full or job is done, sets buffer flag (partial buffers may be sent to the client).

5 tar does the following:

   a Sends status and control information to bpbrm.

   b Reads shared memory information from the local backup ID file (waits for the file to exist and become valid).

   c Waits for the buffer flag that indicates the data is ready to be read.

   d Reads data from the buffer, extracts files and restores them. When the shmfat (shared memory) flag is provided, tar considers the data to be already filtered.

6 The FT Server process nbftsrvr waits for the shared memory buffer flag to be set. nbftsrvr then transfers the image data to the FT Client (nbftclnt) shared memory buffer, and clears the buffer flag.

7 The FT Client (nbftclnt) waits for the data from nbftsrvr and writes the data to the shared memory buffer on the client. nbftclnt then sets the buffer flag.

8 At the end of the job:

   a bptm informs tar and bpbrm that the job is complete.

   b bptm directs nbftclnt to close the fibre channel connection.

   c nbftclnt closes the fibre channel connection and deletes the BID file.

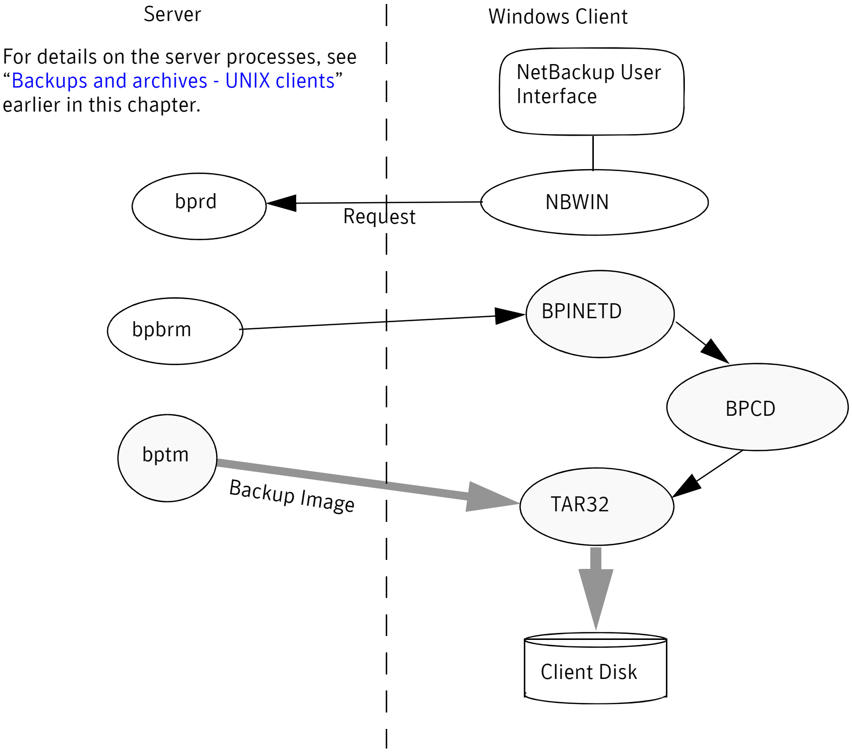
Restores - Windows clients

NetBackup supports the same types of operations on Windows clients as it does for UNIX clients. The next figure shows the client processes involved in these operations.

- NBWIN is the user interface program on the client. The bpbackup and bparchive functions 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 will invoke 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.

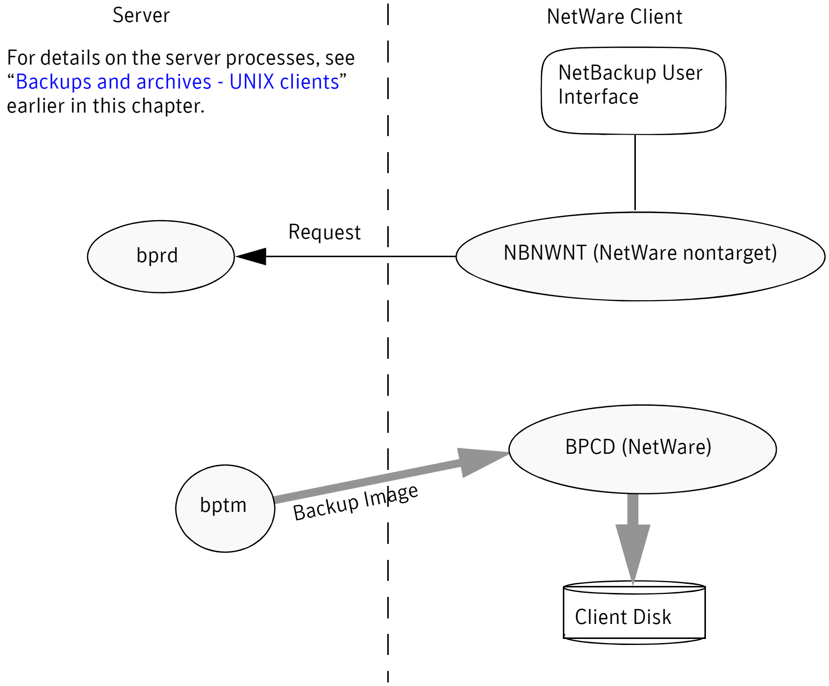


Restores - NetWare clients

NetBackup supports the same types of restore operations on NetWare clients as it does on UNIX clients. The next figure shows the client processes involved in these operations. In this figure:

- The NetWare nontarget user interface program is called `NBNWNT`. The NetWare target user interface program is `BP` on the Netware console. The `bprestore` and `bplist` functions 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.

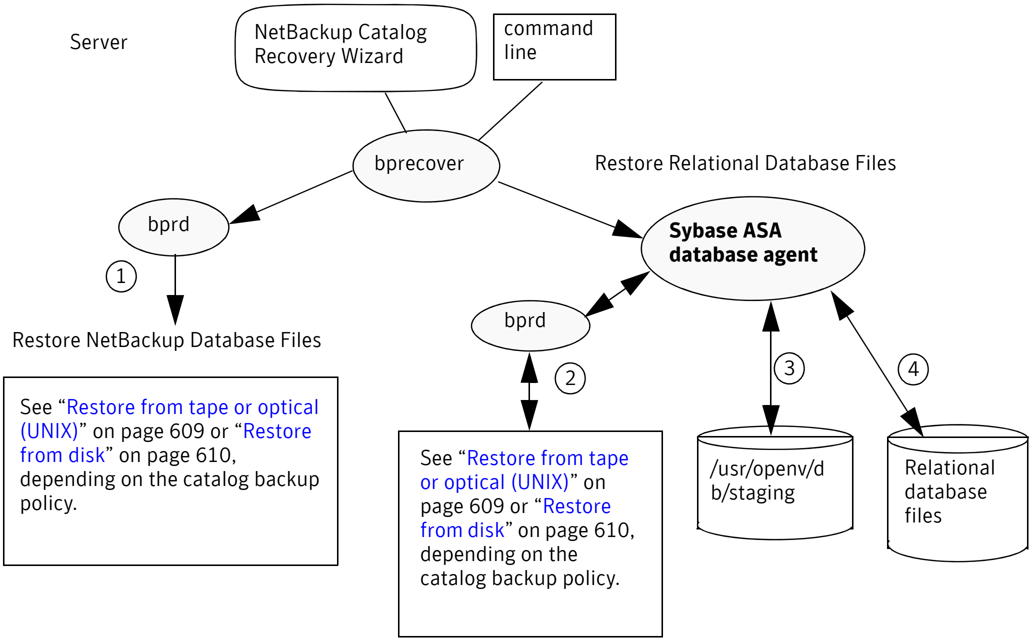
The server processes are the same as described for UNIX.


