

# Symantec NetBackup™ Troubleshooting Guide

UNIX, Windows, and Linux

Release 7.7



# Symantec NetBackup™ Troubleshooting Guide

Documentation version: 7.7

## Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, Veritas, the Veritas 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.

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

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

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

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

Symantec Corporation  
350 Ellis Street  
Mountain View, CA 94043

<http://www.symantec.com>

# Technical Support

Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within the company to answer your questions in a timely fashion.

Our support offerings include the following:

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

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

[support.symantec.com](http://support.symantec.com)

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

## Contacting Technical Support

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

[support.symantec.com](http://support.symantec.com)

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

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

- Product release level
- Hardware information
- Available memory, disk space, and NIC information

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

## Licensing and registration

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

[support.symantec.com](http://support.symantec.com)

## Customer service

Customer service information is available at the following URL:

[support.symantec.com](http://support.symantec.com)

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

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

## Support agreement resources

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

Asia-Pacific and Japan [customercare\\_apj@symantec.com](mailto:customercare_apj@symantec.com)

Europe, Middle-East, and Africa [semea@symantec.com](mailto:semea@symantec.com)

North America and Latin America [supportsolutions@symantec.com](mailto:supportsolutions@symantec.com)

# Contents

|   |    |
|---|----|
| Technical Support .....   | 4  |
| Chapter 1   |    |
| Introduction .....  | 10 |
| Recent changes to this guide .....  | 10 |
| Troubleshooting a problem .....   | 10 |
| Problem report for Technical Support .....  | 13 |
| About gathering information for NetBackup-Java applications .....                                   | 14 |
| Chapter 2   |    |
| Troubleshooting procedures .....  | 17 |
| About troubleshooting procedures .....  | 18 |
| Troubleshooting NetBackup problems .....  | 19 |
| Verifying that all processes are running on UNIX servers .....                                      | 22 |
| Verifying that all processes are running on Windows servers .....                                   | 24 |
| Troubleshooting installation problems .....   | 27 |
| Troubleshooting configuration problems .....  | 28 |
| Device configuration problem resolution .....   | 30 |
| Testing the master server and clients .....   | 33 |
| Testing the media server and clients .....  | 37 |
| Resolving network communication problems with UNIX clients .....                                    | 40 |
| Resolving network communication problems with Windows<br>clients .....                              | 45 |
| About troubleshooting networks and host names .....   | 49 |
| Verifying host name and service entries in NetBackup .....  | 53 |
| Example of host name and service entries on UNIX master server<br>and client .....                  | 57 |
| Example of host name and service entries on UNIX master server<br>and media server .....            | 58 |
| Example of host name and service entries on UNIX PC<br>clients .....                                | 59 |
| Example of host name and service entries on UNIX server that<br>connects to multiple networks ..... | 60 |
| About the bpcintcmd utility .....   | 62 |
| Using the Host Properties window to access configuration<br>settings .....                          | 64 |
| Resolving full disk problems .....  | 65 |

|  |     |
|--|-----|
| Frozen media troubleshooting considerations .....  | 66  |
| Logs for troubleshooting frozen media .....  | 67  |
| About the conditions that cause media to freeze .....  | 67  |
| Resolving PBX problems .....   | 70  |
| Checking PBX installation .....  | 71  |
| Checking that PBX is running .....   | 71  |
| Checking that PBX is set correctly .....   | 72  |
| Accessing the PBX logs .....   | 73  |
| Troubleshooting PBX security .....   | 74  |
| Determining if the PBX daemon or service is available .....                                      | 76  |
| About troubleshooting Auto Image Replication .....   | 77  |
| Troubleshooting Auto Image Replication .....   | 77  |
| About troubleshooting automatic import jobs .....  | 84  |
| Troubleshooting network interface card performance .....   | 88  |
| About SERVER entries in the bp.conf file .....   | 89  |
| About unavailable storage unit problems .....  | 89  |
| Resolving a NetBackup Administration operations failure on<br>Windows .....                      | 90  |
| Resolving garbled text displayed in NetBackup Administration Console<br>on a UNIX computer ..... | 91  |
| <br>Chapter 3  |     |
| Using NetBackup utilities .....  | 92  |
| About NetBackup troubleshooting utilities .....  | 92  |
| About the analysis utilities for NetBackup debug logs .....                                      | 93  |
| About the Logging Assistant .....  | 97  |
| About network troubleshooting utilities .....  | 97  |
| About the NetBackup support utility (nbsu) .....   | 98  |
| Output from the NetBackup support utility (nbsu) .....   | 100 |
| Status code information gathered by the NetBackup support utility<br>(nbsu) .....                | 103 |
| Example of a progress display for the NetBackup support utility<br>(nbsu) .....                  | 104 |
| About the NetBackup consistency check utility (NBCC) .....                                       | 105 |
| Output from the NetBackup consistency check utility<br>(NBCC) .....                              | 106 |
| Example of an NBCC progress display .....  | 107 |
| About the NetBackup consistency check repair (NBCCR) utility .....                               | 113 |
| About the nbcplogs utility .....   | 115 |
| About the robotic test utilities .....   | 116 |
| Robotic tests on UNIX .....  | 117 |
| Robotic tests on Windows .....   | 118 |

|           |   |     |
|-----------|---|-----|
| Chapter 4 | Disaster recovery .....   | 120 |
|           | About disaster recovery .....   | 120 |
|           | Recommended backup practices .....  | 121 |
|           | About disk recovery procedures for UNIX and Linux .....                                   | 124 |
|           | Recovering the master server disk for UNIX and Linux .....                                | 124 |
|           | About recovering the NetBackup media server disk for UNIX .....                           | 129 |
|           | Recovering the system disk on a UNIX client workstation .....                             | 130 |
|           | About clustered NetBackup server recovery for UNIX and Linux .....                        | 130 |
|           | Replacing a failed node on a UNIX or Linux cluster .....                                  | 131 |
|           | Recovering the entire UNIX or Linux cluster .....   | 132 |
|           | About disk recovery procedures for Windows .....  | 133 |
|           | About recovering the master server disk for Windows .....                                 | 134 |
|           | About recovering the NetBackup media server disk for<br>Windows .....                     | 139 |
|           | Recovering a Windows client disk .....  | 140 |
|           | About clustered NetBackup server recovery for Windows .....                               | 142 |
|           | Replacing a failed node on a Windows VCS cluster .....                                    | 143 |
|           | Recovering the shared disk on a Windows VCS cluster .....                                 | 144 |
|           | Recovering the entire Windows VCS cluster .....   | 145 |
|           | About recovering the NetBackup catalog .....  | 146 |
|           | About NetBackup catalog recovery on Windows computers .....                               | 147 |
|           | About NetBackup catalog recovery from disk devices .....                                  | 147 |
|           | About NetBackup catalog recovery and symbolic links .....                                 | 148 |
|           | About NetBackup catalog recovery and OpsCenter .....                                      | 148 |
|           | NetBackup disaster recovery email example .....   | 149 |
|           | About recovering the entire NetBackup catalog .....                                       | 152 |
|           | About recovering the NetBackup catalog image files .....                                  | 163 |
|           | About recovering the NetBackup relational database .....                                  | 176 |
|           | Recovering the NetBackup catalog when NetBackup Access<br>Control is configured .....     | 184 |
|           | Recovering the NetBackup catalog from a nonprimary copy of a<br>catalog backup .....      | 186 |
|           | Recovering the NetBackup catalog without the disaster recovery<br>file .....              | 186 |
|           | Recovering a NetBackup user-directed online catalog backup from<br>the command line ..... | 188 |
|           | Restoring files from a NetBackup online catalog backup .....                              | 191 |
|           | Unfreezing the NetBackup online catalog recovery media .....                              | 191 |
|           | Index .....   | 193 |

# Introduction

This chapter includes the following topics:

- [Recent changes to this guide](#)
- [Troubleshooting a problem](#)
- [Problem report for Technical Support](#)
- [About gathering information for NetBackup-Java applications](#)

## Recent changes to this guide

All topics from the following chapters have been incorporated into the *NetBackup Logging Reference Guide*:

- Chapters on logging
- The appendix "Backup and restore functional overview"
- The appendix "Media and device management functional description"

See the *NetBackup Logging Reference Guide* for those topics:

[Http://www.symantec.com/docs/DOC5332](http://www.symantec.com/docs/DOC5332)

---

**Note:** For descriptions and recommended actions on NetBackup status codes, see the *NetBackup Status Codes Reference Guide*.

---

## Troubleshooting a problem

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

**Table 1-1** Steps for troubleshooting NetBackup problems

| Step   | Action   | Description   |
|--------|--|---|
| Step 1 | Remember the error message                             | <p>Error messages are usually the vehicle for telling you something went wrong. If you don't see an error message in an interface, but still suspect a problem, check the reports and logs. NetBackup provides extensive reporting and logging facilities. These can provide an error message that points you directly to a solution.</p> <p>The logs also show you what went right and the NetBackup operation that was ongoing when the problem occurred. For example, a restore operation needs media to be mounted, but the required media is currently in use for another backup. Logs and reports are essential troubleshooting tools.</p> <p>See the <a href="#">NetBackup Logging Reference Guide</a>.</p>  |
| Step 2 | Identify what you were doing when the problem occurred | <p>Ask the following questions:</p> <ul style="list-style-type: none"><li>■ What operation was tried?</li><li>■ What method did you use?<br/>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.</li><li>■ What type of server platform and operating system was involved?</li><li>■ If your site uses both the master server and the media server, was it a master server or a media server?</li><li>■ If a client was involved, what type of client was it?</li><li>■ Have you performed the operation successfully in the past? If so, what is different now?</li><li>■ What is the service pack level?</li><li>■ Do you use operating system software with the latest fixes supplied, especially those required for use with NetBackup?</li><li>■ 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?</li></ul> |

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

| Step   | Action  | Description   |
|--------|---|---|
| Step 3 | Record all information                          | <p>Capture potentially valuable information:</p> <ul style="list-style-type: none"> <li>■ NetBackup progress logs</li> <li>■ NetBackup Reports</li> <li>■ NetBackup Utility Reports</li> <li>■ NetBackup debug logs</li> <li>■ Media and Device Management debug logs</li> <li>■ On UNIX NetBackup servers, check for error or status messages in the system log or standard output.</li> <li>■ Error or status messages in dialog boxes</li> <li>■ On Windows, NetBackup servers, check for error or status information in the Event Viewer Application and System log.</li> </ul> <p>Record this information for each try. Compare the results of multiple tries. A record of tries is also useful for others at your site and for Technical Support in the event that you cannot solve the problem. You can get more information about logs and reports.</p> <p>See the <a href="#">NetBackup Logging Reference Guide</a>.</p> |
| Step 4 | Correct the problem                             | <p>After you define the problem, use the following information to correct it:</p> <ul style="list-style-type: none"> <li>■ Take the corrective action that the status code or message recommends. See the <a href="#">Status Codes Reference Guide</a>.</li> <li>■ If no status code or message exists, or the actions for the status code do not solve the problem, try these additional troubleshooting procedures: See “<a href="#">Troubleshooting NetBackup problems</a>” on page 19.</li> </ul>   |
| Step 5 | Complete a problem report for Technical Support | <p>If your troubleshooting is unsuccessful, prepare to contact Technical Support by filling out a problem report.</p> <p>See “<a href="#">Problem report for Technical Support</a>” on page 13.</p> <p>See “<a href="#">About gathering information for NetBackup-Java applications</a>” on page 14.</p> <p>On UNIX systems, the <code>/usr/openv/netbackup/bin/goodies/support</code> script creates a file containing data necessary for Technical Support to debug any problems you encounter. For more details, consult the usage information of the script by means of the <code>support -h</code> command.</p>  |
| Step 6 | Contact Technical Support                       | <p>The Symantec Technical Support website has a wealth of information that can help you solve NetBackup problems.</p> <p>Access Technical Support at the following URL:</p> <p><a href="http://www.symantec.com/business/support/">www.symantec.com/business/support/</a></p>   |

---

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

---

## Problem report for Technical Support

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

Date: \_\_\_\_\_

Record the following product, platform, and device information:

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

---

---

---

---

---

---

---

Define the problem.

---

---

---

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

---

---

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

---

---

---

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

- Initial installation
- Configuration change (explain)
- System change or problem (explain)
- Have you observed the problem before? (If so, what did you do that time?)