Server
NetWare Client
For details on the server processes, see "Backups and archives - UNIX clients" earlier in this chapter.
NetBackup User Interface
bprd
Request
NBNWNT (NetWare nontarget)
BPCD (NetWare)
bptm
Backup Image
Client Disk

Restores of catalog backups

A restore of a catalog can be initiated by means of the NetBackup Catalog Recovery Wizard in the Administration Console, or by manual use of the bprecover command. See the "Disaster recovery" chapter for assistance.

Figure A-15 Catalog restore and recovery


Server
NetBackup Catalog Recovery Wizard
command line
bprecover
Restore Relational Database Files
bprd
Sybase ASA database agent
1
Restore NetBackup Database Files
bprd
2
3
4
See "Restore from tape or optical (UNIX)" on page 609 or "Restore from disk" on page 610, depending on the catalog backup policy.
See "Restore from tape or optical (UNIX)" on page 609 or "Restore from disk" on page 610, depending on the catalog backup policy.
/usr/openv/db/staging
Relational database files

A restore of the NetBackup database and relational database files from a hot catalog backup consists of the following steps:

1. The NetBackup database files are restored by means of the standard NetBackup restore procedure.

The remaining steps pertain to the relational database files.

2. 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), or to *`install_path`*`\NetBackupDB\staging` (Windows).

3. 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.

4 The relational database files are moved from the staging directory to a location determined by the `bp.conf` file `VXDBMS_NB_DATA` setting on UNIX and by the corresponding registry key on Windows. The default location is `/usr/openv/db/data` on UNIX and *`install_path`*`\NetBackupDB\data` on Windows.

If the relational database files have been relocated, they are moved from the staging directory to the locations specified in the `/usr/openv/db/data/vxdbms.conf` file (UNIX) or the *`install_path`*`\NetBackupDB\data\vxdbms.conf` file (Windows). For a description of how the NetBackup relational database files can be relocated after installation, refer to the “NetBackup Relational Database” appendix in the *NetBackup Administrator’s Guide, Volume I*.

Logs

For messages relating to all catalog recovery steps, consult the `/usr/openv/netbackup/logs/admin` logs (UNIX), or *`install_path`*`\NetBackup\logs\admin` (Windows).

For messages relating to step 1 and step 2, above, consult the `tar`, `bpbrm`, and `bpcd` logs.

For messages pertaining only to the relational database files, see the progress logs in: `/usr/openv/netbackup/logs/user_ops/root/logs` (UNIX), or *`install_path`*`\NetBackup\logs\user_ops\root\logs` (Windows).

NetBackup directories and files

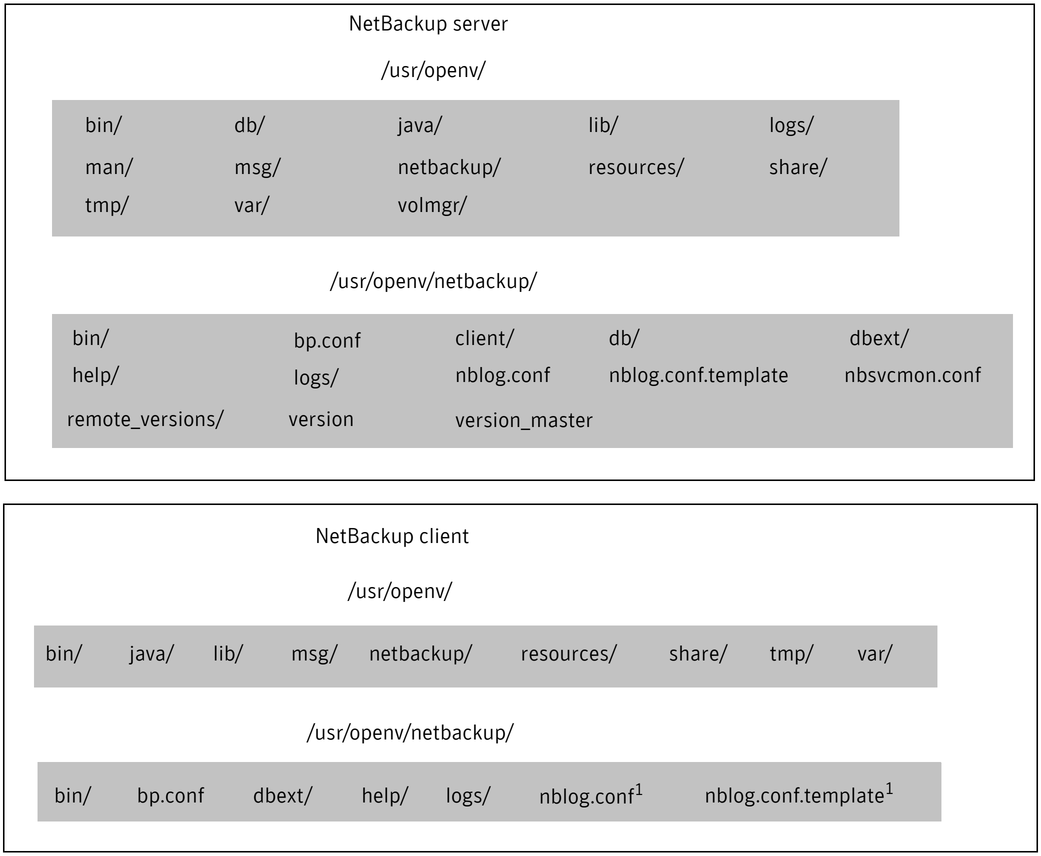
The following diagram shows the NetBackup file and directory structure on UNIX servers and clients. If a host is only a client and not a server, only the files in the Client portion are present. If a host is both a client and a server, the client shares files as necessary from those in the Server portion.

A Windows NetBackup server has equivalent files and folders located where NetBackup is installed (`C:\Program Files\VERITAS` by default).

NetBackup directory structure - UNIX

The directories and files listed below are described in tables on the following pages.

Figure A-16 NetBackup directories and files



NetBackup server

/usr/openv/

bin/	db/	java/	lib/	logs/
man/	msg/	netbackup/	resources/	share/
tmp/	var/	volmgr/		

/usr/openv/netbackup/

bin/	bp.conf	client/	db/	dbext/
help/	logs/	nblog.conf	nblog.conf.template	nbsvcmon.conf
remote_versions/	version	version_master		

NetBackup client

/usr/openv/

bin/	java/	lib/	msg/	netbackup/	resources/	share/	tmp/	var/

/usr/openv/netbackup/

bin/	bp.conf	dbext/	help/	logs/	nblog.conf[1]	nblog.conf.template[1]

[1] Included only on NetBackup-server supported platforms

Contents of /usr/openv

The following table describes the `/usr/openv/` files and directories.

Table A-1 NetBackup directories and files in /usr/openv/ - servers and UNIX clients

File or directory in `/usr/openv/`	Contents
`bin/`	Contains miscellaneous executable binaries including the vnetd daemon and utilities for legacy enhanced authentication.
`db/`	Contains the NetBackup Relational Database (ASA) and database data file.
`java/`	Contains the NetBackup-Java Administration Console and the Backup, Archive and Restore user interface.
`lib/`	Contains shared libraries required for NetBackup operation.
`logs/`	Contains all logs written by unified logging. You do not have to create subdirectories for these logs.
`man/`	Contains man pages for NetBackup commands.
`msg/`	Contains message files and a configuration file for all installed languages of NetBackup.
NB-Java.tar.Z	A tar file containing the NetBackup-Java interfaces.
netbackup/	See “NetBackup directories and files in /usr/openv/netbackup/ - servers and UNIX clients” on page 619.
resources/	Contains NetBackup message catalogs used by unified logging (VxUL).
share/	Contains static configuration files. These files are normally unchanged between NetBackup releases.
tmp/	Contains the NetBackup Relational Database (ASA) installation trace files, and the log files regarding starting and stopping the database.
var/	Contains variable configuration files. These files, which are related to licensing, authentication, authorization, and networking, may change while NetBackup is running. `/usr/openv/var/global` contains various static and variable configuration files. In a cluster, the `/global` directory is shared between nodes.
volmgr/	Contains media and device management directories and files. See “Media and device management components” on page 639.