---

---

---

Logs or other failure data you have saved:

- All log entries report
- Media and Device Management debug logs
- NetBackup debug logs
- System logs (UNIX)
- Event Viewer Application and System logs (Windows)

Ways that you can communicate with us:

- ftp
- telnet
- email
- WebEx

## About gathering information for NetBackup-Java applications

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

The following scripts are available for gathering information:

|   |   |
|---|---|
| <p>jnbSA<br/>         (NetBackup-Java administration application startup script)</p>        | <p>Logs the data in a log file in <code>/usr/opencv/netbackup/logs/user_ops/nbjlogs</code>. 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 <code>/usr/opencv/java/Debug.properties</code> for the options that can affect the contents of this log file.</p>   |
| <p>NetBackup-Java administration application on Windows</p>                                 | <p>If NetBackup is installed on the computer where the application was started, the script logs the data in a log file at <code>install_path\NetBackup\logs\user_ops\nbjlogs</code>.</p> <p>If NetBackup was not installed on this computer, the script logs the data in a log file at <code>install_path\Veritas\Java\logs</code>.</p> <p><b>Note:</b> When NetBackup is installed where the application is started, and when <code>install_path</code> is not set in the <code>setconf.bat</code> file, the script logs the data here: <code>install_path\Veritas\Java\logs</code>.</p> |
| <p><code>/usr/opencv/java/get_trace</code></p>  | <p>UNIX/Linux only.</p> <p>Provides a Java Virtual Machine stack trace for support to analyze. This stack trace is written to the log file that is associated with the instance of execution.</p>   |
| <p>UNIX/Linux:<br/> <code>/usr/opencv/netbackup/bin/support/nbsu</code></p> <p>Windows:</p> | <p>Queries the host and gathers appropriate diagnostic information about NetBackup and the operating system.</p> <p>See <a href="#">"About the NetBackup support utility (nbsu)"</a> on page 98.</p>  |
| <p><code>install_path\NetBackup\bin\support\nbsu.exe</code></p>                             |   |

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

|   |   |
|---|---|
| <p>An application does not respond.</p> | <p>Wait for several minutes before you assume that the operation is hung. Some operations can take quite a while to complete, especially operations in the <b>Activity Monitor</b> and <b>Reports</b> applications.</p> |
|---|---|

**About gathering information for NetBackup-Java applications**

|  |  |
|--|--|
| UNIX/Linux only:<br>Still no response after several minutes. | Run <code>/usr/opensv/java/get_trace</code> under the account where you started the Java application. This script causes a stack trace to write to the log file.<br><br>For example, if you started <code>jnbSA</code> from the root account, start <code>/usr/opensv/java/get_trace</code> as root. Otherwise, the command runs without error, but fails to add the stack trace to the debug log. This failure occurs because root is the only account that has permission to run the command that dumps the stack trace. |
| Get data about your configuration.                           | Run the <code>nbsu</code> command that is listed in this topic. Run this command after you complete the NetBackup installation and every time you change the NetBackup configuration.  |
| Contact Symantec Technical Support                           | Provide the log file and the output of the <code>nbsu</code> command for analysis.   |

# Troubleshooting procedures

This chapter includes the following topics:

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

- [About SERVER entries in the bp.conf file](#)
- [About unavailable storage unit problems](#)
- [Resolving a NetBackup Administration operations failure on Windows](#)
- [Resolving garbled text displayed in NetBackup Administration Console on a UNIX computer](#)

## About troubleshooting procedures

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

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

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

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

Troubleshooting procedures can be divided into the following categories:

|                               |  |
|-------------------------------|--|
| Preliminary troubleshooting   | <p>The following procedures describe what to check first. They branch off to other procedures as appropriate.</p> <p>See <a href="#">“Troubleshooting NetBackup problems”</a> on page 19.</p> <p>See <a href="#">“Verifying that all processes are running on UNIX servers”</a> on page 22.</p> <p>See <a href="#">“Verifying that all processes are running on Windows servers”</a> on page 24.</p> |
| Installation troubleshooting  | <p>Problems that apply specifically to installation.</p> <p>See <a href="#">“Troubleshooting installation problems”</a> on page 27.</p>  |
| Configuration troubleshooting | <p>Problems that apply specifically to configuration.</p> <p>See <a href="#">“Troubleshooting configuration problems”</a> on page 28.</p>  |

- General test and troubleshooting These procedures define general methods for finding server and client problems and should be used last.
- See [“Testing the master server and clients”](#) on page 33.
  - See [“Testing the media server and clients”](#) on page 37.
  - See [“Resolving network communication problems with UNIX clients”](#) on page 40.
  - See [“Resolving network communication problems with Windows clients”](#) on page 45.
  - See [“Verifying host name and service entries in NetBackup”](#) on page 53.
  - See [“About the bpcintcmd utility”](#) on page 62.
  - See [“Verifying host name and service entries in NetBackup”](#) on page 53.
- Other troubleshooting procedures
- See [“Resolving full disk problems”](#) on page 65.
  - See [“Frozen media troubleshooting considerations”](#) on page 66.
  - See [“About the conditions that cause media to freeze”](#) on page 67.
  - See [“Troubleshooting network interface card performance”](#) on page 88.

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

- See [“Example of host name and service entries on UNIX master server and client”](#) on page 57.
- See [“Example of host name and service entries on UNIX master server and media server”](#) on page 58.
- See [“Example of host name and service entries on UNIX PC clients”](#) on page 59.
- See [“Example of host name and service entries on UNIX server that connects to multiple networks”](#) on page 60.

## Troubleshooting NetBackup problems

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

This preliminary NetBackup troubleshooting procedure explains what to check first and branches to other procedures as appropriate. These procedures do not try to

cover every problem that can occur. However, they do recommend the methods that usually result in successful problem resolution.

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

**Table 2-1** Steps for troubleshooting NetBackup problems

| Step   | Action                                    | Description  |
|--------|---|--|
| Step 1 | Verify operating systems and peripherals. | <p>Ensure that your servers and clients are running supported operating system versions and that any peripherals you use are supported.</p> <p>See the <a href="#">NetBackup Master Compatibility List</a>.</p> <p>In addition, the NetBackup release notes include a section "Required operating system patches and updates for NetBackup" that should be checked. The release notes for your release are available here:<br/> <a href="http://www.symantec.com/docs/DOC5332">http://www.symantec.com/docs/DOC5332</a></p> <p>Additional information is available on the following website:<br/> <a href="http://www.symantec.com/docs/TECH59978">http://www.symantec.com/docs/TECH59978</a></p>                          |
| Step 2 | Use reports to check for errors.          | <p>Use the <b>All Log Entries</b> 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.</p> <p>See the Reports information in the <a href="#">NetBackup Administrator's Guide, Volume I</a>.</p> <p>If the problem involved a backup or archive, check the <b>Status of Backups</b> report. This report gives you the status code.</p> <p>If you find a status code or message in either of these reports, perform the recommended corrective actions.</p> <p>See the <a href="#">Status Codes Reference Guide</a>.</p> |