Contents of /usr/openv/netbackup

The following table describes the `/usr/openv/netbackup` files and directories.

Table A-2 NetBackup directories and files in /usr/openv/netbackup/ - servers and UNIX clients

File or Directory in `/usr/openv/netbackup/`	**Contents**
`bin/`	Commands, scripts, programs, daemons, and files required for NetBackup operation and administration. On a server, there are two subdirectories under bin. `admincmd`: Contains various commands 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. The *NetBackup Administrator's Guide, Vol II,* has a detailed explanation of each option and how to set it. 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 as described in the table "NetBackup catalogs" on page 630.
`dbext/`	For NetBackup database agent software, contains the version file, compressed tar file, and install_dbext script.
`help/`	Help files used by NetBackup programs. These files are in ASCII format.
`logs/`	Legacy debug logs for NetBackup processes. You must create the necessary subdirectories in order for these log files to be written (see "Legacy NetBackup logging" on page 96). See the table "NetBackup daemons and programs" on page 620 for an explanation of the processes that produce the logs.
nblog.conf	Specifies settings for unified logging. **Note:** *Do not edit this file manually:* use the vxlogcfg command instead. See "Configuring and using unified logging" on page 90.
nblog.conf.template	Specifies settings for unified logging. **Note:** *Do not edit this file manually:* use the vxlogcfg command instead. See "Configuring and using unified logging" on page 90.

Table A-2 NetBackup directories and files in /usr/openv/netbackup/ - servers and UNIX clients

File or Directory in `/usr/openv/netbackup/`	Contents
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

The following table, "NetBackup daemons and programs," 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.

Note: You must create legacy logging directories manually; see "logs" in the previous table, and "Legacy NetBackup logging" on page 96.

Table A-3 NetBackup daemons and programs

Program/Daemon	Description
`bp`	On UNIX clients, this menu-driven, character-based interface program has options for starting user-directed backups, restores, and archives. **Started By:** `/usr/openv/netbackup/bin/bp` command on the client. **Stopped By:** Exiting the interface program. **Debug Log:** `/usr/openv/netbackup/logs/bp` on the client. The debug logs for `bpbackup`, `bparchive`, `bprestore`, and `bplist` also have information about `bp` activities.
`BP.NLM`	On NetWare target clients, this 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. **Debug Log:** `SYS:\VERITAS\NBUCLT\NETBACK\LOGS\BP\`*mmddyy*`.log` file on the client.

Table A-3 NetBackup daemons and programs (continued)

Program/Daemon	Description
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 executing the /usr/openv/netbackup/bin/bparchive command on the client. **Stopped By:** Completion of operation. **Debug Log:** bparchive legacy log directory on the client.
bpbackup	On UNIX clients, this program communicates with bprd on the master server when a user starts a backup. **Started By:** Starting a backup by using the client-user interface or 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:** bpbrm on the server with the storage unit. **Stopped By:** Completion of operation. **Debug Log:** bpbkar legacy log directory on the client.
BPBKAR32	On Windows clients, the Backup/Archive Manager generates the backup images. **Started By:** BPCDW32 on the client. **Stopped By:** Completion of operation. **Debug Log:** BPBKAR legacy log directory in the NetBackup logs directory on the client.
bpbrm	On master and media servers, the Backup/Restore Manager manages the client and bptm or bpdm process. It also uses error status from the client and from bptm or bpdm to determine the final status of backup or restore operations. **Started By:** For each backup or restore, nbjm starts an instance of bpbrm on the server with the appropriate storage unit. **Stopped By**: Completion of operation. **Debug Log:** bpbrm legacy log directory on the server.

Table A-3 NetBackup daemons and programs (continued)

Program/Daemon	Description
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, this 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, this 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:** There is no terminate option for this command outside of using kill. **Debug Log:** bpdbjobs legacy log directory on the server.

Table A-3 NetBackup daemons and programs (continued)

Program/Daemon	Description
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: for the read phase of disk duplication, for the read phase of synthetic backups, for disk verify and disk import, to do true image restore from disk, and to delete disk images. **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.
bpjava-msvc	NetBackup-Java master server application program. This program runs on all NetBackup UNIX systems and authenticates users that start the NetBackup-Java interface programs. **Started By:** inetd during startup of the NetBackup Java interfaces. **Stopped By:** When authentication is complete. **Debug Log:** bpjava-msvc legacy log directory on the server.

Table A-3 NetBackup daemons and programs (continued)

Program/Daemon	Description
`bpjava-usvc`	NetBackup-Java user server application program. This program services all requests from the NetBackup-Java user and administration interfaces. **Started By:** `bpjava-msvc` upon successful login through the Login dialog box that is presented when a NetBackup-Java interface is started. **Stopped By:** When the interface program is terminated. **Debug Log:** `bpjava-usvc` legacy log directory.
`bplist`	On UNIX clients, this program communicates with `bprd` on the master server when a user browses the database during a restore operation. **Started By:** Starting a search of the image database by using the client-user interface or executing the `/usr/openv/netbackup/bin/bplist` command on the client. **Stopped By:** Completion of operation **Debug Log:** `bplist` legacy log directory on the client.
`bprd`	On master servers, the request daemon responds to client and administrative requests for the following: ■ Restores ■ Backups (scheduled and user-directed) ■ Archives ■ List 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.

Table A-3 NetBackup daemons and programs (continued)

Program/Daemon	Description
BPSVR.NLM	On NetWare nontarget clients, this 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, this 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.
bptm	On master and media servers, `bptm` manages both disk and tape backup and restore, and is used when the storage unit type is either disk or Media Manager. This program manages the transfer of images between the client and the storage device. **Started By:** For each backup or restore, `bpbrm` starts an instance of `bptm` on the server that has the storage unit. **Stopped By:** Completion of operation. **Debug Log:** `bptm` legacy log directory on the server.
jbpSA	A Java-based program for performing backups, archives and restores of UNIX clients. **Started By:** On UNIX, the `/usr/openv/netbackup/bin/jbpSA` command. **Debug Log:** None, although the logs for the `bpbackup`, `bparchive`, `bplist`, and `bprestore` commands on the client can be useful. Also, check the `bpjava-msvc` and `bpjava-usvc` logs.
jnbSA	A Java-based administration utility for managing NetBackup on UNIX. In addition, administration of supported UNIX systems can be performed by using the NetBackup-Java Windows Display Console on a Windows system. **Started By:** On UNIX, the `/usr/openv/netbackup/bin/jnbSA` command. On a NetBackup-Java Windows Display console, the NetBackup - Java on *host* menu item on the Programs/NetBackup menu. **Stopped By:** Exit option in `jnbSA`. **Debug Log:** None, although the logs for `bpjava-msvc` and `bpjava-usvc` can be helpful.

Table A-3 NetBackup daemons and programs (continued)

Program/Daemon	Description
`nbemm`	On the server 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 82.
`nbfdrv64`	On a media server enabled for SAN Client backup over fibre channel, nbfdrv64 is a user mode component that is used for both backup and restore. nbfdrv64 uses a windrvr6 proxy to move fibre channel data between nbftclnt and bptm buffers. **Started By:** `/usr/openv/netbackup/bin/nbftsrvr` **Stopped By:** `/usr/openv/netbackup/bin/nbftsrvr -terminate` **Debug Log:** On the server, `/usr/openv/logs` (UNIX) or *`install_path`*`\logs` (Windows). See "Unified logging" on page 82.
`nbftclnt`	On clients 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 82.
`nbftsrvr`	On a media server enabled for SAN Client backup over fibre channel, nbftsrvr 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 82.
`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 82.

Table A-3 NetBackup daemons and programs (continued)

Program/Daemon	Description
`NBNWNT.EXE`	For NetWare nontarget clients, this 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.
`nbpem`	On master servers, the nbpem service gets the policy list from bpdbm by means of nbproxy, builds the job worklist, starts due jobs, and sets timers for next due jobs. **Started By:** Started when NetBackup starts. **Stopped By:** `/usr/openv/netbackup/bin/nbpem -terminate` **Debug Log:** On the server, `/usr/openv/logs` (UNIX) or *`install_path`*`\logs` (Windows). See “Unified logging” on page 82.
`nbproxy`	Runs on the master and media server as a child of the process it serves. `nbproxy` provides a thread-safe API for libraries that are not yet thread safe. **Started By**: the process that is using `nbproxy` as a proxy. **Stopped By:** stopping the process that is using `nbproxy`. **Debug Log:** `nbproxy` legacy log directory on the server.
`nbrb`	On the server defined as the EMM server, the nbrb service accepts resource requests from nbjm, acquires physical resources from nbemm, and manages logical resources. **Started By**: Started when NetBackup starts. **Stopped By:** `/usr/openv/netbackup/bin/nbrb -terminate` **Debug Log:** On the server, `/usr/openv/logs` (UNIX) or *`install_path`*`\logs` (Windows). See “Unified logging” on page 82.
`ndmpagent`	Controls backup and restore operations on a NAS server. ndmpagent is for remote NDMP: backing up NDMP data to a drive configured in a Media Manager storage unit on a NetBackup media server. **Started By:** `bpbrm`. **Stopped By:** Completion of backup or restore. **Debug Log:** On the server, `/usr/openv/logs` (UNIX) or *`install_path`*`\logs` (Windows). See “Unified logging” on page 82.

Table A-3 NetBackup daemons and programs (continued)

Program/Daemon	Description
`nbstserv`	Runs on the master server. The nbstserv service manages lifecycle operations including duplication, staging, and image expiration. **Started By**: Started when NetBackup starts. **Stopped By:** `/usr/openv/netbackup/bin/nbstserv -terminate` **Debug Log:** On the server, `/usr/openv/logs` (UNIX) or *`install_path`*`\logs` (Windows). See under "Processes that use unified logging" on page 84, for OID 226 and 272.
`NBWIN.EXE`	For Windows clients, this 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 82.
`pbx_exchange`	Private Branch Exchange (PBX) is a common services framework that helps limit the number of TCP/IP ports that the CORBA services of NetBackup use. **Started By:** Started when NetBackup starts, or by `/opt/VRTSpbx/bin/vxpbx_exchanged start` **Stopped By:** Stopped when NetBackup stops, or by `/opt/VRTSpbx/bin/vxpbx_exchanged stop` **Debug Log:** On the server, `/opt/VRTSpbx/log` (UNIX) or *`install_path`*`\VxPBX\log` (Windows). See "PBX logging" on page 66.

Table A-3 NetBackup daemons and programs (continued)

Program/Daemon	Description
`ql2300_stub`	On a Solaris media server enabled for SAN Client transfers over fibre channel: ql2300_stub is a device driver used to read and write to the NVRAM on a target mode Fibre Channel Host Bus Adapter. On Linux, it also prevents initiator mode drivers from binding to the target mode fibre channel HBAs. **Started By:** Device driver started by the operating system on a reboot after `nbftsrv_config -nbhba` on Linux and Solaris. On Linux, it is also started on all reboots after `nbftsrv_config`. **Stopped By:** Device driver stopped by `nbfdrv64` on Linux and `nbftsrv_config` on Solaris. **Debug Log:** Logging for the device driver is handled by the host operating system in the system messages log: `/var/adm/messages` (Solaris) or `/var/log/messages` (Linux).
`tar`	On UNIX clients, the Tape ARchive program is a special version of `tar` provided with NetBackup and used to restore images. **Started By:** For each restore, `bpbrm` starts an instance of `tar` on the client. **Stopped By:** Completion of restore operation. **Debug Log:** `tar` legacy log directory on the client.
`TAR32`	On Windows clients, the `TAR32` program is a special version of `tar` provided with NetBackup and used to restore images. **Started By:** For each restore, NetBackup starts an instance of `TAR32` on the client. **Stopped By:** Completion of restore operation. **Debug Log:** `TAR` legacy log directory on the client.
`windrvr6`	On a Media Server 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 started by the operating system at boot (Solaris) or by nbfdrv64 (Linux). **Stopped By:** Device driver stopped by the operating system at shutdown. **Debug Log:** Logging is handled by the host operating system in the system messages log: `/var/adm/messages` (Solaris) or `/var/log/messages` (Linux).

NetBackup catalogs

The following table describes the NetBackup catalogs. These catalogs contain 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, containing information about the policy.

Table A-4 NetBackup catalogs

Database	Contents
config	Configuration information. This database resides on the master server and has three parts: policy: Contains information about each NetBackup policy. config: Contains information about global attributes, storage units, and database backups. altnames: Contains 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 information recorded during backup operations and used in the NetBackup reports. failure_history: Contains 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 used by bptm. Also has an errors file that contains error history information for media and devices.

Media and device management functional description

This section explains the operation of media server software and contains the following discussions:

- "Startup process"
- "Media and device management process"
- "Shared Storage option management process"
- "Barcode Operations"
- "Media and device management components"

Note: For a description of the EMM server and nbemm, refer to "EMM server and master server" on page 587.

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). See "Starting media and device management" on page 632 for the complete command path.