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

| Step   | Action   | Description  |
|--------|--|--|
| Step 3 | Check the operating system logs.                     | <p>Check the system log (UNIX) or the <b>Event Viewer</b> Application and System log (Windows) if the problem pertains to media or device management and one of the following is true:</p> <ul style="list-style-type: none"> <li>■ NetBackup does not provide a status code.</li> <li>■ You cannot correct the problem by following the instructions in NetBackup status codes and messages.</li> <li>■ You cannot correct the problem by following the instructions in media and device management status codes and messages.</li> </ul> <p>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.</p> |
| Step 4 | Review the debug logs.                               | <p>Read the applicable enabled debug logs and correct any problems you detect. If these logs are not enabled, enable them before you retry the failed operation.</p> <p>See the <a href="#">NetBackup Logging Reference Guide</a>.</p>   |
| Step 5 | Retry the operation.                                 | <p>If you performed corrective actions, retry the operation. If you did not perform corrective actions or if the problem persists, continue with the next step.</p>  |
| Step 6 | Get more information for installation problems.      | <p>If you see the problem during a new installation or upgrade installation, or after you make changes to an existing configuration, see the following procedures:</p> <p>See <a href="#">“Troubleshooting installation problems”</a> on page 27.</p> <p>See <a href="#">“Troubleshooting configuration problems”</a> on page 28.</p>  |
| Step 7 | Ensure that the servers and clients are operational. | <p>If you experienced a server or a client disk crash, procedures are available on how to recover the files that are critical to NetBackup operation.</p> <p>See <a href="#">“About disk recovery procedures for UNIX and Linux”</a> on page 124.</p> <p>See <a href="#">“About disk recovery procedures for Windows”</a> on page 133.</p>   |

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

| Step    | Action   | Description  |
|---------|--|--|
| Step 8  | Ensure that the partitions have enough disk space. | <p>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."</p> <p>On UNIX systems, use the <code>df</code> command to view disk partition information. On Windows systems, use Disk Manager or Explorer.</p> <p>Check the following disk partitions:</p> <ul style="list-style-type: none"> <li>■ The partition where NetBackup software is installed.</li> <li>■ On the NetBackup master or media server, the partition where the NetBackup databases reside.</li> <li>■ The partition where the NetBackup processes write temporary files.</li> <li>■ The partition where NetBackup logs are stored.</li> <li>■ The partition where the operating system is installed.</li> </ul> |
| Step 9  | Increase the logging level.                        | <p>Enable verbose logging either for everything or only for the areas that you think are related to the problem.</p> <p>See the <i>NetBackup Logging Reference Guide</i> for information on changing the logging level.</p>  |
| Step 10 | Determine which daemons or processes are running.  | <p>Follow the procedures for UNIX or Windows NetBackup servers.</p> <p>See <a href="#">"Verifying that all processes are running on UNIX servers"</a> on page 22.</p> <p>See <a href="#">"Verifying that all processes are running on Windows servers"</a> on page 24.</p>   |

## Verifying that all processes are running on UNIX servers

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

**To verify that all processes are running on UNIX servers**

- 1 To see the list of processes (daemons) running on the master server and on the media server, enter the following command:

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

- 2 Ensure that the following processes are running on the NetBackup servers:

**Master server**

|                             |                   |
|-----------------------------|-------------------|
| bpcd -standalone            | nbpem             |
| bpcompatd                   | nbproxy           |
| nbcssc                      | nbrb              |
| bpdbm                       | nbrmms            |
| bpjobd                      | nbsl              |
| bprd                        | nbstserv          |
| nbars                       | nbsvcmonNB_dbsrv  |
| nbdisco (discovery manager) | pbx_exchange      |
| nbemm                       | vmd               |
| nbevtmgrnbjm                | vnetd -standalone |
| nbim (index manager)        |                   |

**Media server**

```
avrd (automatic volume recognition, only if drives are configured
on the server)
bpcd -standalone
bpcompatd
ltid (needed only if tape devices are configured on the server)
mtstrmd (if the system has data deduplication configured)
nbrmms
nbsl
nbsvcmon
pbx_exchange
spad (if the system has data deduplication configured)
spoold (if the system has data deduplication configured)
vmd (volume)
vnetd -standalone
Any tape or robotic processes, such as tldd, tldcd
```

---

**Note:** Additional processes may also need to be running if other add-on products, database agents, and so forth are installed. For additional assistance, see <http://www.symantec.com/docs/TECH135186>.

---

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

```
/usr/opensv/netbackup/bin/initbprd
```

- 4 If any of the media server processes are not running, stop the device process `ltid` by running the following command:

```
/usr/opensv/volmgr/bin/stoptlid
```

- 5 To verify that the `ltid`, `avrd`, and robotic control processes are stopped, run the following command:

```
/usr/opensv/volmgr/bin/vmps
```

- 6 If you use ACS robotic control, the `acsssi` and the `acsse1` processes may continue to run when `ltid` is terminated. Use the UNIX `kill` command to individually stop those robotic control processes.

- 7 Then, start all device processes by running the following command:

```
/usr/opensv/volmgr/bin/ltid
```

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

- 8 If necessary, you can use the following to stop and restart all the NetBackup server processes:

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

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

## Verifying that all processes are running on Windows servers

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

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

| Step   | Action                                    | Description   |
|--------|---|---|
| Step 1 | Start all services on the master servers. | <p>The following services must be running for typical backup and restore operations (steps 1, 2, and 3 in this table). If these services are not running, start them by using the NetBackup <b>Activity Monitor</b> or the Services application in the Windows Control Panel.</p> <p>To start all of the services, run <code>install_path\NetBackup\bin\bpup.exe</code>.</p> <p>Services on master servers:</p> <ul style="list-style-type: none"> <li>■ NetBackup Authentication</li> <li>■ NetBackup Client Service</li> <li>■ NetBackup CloudStore Service Container</li> <li>■ NetBackup Compatibility Service</li> <li>■ NetBackup Database Manager</li> <li>■ NetBackup Discovery Framework</li> <li>■ NetBackup Enterprise Media Manager</li> <li>■ NetBackup Event Manager</li> <li>■ NetBackup Indexing Manager</li> <li>■ NetBackup Job Manager</li> <li>■ NetBackup Policy Execution Manager</li> <li>■ NetBackup Relational Database Manager</li> <li>■ NetBackup Remote Manager and Monitor Service</li> <li>■ NetBackup Request Daemon</li> <li>■ NetBackup Resource Broker</li> <li>■ NetBackup Service Layer</li> <li>■ NetBackup Service Monitor</li> <li>■ NetBackup Storage Lifecycle Manager</li> <li>■ NetBackup Vault Manager</li> <li>■ NetBackup Volume Manager</li> <li>■ Symantec Private Branch Exchange</li> </ul> <p><b>Note:</b> Additional processes may also need to be running if other add-on products, database agents, and so forth are installed. For additional assistance, see <a href="http://www.symantec.com/docs/TECH135186">http://www.symantec.com/docs/TECH135186</a></p> |