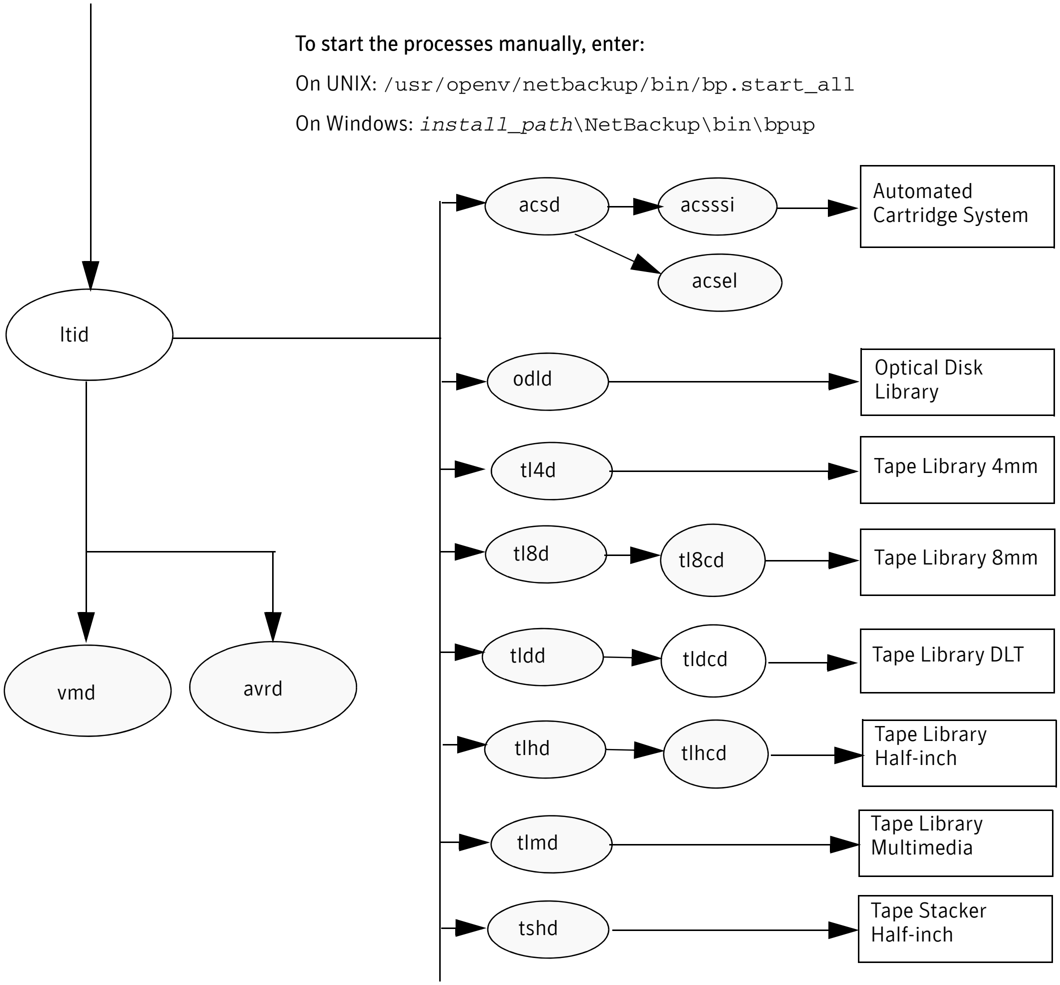
`ltid` automatically starts other daemons and programs as necessary. The graphic "Starting media and device management" shows the daemons that should be running after initial startup. In the case of robotic daemons, such as tl8d and tlhd, the associated robot must also be configured for the daemon to run. See the "Media and device management daemons and programs" table for other ways to start and stop these daemons.

As shown in the figure "Starting media and device management," the TL8, TLH, and TLD require two types of daemons: robotic and robotic control.

- Each host with a robotic drive attached must have a robotic daemon. These daemons provide the interface between `ltid` 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.

Figure A-17 Starting media and device management



At system startup, the server automatically starts **`ltid`**, which starts applicable robotic daemons.

To start the processes manually, enter:

On UNIX: `/usr/openv/netbackup/bin/bp.start_all`

On Windows: *`install_path`*`\NetBackup\bin\bpup`

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 as described under "Backup and archive processes" on page 587.

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. For an overview, refer to the figure "Media and device management example process."

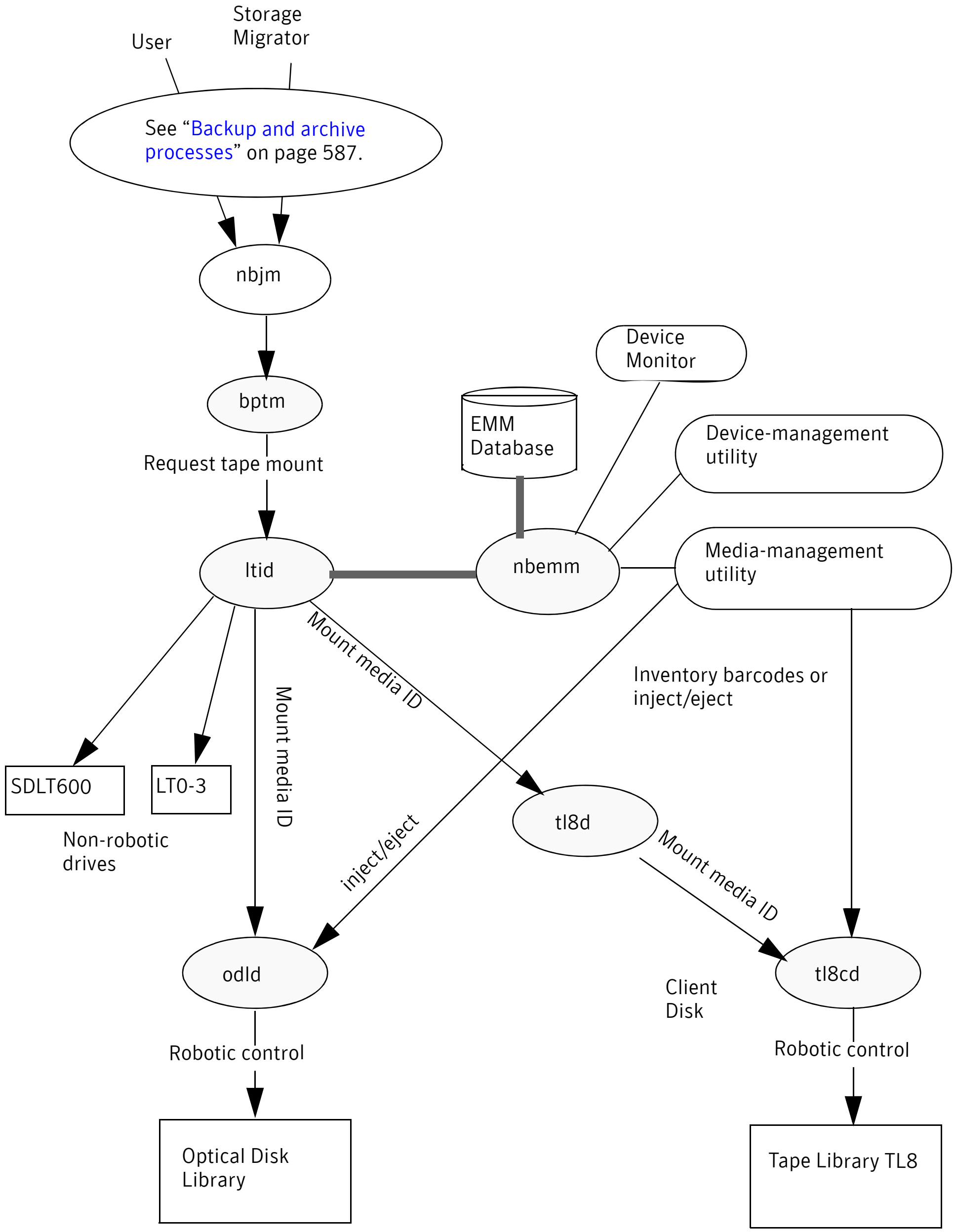
Assuming that the media is physically in the robot, the media is mounted and the operation proceeds. If the media is not in the robot, nbrb creates a pending request, which appears as a pending request in the Device Monitor. An operator must then insert the media in the robot and use the appropriate 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. See the *NetBackup Administrator's Guide, Volume II,* for more information on NetBackup media selection for nonrobotic drives.