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

| Step   | Action  | Description  |
|--------|---|--|
| Step 2 | Start all services on the media servers.          | <p>Services on media servers:</p> <ul style="list-style-type: none"> <li>■ NetBackup Client Service</li> <li>■ NetBackup Deduplication Engine (if the system has data deduplication configured)</li> <li>■ NetBackup Deduplication Manager (if the system has data deduplication configured)</li> <li>■ NetBackup Deduplication Multi-Threaded Agent (if the system has data deduplication configured)</li> <li>■ NetBackup Device Manager service (if the system has configured devices)</li> <li>■ NetBackup Remote Manager and Monitor Service (if the system has data deduplication configured)</li> <li>■ NetBackup Volume Manager service</li> </ul> |
| Step 3 | Start all services on the clients.                | <p>Services on clients:</p> <ul style="list-style-type: none"> <li>■ NetBackup Client Service</li> <li>■ NetBackup Legacy Client Service</li> <li>■ Symantec Private Branch Exchange</li> </ul>  |
| Step 4 | Start <code>avrd</code> and processes for robots. | <p>Use the NetBackup <b>Activity Monitor</b> to see if the following processes are running:</p> <ul style="list-style-type: none"> <li>■ <code>avrd</code> (automatic media recognition), only if drives are configured on the server</li> <li>■ Processes for all configured robots.</li> </ul> <p>See the <a href="#">NetBackup Administrator's Guide, Volume I</a>.</p> <p>If these processes are not running, stop and restart the NetBackup <b>Device Manager</b> service. Use the NetBackup <b>Activity Monitor</b> or the Services application in the Windows Control Panel.</p>  |

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

| Step   | Action  | Description  |
|--------|---|--|
| Step 5 | Restart the operation or do additional troubleshooting. | <p>If you had to start any of the processes or services in the previous steps, retry the operation.</p> <p>If the processes and services are running or the problem persists, you can try to test the servers and clients.</p> <p>See <a href="#">“Testing the master server and clients”</a> on page 33.</p> <p>See <a href="#">“Testing the media server and clients”</a> on page 37.</p> <p>If you cannot start any of these processes or services, check the appropriate debug logs for NetBackup problems.</p> <p>See the <a href="#">NetBackup Logging Reference Guide</a>.</p> <p>When these processes and services start, they continue to run unless you stop them manually or a problem occurs on the system. On Windows systems, we recommend that you add commands for starting them to your startup scripts, so they restart in case you have to restart.</p> |

## Troubleshooting installation problems

Use the following steps to troubleshoot installation problems.

**Table 2-3** Steps for troubleshooting installation problems.

| Step   | Action   | Description  |
|--------|--|--|
| Step 1 | Determine if you can install the software on the master server and the media servers by using the release media. | <p>Some reasons for failure are as follows:</p> <ul style="list-style-type: none"> <li>■ Not logged on as an administrator on a Windows system (you must have permission to install services on the system)</li> <li>■ Permission denied (ensure that you have permission to use the device and to write the directories and files being installed)</li> <li>■ Bad media (contact Technical Support)</li> <li>■ Defective drive (replace the drive or refer to vendor’s hardware documentation)</li> <li>■ Improperly configured drive (refer to the system and the vendor documentation)</li> </ul> |

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

| Step   | Action   | Description  |
|--------|--|--|
| Step 2 | Determine if you can install NetBackup client software on the clients. | <p><b>Note:</b> Before you install or use NetBackup on a Linux client, verify that the <code>bpcd -standalone</code> and <code>vnetd -standalone</code> services are started on that computer. These services ensure proper communication between the NetBackup master and the Linux client.</p> <p><b>Note:</b> NetBackup UNIX or Linux servers can push client software to UNIX/Linux clients, and Windows servers can push to Windows clients. You can also download the client software from the NetBackup appliance, and then run the install on the client.</p> <p><b>Note:</b> See the <a href="#">NetBackup Appliance Administrator's Guide</a>.</p> <p>Do the following:</p> <ul style="list-style-type: none"> <li>■ For an install to a trusting UNIX client, verify the following: <ul style="list-style-type: none"> <li>■ The correct client name is in your policy configuration.</li> <li>■ The correct server name is in the client <code>.rhosts</code> file.</li> </ul> </li> </ul> <p>If the installation hangs, check for problems with the shell or the environment variables for the root user on the client. The files that you check depend on the platform, operating system, and shell you use. For example, your <code>.login</code> on a Sun system runs an <code>stty</code> (such as <code>stty ^erace</code>) before it defines your terminal type. If this action causes the install process to hang, you can modify the <code>.login</code> file to define the terminal before you run the <code>stty</code>. Or, move the client <code>.login</code> to another file until the install is complete.</p> <ul style="list-style-type: none"> <li>■ For an installation to a secure UNIX client, check your <code>ftp</code> configuration. For example, you must use a user name and password that the client considers valid.</li> </ul> |
| Step 3 | Resolve network problems.  | <p>Determine if the problem is related to general network communications.</p> <p>See <a href="#">"Resolving network communication problems with UNIX clients"</a> on page 40.</p> <p>See <a href="#">"Resolving network communication problems with Windows clients"</a> on page 45.</p>   |