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 A-18 Media and device management example process



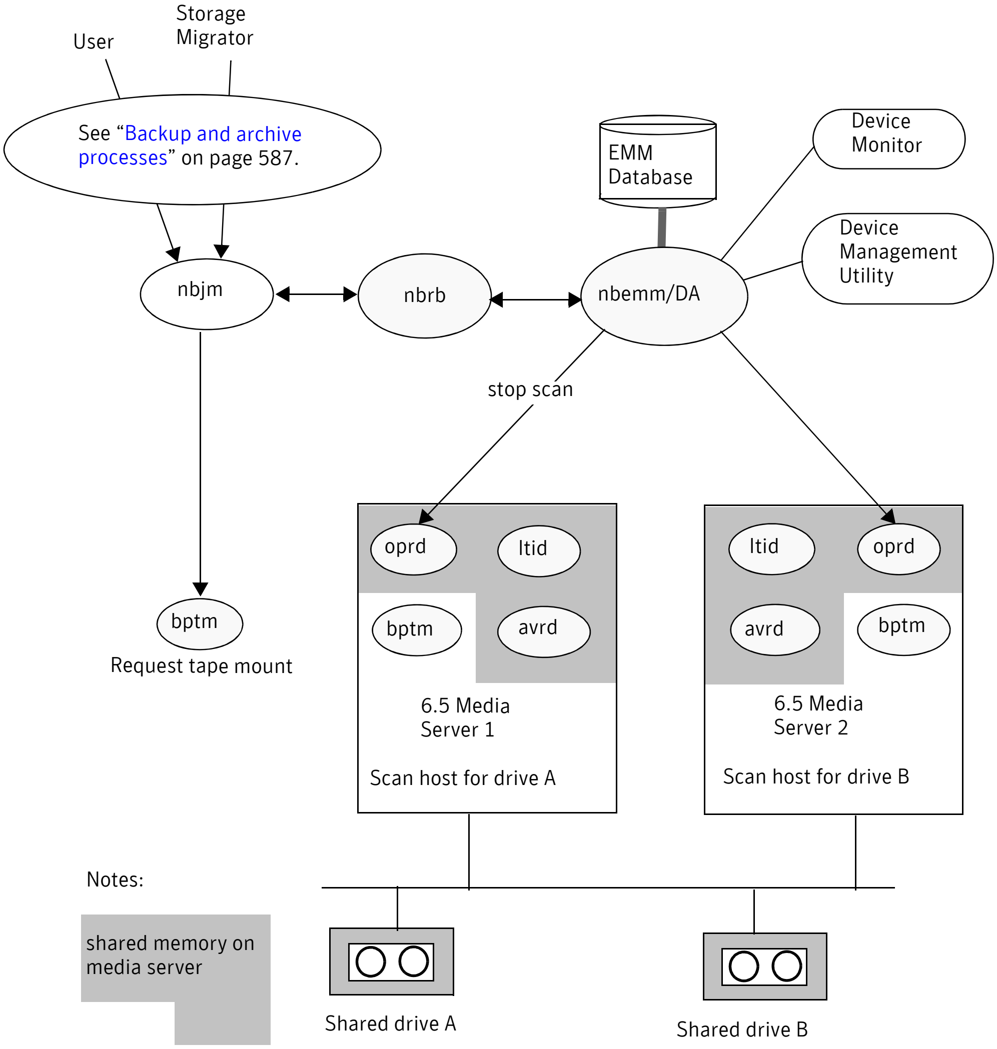
Shared Storage option management process

Shared Storage Option (SSO) is an extension to tape drive allocation and configuration for media and device management. SSO allows individual tape drives (stand-alone or in a robotic library) to be dynamically shared between multiple NetBackup media servers or SAN media servers. For more information, see the *NetBackup Shared Storage Guide*.

Refer to the following figure for a process diagram.

1. NetBackup, Storage Migrator, or users can initiate backups. nbjm makes a mount request for the backup.
2. nbrb tells the EMM server to obtain a drive for the backup.
3. nbrb tells the device allocator (DA) in the EMM server to stop scanning the selected drive.
4. 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.
5. nbemm informs nbrb when scanning on the selected drive has stopped.
6. nbrb informs nbjm that the selected drive (A) is available for the backup.
7. nbjm conveys the mount request and drive selection to bptm, which proceeds with the backup. To protect the integrity of the write operation, bptm uses SCSI reservations.
   For more information, see "How NetBackup reserves drives" in the *NetBackup Administrator's Guide, Volume II*.
8. The mount-media operation is initiated.
9. 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.
10. When the backup is complete, nbjm tells nbrb to release resources.
11. nbrb de-allocates the drive in EMM.
12. 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 A-19 Media and device management process flow showing SSO components



Barcode Operations

Barcode reading is mainly a function of the robot hardware rather than media and device management. When a robot has a barcode reader, it scans any barcode that may be on a tape and stores the code in its internal memory. This associates the slot number and the barcode of the tape in that slot. NetBackup determines that association for its own use by interrogating the robot.

If a robot supports barcodes, NetBackup automatically compares a tape's barcode to what is in the EMM database as an extra measure of verification before mounting the tape.

Media requests involving barcodes

A request for media that is in a robot that can read barcodes begins in the same manner as other requests (see the "Barcode request" figure).

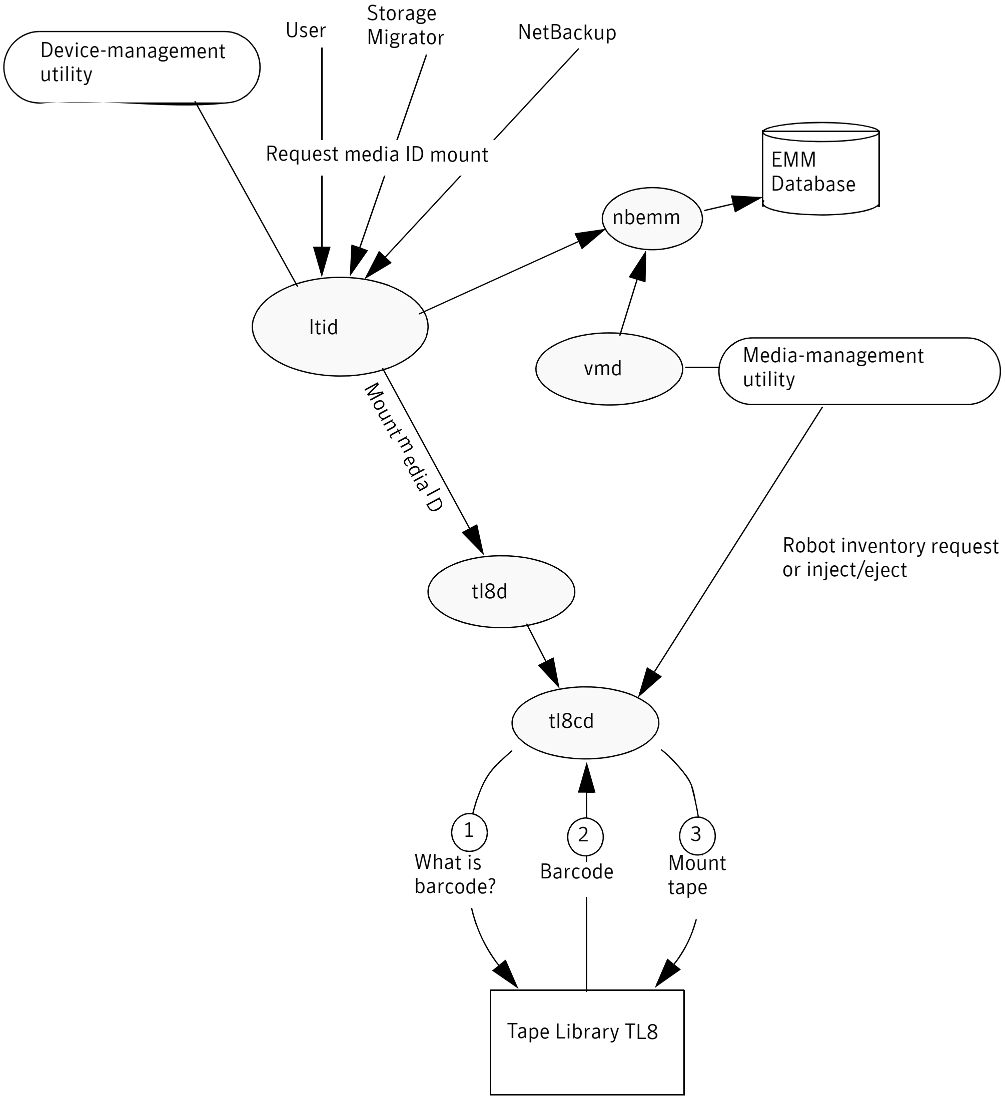
`ltid` includes the media ID and location information in a mount request to the robotic daemon for the robot that has the media ID. This request causes the robotic daemon to query the robotic-control daemon or the robot for the barcode of the tape in the designated slot. (This is a preliminary check 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).