## Troubleshooting configuration problems

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

**Table 2-4** Steps for troubleshooting configuration problems

| Step   | Action                                   | Description   |
|--------|--|---|
| Step 1 | Check for device configuration problems. | <p>Check for the following device configuration problems:</p> <ul style="list-style-type: none"> <li>■ Configuration for robotic drive does not specify the robot.</li> <li>■ Drive is configured as wrong type or density.</li> <li>■ Incorrect Robotic Drive Number.</li> <li>■ SCSI ID for the robotic control is specified instead of the logical Robot Number that is assigned to the robot.</li> <li>■ The same robot number is used for different robots.</li> <li>■ SCSI ID for the drive is specified instead of a unique Drive Index number.</li> <li>■ A platform does not support a device or was not configured to recognize it.</li> <li>■ Robotic device is not configured to use LUN 1, which some robot hardware requires.</li> <li>■ On UNIX, drive no-rewind device path is specified as a rewind path.</li> <li>■ On UNIX, tape devices are not configured with "Berkeley style close." NetBackup requires this feature which is configurable on some platforms. Further explanation is available.</li> <li>■ On UNIX, tape devices (other than QIC) are not configured as "variable mode." NetBackup requires this feature which is configurable on some platforms. When this condition exists, you can frequently perform backups but not restores. For more information, see the <a href="#">Status Codes Reference Guide</a>.</li> <li>■ On UNIX, pass-through paths to the tape drives have not been established.</li> </ul> <p>More description is available on device configuration problems:<br/> See the <a href="#">NetBackup Device Configuration Guide</a>.</p> |
| Step 2 | Check the daemons or services.           | <p>Check for the following problems with the daemons or services:</p> <ul style="list-style-type: none"> <li>■ The daemons or services do not start during restart (configure system so they start).</li> <li>■ Wrong daemons or services are started (problems with media server startup scripts).</li> <li>■ Configuration was changed while daemons or services were running.</li> <li>■ On Windows, the <code>%SystemRoot%\System32\drivers\etc\services</code> file does not have an entry for <code>vmd</code>, <code>bprd</code>, <code>bpdbm</code>, and <code>bpcd</code>. Also, ensure that the processes have entries for configured robots. A list of these processes is available. See the <a href="#">NetBackup Administrator's Guide, Volume I</a>.</li> <li>■ On UNIX, the <code>/etc/services</code> file (or NIS or DNS) does not have an entry for <code>vmd</code>, <code>bprd</code>, <code>bpdbm</code>, or robotic daemons.</li> </ul>   |

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

| Step   | Action   | Description  |
|--------|--|--|
| Step 3 | Retry the operation and check for status codes and messages. | <p>If you found and corrected any configuration problems, retry the operation and check for NetBackup status codes or messages in the following:</p> <ul style="list-style-type: none"> <li>Check the <b>All Log Entries</b> 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.<br/>If the problem involved a backup or archive, check the job's Detailed Status in the <b>Activity Monitor</b>. Also check the <b>Status of Backups</b> report.<br/>If you find a status code or message in either of these reports, perform the recommended corrective actions.<br/>See the <a href="#">Status Codes Reference Guide</a>.</li> <li>Check the system logs on UNIX or the Event Viewer Application and System log on Windows if the following is true: The problem pertains to media or device management, and NetBackup does not provide a status code. Or you cannot correct the problem by following the instructions in the status codes.</li> <li>Check the appropriate enabled debug logs. Correct any problems you detect. If these logs are not enabled, enable them before your next try.<br/>See the <a href="#">NetBackup Logging Reference Guide</a>.</li> </ul> |
| Step 4 | Retry the operation and do additional troubleshooting.       | <p>If you performed corrective actions, retry the operation. If you did not perform corrective actions or the problem persists, go to one of the following procedures.</p> <p>See <a href="#">“Resolving full disk problems”</a> on page 65.</p> <p>See <a href="#">“Frozen media troubleshooting considerations”</a> on page 66.</p> <p>See <a href="#">“About the conditions that cause media to freeze”</a> on page 67.</p> <p>See <a href="#">“Troubleshooting network interface card performance”</a> on page 88.</p>   |

## Device configuration problem resolution

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

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

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

**Table 2-5** Recommended actions for device configuration messages

| Message                                 | Explanation   | Recommended action   |
|---|---|--|
| Drive does not support serialization    | The drive does not return its serial number. Note that some manufacturers do not support serial numbers. Although automatic device configuration does not function optimally, the drive can be manually configured and operated without its serial number.  | Ask the manufacturer for a newer firmware version that returns serial numbers (if available), or manually configure and operate the drive without a serial number.   |
| Robot does not support serialization    | The robot does not return its serial number or the serial numbers of the drives that are contained within it. Note that some manufacturers do not support serial numbers. Although automatic device configuration does not function optimally, the robot and drives can be manually configured and operated without serial numbers. | Ask the manufacturer for a newer firmware version that returns serial numbers (if available). Or manually configure and operate the robot and drives without serial numbers.   |
| No license for this robot type          | NetBackup server does not support the robotic type that is defined for this robot.  | Define a different robot. Use only the robotic libraries that NetBackup server supports.   |
| No license for this drive type          | The drive type that is defined for this drive that the NetBackup server does not support.   | Define a different drive. Use only the drives that NetBackup supports  |
| Unable to determine robot type          | NetBackup does not recognize the robotic library. The robotic library cannot be auto-configured.  | Do the following: <ul style="list-style-type: none"> <li>■ Download a new device_mapping file from the Symantec Support website, and try again.</li> <li>■ Configure the robotic library manually.</li> <li>■ Use only the robotic libraries that NetBackup supports.</li> </ul> |
| Drive is standalone or in unknown robot | Either the drive is standalone, or the drive or robot does not return a serial number. Note that some manufacturers do not support serial numbers. Although automatic device configuration does not function optimally, the drive or robot can be manually configured and operated without a serial number.                         | Ask the manufacturer for a newer firmware version that returns serial numbers (if available), or manually configure and operate the drive robot without serial numbers.  |

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

| Message  | Explanation  | Recommended action  |
|--|--|---|
| Robot drive number is unknown  | Either the drive or robot does not return a serial number. Note that some manufacturers do not support serial numbers. Although automatic device configuration does not function optimally, the drive or robot can be manually configured and operated without a serial number.                            | Ask the manufacturer for a newer firmware version that returns serial numbers (if available). Or manually configure and operate the drive and robot without serial numbers.   |
| Drive is in an unlicensed robot  | The drive is in a robotic library that cannot be licensed for NetBackup server. Since the robot cannot be licensed for NetBackup server, any drives that were configured in that robot are unusable.   | Configure a drive that does not reside in the unlicensed robot.   |
| Drive's SCSI adapter does not support pass-thru (or pass-thru path does not exist) | A drive was found that does not have a SCSI pass-through path configured. The possible causes are: <ul style="list-style-type: none"> <li>■ The drive is connected to an adapter that does not support SCSI pass-through.</li> <li>■ The pass-through path for this drive has not been defined.</li> </ul> | Change the drive's adapter or define a pass-through path for the drive. For information about the SCSI adapter pass-through, see the <a href="#">NetBackup Device Configuration Guide</a> .   |
| No configuration device file exists  | A device has been detected without the corresponding device file necessary to configure that device.   | For directions about how to create device files, see the <a href="#">NetBackup Device Configuration Guide</a> .   |
| Unable to determine drive type   | The NetBackup server does not recognize the drive. The drive cannot be auto-configured.  | Do the following: <ul style="list-style-type: none"> <li>■ Download a new device_mapping file from the Symantec Support website, and try again.</li> <li>■ Configure the drive manually.</li> <li>■ Use only the drives that NetBackup supports.</li> </ul> |

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

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

## Testing the master server and clients

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

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

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

The explanations in these procedures assume that you are familiar with the backup processes and restore processes. For further information, see the *NetBackup Logging Reference Guide*.