Figure A-20 Barcode request



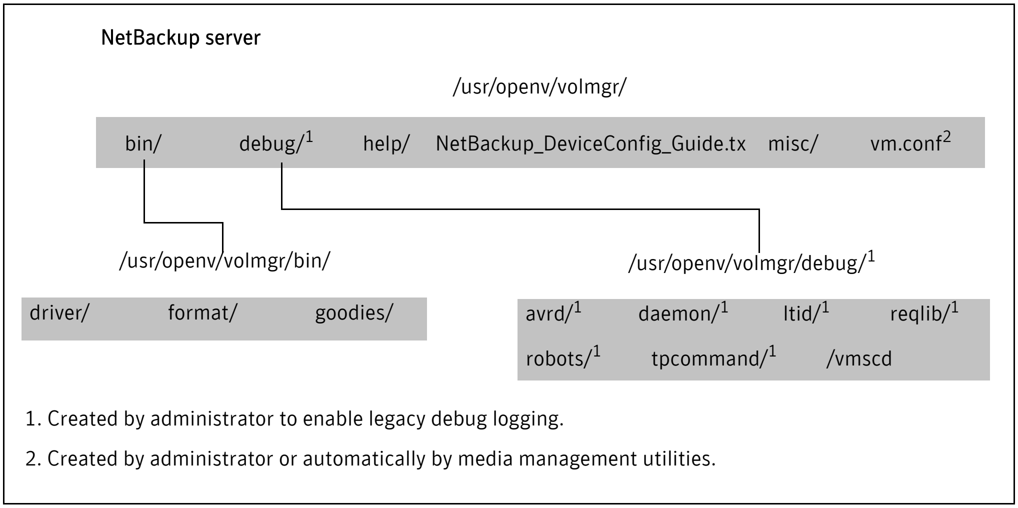
Media and device management components

Directories and files

The following diagram 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`).

The "Media and device management directories and files" table describes the directories and files that are of special interest.

Figure A-21 Media and device management directories and files



1. Created by administrator to enable legacy debug logging.

2. Created by administrator or automatically by media management utilities.

Table A-5 Media and device management directories and files

File or Directory	Contents
`bin`	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.
`debug`	Legacy debug logs for the Volume Manager daemon, `vmd`, and all requesters of `vmd`, `ltid`, and device configuration. The administrator must create these directories for debug logging to occur.

Table A-5 Media and device management directories and files

File or Directory	Contents
`help`	Help files used by media and device management programs. These files are in ASCII format.
`misc`	Lock files and temporary files required by various components of media and device management.
`vm.conf`	Media and device management configuration options.

Media and device management programs and daemons

The “Media and device management daemons and programs” table 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 A-6 Media and device management daemons and programs

Program/ Daemon	Description
`acsd`	The Automated Cartridge System daemon interfaces with the Automated Cartridge System. It communicates with the server that controls the ACS robotics through the `acsssi` process (UNIX) or the STK Libattach Service (Windows). Also, for UNIX, see the `acsssi` and `acssel` programs. **Started By:** Starting `ltid` (or on UNIX, independently by using the `/usr/openv/volmgr/bin/ascd` command. **Stopped By:** Stopping `ltid` (or on UNIX, independently by finding the PID (process id) and then using the `kill` command). **Debug Log:** Errors are logged in the system log and robots debug log. Debug information is included by adding `VERBOSE` to the `vm.conf` file. On UNIX, debug information is also included by starting the daemon with the `-v` option: this option can also be used through `ltid`, or by putting `VERBOSE` in the `vm.conf` file.
acssel	Available only on UNIX. See the *NetBackup Device Configuration Guide* for details.

Table A-6 Media and device management daemons and programs

Program/ Daemon	Description
acsssi	Available only on UNIX. See the *NetBackup Device Configuration Guide* for details.
avrd	The automatic-volume-recognition daemon controls automatic volume assignment and label scanning. This lets NetBackup read labeled tape and optical disk volumes and to automatically assign the associated removable media to requesting processes. **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/avrd command). **Stopped By:** Stopping ltid, (or on UNIX, independently by finding the PID (process id) and then using the kill command). **Debug Log:** All errors are logged in the system log. Debug information is included by adding VERBOSE to the vm.conf file. On UNIX, debug information is also included by aborting avrd and starting the daemon with the -v option.
ltid	The device demon (UNIX) or NetBackup Device Manager service (Windows) controls the reservation and assignment of tapes and optical disks. **Started By:** /usr/openv/volmgr/bin/ltid command on UNIX or **Stop/Restart Device Manager Service** command in Media and Device Management window on Windows. **Stopped By:** /usr/openv/volmgr/bin/stopltid command on UNIX or **Stop/Restart Device Manager Service** command in the Media and Device Management window on Windows. **Debug Log:** Errors are logged in the system log and ltid debug log. Debug information is included if the daemon is started with the -v option (available only on UNIX) or adding VERBOSE to the vm.conf file.
odld	The Optical Disk Library daemon interfaces with the Optical Disk Library, communicating with the robotics through a SCSI interface. This library is not supported on Windows. **Started By:** Starting ltid or independently by using the /usr/openv/volmgr/bin/odld command. **Stopped By:** Stopping ltid or independently by finding the PID (process id) and then using the kill command. **Debug Log:** All errors are logged in the system log. Debug information is included if the daemon is started with the -v option (either by itself or through ltid) or adding VERBOSE to the vm.conf file.

Table A-6 Media and device management daemons and programs

Program/ Daemon	Description
`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`).
`tl8cd`	The Tape Library 8MM Control daemon provides the robotic control for a TL8 robot and communicates with the robotics through a SCSI interface. `tl8cd` receives mount and unmount requests from `tl8d` on the host to which the drive is attached and then communicates these requests to the robot. **Started By:** Starting `ltid` (or on UNIX, independently by using the `/usr/openv/volmgr/bin/tl8cd` command). **Stopped By:** Stopping `ltid` or by using the `tl8cd -t` command. **Debug Log:** Errors are logged in the system log and robots debug log. Debug information is included by adding `VERBOSE` to the `vm.conf` file. On UNIX, debug information is also included by starting the daemon with the `-v` option (either by itself or through `ltid`).

Table A-6 Media and device management daemons and programs

Program/ Daemon	Description
tldd	The Tape Library DLT daemon works in conjunction with tldcd to handle requests to TLD robots (Tape Library DLT and Tape Stacker DLT). tldd provides the interface between the local ltid and the robotic control (tldcd) in the same manner as explained previously for tl8d. **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/tldd command). **Stopped By:** Stopping ltid (or on UNIX, independently by finding the PID (process id) and then using the kill command). **Debug Log:** Errors are logged in the system log and robots debug log. Debug information is included by adding VERBOSE to the vm.conf file. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through ltid).
tldcd	The Tape Library DLT Control daemon provides robotic control for a TLD robot in the same manner as explained previously for tl8cd. **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/tldcd command). **Stopped By:** Using the tldcd -t command. Stopping ltid or by using the tldcd -t command. **Debug Log:** Errors are logged in the system log and robots debug log. Debug information is included by adding VERBOSE to the vm.conf file. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through ltid).
tlhd	The Tape Library Half-inch daemon works in conjunction with tlhcd to handle requests to TLH robots that are in an IBM Automated Tape Library (ATL). tlhd provides the interface between the local ltid and the robotic control (tlhcd) in the same manner as explained previously for tl8d. **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/tlhd command). **Stopped By:** Stopping ltid (or on UNIX, independently by finding the PID (process id) and then using the kill command). **Debug Log:** Errors are logged in the system log and robots debug log. Debug information is included by adding VERBOSE to the vm.conf file. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through ltid).