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

See the [NetBackup Administrator's Guide, Volume I](#).

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

| Step   | Action                           | Description   |
|--------|----------------------------------|---|
| Step 1 | Enable debug logs.               | <p>Enable the appropriate debug logs on the master server.</p> <p>For information on logging, see the <i>NetBackup Logging Reference Guide</i>.</p> <p>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.</p>   |
| Step 2 | Configure a test policy.         | <p>Configure a test policy to use a basic disk storage unit.</p> <p>Or, configure a test policy and set the backup window to be open while you test. Name the master server as the client and a storage unit that is on the master server (preferably a nonrobotic drive). Also, configure a volume in the NetBackup volume pool and insert the volume in the drive. If you don't label the volume by using the <code>bplabel</code> command, NetBackup automatically assigns a previously unused media ID.</p>                   |
| Step 3 | Verify the daemons and services. | <p>To verify that the NetBackup daemons or services are running on the master server, do the following:</p> <ul style="list-style-type: none"> <li>■ To check the daemons on a UNIX system, enter the following command:           <pre style="margin-left: 20px;">/usr/openv/netbackup/bin/bpps -x</pre> </li> <li>■ To check the services on a Windows system, use the NetBackup Activity Monitor or the Services application of the Windows Control Panel.</li> </ul>  |
| Step 4 | Backup and restore a policy.     | <p>Start a manual backup of a policy by using the manual backup option in the NetBackup administration interface. Then, restore the backup.</p> <p>These actions verify the following:</p> <ul style="list-style-type: none"> <li>■ NetBackup server software is functional, which includes all daemons or services, programs, and databases.</li> <li>■ NetBackup can mount the media and use the drive you configured.</li> </ul>   |
| Step 5 | Check for failure.               | <p>If a failure occurs, check the job's <b>Detailed Status</b> in the <b>Activity Monitor</b>.</p> <p>You can also try the NetBackup <b>All Log Entries</b> report. For the failures that relate to drives or media, verify that the drive is in an UP state and that the hardware functions.</p> <p>To isolate the problem further, use the debug logs.</p> <p>For an overview of the sequence of processing, see the information on backup processes and restore processes in the <i>NetBackup Logging Reference Guide</i>.</p> |

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

| Step    | Action                                      | Description  |
|---------|---|--|
| Step 6  | Consult information besides the debug logs. | <p>If the debug logs do not reveal the problem, check the following:</p> <ul style="list-style-type: none"> <li>■ Systems Logs on UNIX systems</li> <li>■ Event Viewer and System logs on Windows systems</li> <li>■ Media Manager debug logs on the media server that performed the backup, restore, or duplication</li> <li>■ The bpdmm and bptmm debug logs on the media server that performed the backup, restore, or duplication</li> </ul> <p>See the vendor manuals for information on hardware failures.</p>   |
| Step 7  | Verify robotic drives.                      | <p>If you use a robot and the configuration is an initial configuration, verify that the robotic drive is configured correctly.</p> <p>In particular, verify the following:</p> <ul style="list-style-type: none"> <li>■ The same robot number is used both in the Media and Device Management and storage unit configurations.</li> <li>■ Each robot has a unique robot number.</li> </ul> <p>On a UNIX NetBackup server, you can verify only the Media and Device Management part of the configuration. To verify, use the <code>tpreq</code> 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, <code>tpunmount</code> the media.</p> |
| Step 8  | Include a robot in the test policy.         | <p>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.</p> <p>Return to step 3 and repeat this procedure for the robot. This procedure verifies that NetBackup can find the volume, mount it, and use the robotic drive.</p>  |
| Step 9  | Use the robotic test utilities.             | <p>If you have difficulties with the robot, try the test utilities.</p> <p>See <a href="#">“About the robotic test utilities”</a> on page 116.</p> <p>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.</p>  |
| Step 10 | Enhance the test policy.                    | <p>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.</p>  |

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

| Step    | Action                        | Description   |
|---------|-------------------------------|---|
| Step 11 | Backup and restore a file.    | <p>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.</p> <p>If a failure occurs, check the NetBackup <b>All Log Entries</b> report. To isolate the problem further, check the appropriate debug logs from the following list.</p> <p>On a UNIX system, the debug logs are in the <code>/usr/openv/netbackup/logs/</code> directory. On a Windows computer, the debug logs are in the <code>install_path\NetBackup\logs\</code> directory.</p> <p>Debug log directories exist for the following processes:</p> <ul style="list-style-type: none"> <li>■ <code>bparchive</code> (UNIX only)</li> <li>■ <code>bpbackup</code> (UNIX only)</li> <li>■ <code>bpbkar</code></li> <li>■ <code>bpcd</code></li> <li>■ <code>bplist</code></li> <li>■ <code>bprd</code></li> <li>■ <code>bprestore</code></li> <li>■ <code>nbwin</code> (Windows only)</li> <li>■ <code>bpinetd</code> (Windows only)</li> </ul> <p>Explanations about which logs apply to specific client types are available.</p> <p>For information on logging, see the <i>NetBackup Logging Reference Guide</i>.</p> |
| Step 12 | Reconfigure the test policy.  | <p>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.</p>  |
| Step 13 | Create debug log directories. | <p>Create debug log directories for the following processes:</p> <ul style="list-style-type: none"> <li>■ <code>bprd</code> on the server</li> <li>■ <code>bpcd</code> on the client</li> <li>■ <code>bpbkar</code> on the client</li> <li>■ <code>nbwin</code> on the client (Windows only)</li> <li>■ <code>bpbackup</code> on the client (except Windows clients)</li> <li>■ <code>bpinetd</code> (Windows only)</li> <li>■ <code>tar</code></li> <li>■ On the media server: <code>bpbrm</code>, <code>bpdm</code>, and <code>bptm</code></li> </ul> <p>Explanations about which logs apply to specific client types are available.</p> <p>For information on logging, see the <i>NetBackup Logging Reference Guide</i>.</p>   |