Table A-6 Media and device management daemons and programs

Program/ Daemon	Description
tlhcd	The Tape Library Half-inch Control daemon provides robotic control for a TLH robot that is in an IBM Automated Tape Library (ATL) in a similar manner to that which was explained previously for tl8cd. **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/tlhcd command). **Stopped By:** Stopping ltid or by using the tlhcd -t command. **Debug Log:** Errors are logged in the system log and robots debug log. Debug information is included if the daemon is started with the -v option (either by itself or through ltid). The -v option is available only on UNIX. Also, add the VERBOSE option to the vm.conf file.
tlmd	The Tape Library Multimedia daemon is the interface between ltid and a TLM robot that is in an ADIC Distributed AML Server (DAS). This daemon communicates with the TLM robotics through a network API interface. **Started By:** Starting ltid or independently by using the /usr/openv/volmgr/bin/tlmd command. **Stopped By:** Stopping ltid or independently by finding the PID (process id) and then using the kill command. **Debug Log:** Errors are logged in the system log and robots debug log. Debug information is included if the daemon is started with the -v option (either by itself or through ltid). The -v option is available only on UNIX. Also, add the VERBOSE option to the vm.conf file.
tpconfig	tpconfig is a command line interface or interactive administrator utility for configuring devices under Media and Device Management. The graphical user interfaces provide equivalent functionality. **Started By:** tpconfig command. **Stopped By:** Quit option from within the utility on UNIX. On Windows, tpconfig is only a command-line interface that runs to completion (no quit option). **Debug Log:** tpcommand debug logs.
tshd	The Tape Stacker Half-inch daemon is the interface between ltid and the half-inch-cartridge stacker and communicates with the robotics through a SCSI interface. This robot is not supported on Windows. **Started By:** Starting ltid (or on UNIX, independently by using the /usr/openv/volmgr/bin/tshd command). **Stopped By:** Stopping ltid (or on UNIX, independently by finding the PID (process id) and then using the kill command). **Debug Log:** All errors are logged in the system log. Debug information is included by adding VERBOSE to the vm.conf file. On UNIX, debug information is also included by starting the daemon with the -v option (either by itself or through ltid).

Table A-6 Media and device management daemons and programs

Program/ Daemon	Description
vmd	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. **Started By:** Starting `ltid` (or on UNIX, independently by using the Initiate Media Manager Volume Daemon option in `vmadm`) **Stopped By:** Terminate Media Manager Volume Daemon option in `vmadm`). **Debug Log:** System log and also a debug log if the `daemon` or `reqlib` debug directories exist (see "Debug logs on servers" on page 82).
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

Background for troubleshooting

In a configuration with multiple networks and clients with more than one hostname, the NetBackup administrator must configure the policy entries carefully, at all times considering the network configuration (physical, hostnames and aliases, NIS/DNS, routing tables, and so on). This is especially true if the desire is to direct backup and restore data across specific network paths.

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 defined by the system's routing tables. The `bp.conf` file is not a factor in determining this.

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 network path to the server is determined by the client's network code that maps the server name to an IP address.

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 routine). This name is visible in the `bprd` debug log when a connection is made as in the line:

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

The client's configured name is then derived from the *peername* by querying the bpdbm process on UNIX systems, or the NetBackup Database Manager service on Windows systems.

The bpdbm process compares the peername to a list of client names generated from:

1. All clients for which a backup has been attempted
   and
2. All clients in all policies

The comparison is first a simple string comparison which, if successful, is verified by comparing hostnames and aliases 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. One example of why the comparison could fail is the case where the client had changed its hostname but its new hostname is not reflected in any policies yet.

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 used in the connection

When the client connects to the server, it sends 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 to work, however, the administrator must also have made a corresponding change on the server. For more information, refer to 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 is pushing a restore to a client from a server. For a user restore, *destination client* and *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.

Depending on the particulars of the restore request (for example, from root on a server, from a client, to a different client, and so on), the name used to connect back to the client to complete the restore is either the client's peername or its configured name.

When modifying 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 this 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.
- Existing client backup and archive images as recorded in the images directory on the master server. On a UNIX server, this is the /usr/openv/netbackup/db/images directory. On a Windows NetBackup server this is the *install_path*\NetBackup\db\images directory.

All of the above can require manual modification by the administrator if 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.

If Domain Name Services are used and the (possibly unqualified) name that the NetBackup client obtains through its gethostname() library (UNIX) or `gethostbyname()` network (Windows) function is unknown to the Domain Name Service (DNS) on the master server, the master server can be unable to reply to client requests. Whether this situation exists, depends on how the client and the server are configured. If `gethostname() or gethostbyname()`on the client returns host names that are not qualified to the extent that DNS on the master server can resolve them, then you will encounter problems.

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

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

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

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

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

key hostname_from_ client client_as_known_by_server

Where

- *key* is a numeric value used by NetBackup to specify the cases where the translation is to be done. Currently this value must always be 0, indicating a configured name translation.
- *hostname_from_client* is the value to translate. This must correspond to the name 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 configured in the NetBackup configuration on the master server and must also be known to the master server's network services.

For example, the line

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

specifies that when the master server receives a request for a configured client name (numeric key 0), the name danr is always replaced by the name danr.eng.aaa.com. This resolves the problem mentioned above, assuming that:

- The client's `gethostname()` function returned 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

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 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

1 Execute the following command:

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

The test utility menu appears.

2 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 are testing.

ACS

```
/usr/openv/volmgr/bin/acstest -r ACSLS_host
```

Note: On UNIX, for `acstest` to work, `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
```

Note: For more information on ACS, TLH, and TLM robotic control, see the *NetBackup Device Configuration Guide*.

In the above commands, *roboticpath* is the full path to the device file for the robotic control (SCSI). Refer to the *NetBackup Device Configuration Guide* and review the section for your platform to find the appropriate value for *roboticpath*.

There is also an optional parameter that specifies the device file path for the drive(s) so that SCSI unloading of the drive(s) can be done with this utility.

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 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

1 Execute the following command:

```
install_path\Volmgr\bin\robtest.exe
```

The test utility menu appears.

2 Select a robot and press Enter.
The test starts.

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

ACS

```
install_path\Volmgr\bin\acstest -r ACSLS_HOST
```

TL4

```
install_path\Volmgr\bin\tl4test -r roboticpath
```

TL8

```
install_path\Volmgr\bin\tl8test -r roboticpath
```

TLD

```
install_path\Volmgr\bin\tldtest -r roboticpath
```

TLH

```
install_path\Volmgr\bin\tlhtest -r robotic_library_name
```

TLM

```
install_path\Volmgr\bin\tlmtest -r DAS_Hostname
```

Note: For more information on ACS, TLH, and TLM robotic control, see the *NetBackup Device Configuration Guide*.

In the above commands, *roboticpath* is the full path to the device file for the robotic control (SCSI). Refer to the *NetBackup Device Configuration Guide* and review the section for your platform to find the appropriate value for *roboticpath*.

There is also an optional parameter that specifies the device file path for the drive(s) so that SCSI unloading of the drive(s) can be done with this utility.

Usage is:

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

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

Index