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

| Step    | Action   | Description  |
|---------|--|--|
| Step 14 | Verify communication between the client and the master server. | <p>Perform a user backup and then a restore from the client that is specified in step 8. These actions verify communications between the client and the master server, and NetBackup software on the client.</p> <p>If an error occurs, check the job's <b>Detailed Status</b> in the <b>Activity Monitor</b>.<br/> check the <b>All Log Entries</b> report and the debug logs that you created in the previous step. A likely cause for errors is a communications problem between the server and the client.</p> |
| Step 15 | Test other clients or storage units.                           | When the test policy operates satisfactorily, repeat specific steps as necessary to verify other clients and storage units.  |
| Step 16 | Test the remaining policies and schedules.                     | When all clients and storage units are functional, test the remaining policies and schedules that use storage units on the master server. If a scheduled backup fails, check the <b>All Log Entries</b> report for errors. Then follow the recommended actions as is part of the error status code.  |

## Testing the media server and clients

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

See [“Testing the master server and clients”](#) on page 33.

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

| Step   | Action                    | Description   |
|--------|---------------------------|---|
| Step 1 | Enable legacy debug logs. | <p>Enable appropriate legacy debug logs on the servers, by entering the following:</p> <p>UNIX/Linux: <code>/usr/opensv/netbackup/logs/mklogdir</code></p> <p>Windows: <code>install_path\NetBackup\logs\mklogdir.bat</code></p> <p>See the <a href="#">NetBackup Logging Reference Guide</a>.</p> <p>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.</p> |

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

| Step   | Action  | Description  |
|--------|---|--|
| Step 2 | Configure a test policy.  | <p>Configure a test policy with a user schedule (set the backup window to be open while you test) by doing the following:</p> <ul style="list-style-type: none"> <li>■ Name the media server as the client and a storage unit that is on the media server (preferably a nonrobotic drive).</li> <li>■ 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.</li> <li>■ Insert the volume in the drive. If you do not pre-label the volume by using the <code>bplabel</code> command, NetBackup automatically assigns a previously unused media ID.</li> </ul>   |
| Step 3 | Verify the daemons and services.                                      | <p>Verify that all NetBackup daemons or services are running on the master server. Also, verify that all Media and Device Management daemons or services are running on the media server.</p> <p>To perform this check, do one of the following:</p> <ul style="list-style-type: none"> <li>■ On a UNIX system, run:           <pre style="margin-left: 20px;">/usr/openv/netbackup/bin/bpps -x</pre> </li> <li>■ On a Windows system, use the Services application in the Windows Control Panel.</li> </ul>   |
| Step 4 | Backup and restore a file.  | <p>Perform a user backup and then a restore of a file from a client that has been verified to work with the master server.</p> <p>This test verifies the following:</p> <ul style="list-style-type: none"> <li>■ NetBackup media server software.</li> <li>■ NetBackup on the media server can mount the media and use the drive that you configured.</li> <li>■ Communications between the master server processes <code>nbpem</code>, <code>nbjm</code>, <code>nbrb</code>, EMM server process <code>nbemm</code>, and media server processes <code>bpcd</code>, <code>bpbrm</code>, <code>bpdm</code>, and <code>bptm</code>.</li> <li>■ Communications between media server process <code>bpbrm</code>, <code>bpdm</code>, <code>bptm</code>, and client processes <code>bpcd</code> and <code>bpkar</code>.</li> </ul> <p>For the failures that relate to drives or media, ensure that the drive is in an UP state and that the hardware functions.</p> |
| Step 5 | Verify communication between the master server and the media servers. | <p>If you suspect a communications problem between the master server and the media servers, check the debug logs for the pertinent processes.</p> <p>If the debug logs don't help you, check the following:</p> <ul style="list-style-type: none"> <li>■ On a UNIX server, the System log</li> <li>■ On a Windows server, the <b>Event Viewer</b> Application and System log</li> <li>■ <code>vmd</code> debug logs</li> </ul>   |

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

| Step   | Action                                   | Description  |
|--------|--|--|
| Step 6 | Ensure that the hardware runs correctly. | <p>For the failures that relate to drives or media, ensure that the drive is running and that the hardware functions correctly.</p> <p>See the vendor manuals for information on hardware failures.</p> <p>If you use a robot in an initial configuration condition, verify that the robotic drive is configured correctly.</p> <p>In particular, verify the following:</p> <ul style="list-style-type: none"> <li>■ The same robot number is used both in the Media and Device Management and storage unit configurations.</li> <li>■ Each robot has a unique robot number.</li> </ul> <p>On a UNIX server, you can verify only the Media and Device Management part of the configuration. To verify, use the <code>tpreq</code> command to request a media mount. Verify that the mount completes and check the drive on which the media was mounted. Repeat the process until the media is mounted and unmounted on each drive from the host where the problem occurred. Perform these steps from the media server. If this works, the problem is probably with the policy or the storage unit configuration on the media server. When you are done, use <code>tpunmount</code> to unmount the media.</p> |

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

| Step   | Action                                       | Description   |
|--------|--|---|
| Step 7 | Include a robotic device in the test policy. | <p>If you previously configured a non-robotic drive and a robot was attached to your media server, change the test policy to name the robot. Also, add a volume for the robot to the EMM server. Verify that the volume is in the NetBackup volume pool and in the robot.</p> <p>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.</p> <p>If a failure occurs, check the NetBackup <b>All Log Entries</b> report. Look for any errors that relate to devices or media.</p> <p>See the <a href="#">NetBackup Administrator's Guide, Volume I</a>.</p> <p>If the <b>All Log Entries</b> report doesn't help, check the following:</p> <ul style="list-style-type: none"> <li>■ On a UNIX server, the system logs on the media server</li> <li>■ <code>vm.d</code> debug logs on the EMM server for the robot</li> <li>■ On a Windows system, the <b>Event Viewer</b> Application and System log</li> </ul> <p>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.</p> <p>Try the test utilities.</p> <p>See "<a href="#">About the robotic test utilities</a>" on page 116.</p> <p>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.</p> |
| Step 8 | Test other clients or storage units.         | When the test policy operates satisfactorily, repeat specific steps as necessary to verify other clients and storage units.   |
| Step 9 | Test the remaining policies and schedules.   | When all clients and storage units are in operation, test the remaining policies and schedules that use storage units on the media server. If a scheduled backup fails, check the <b>All Log Entries</b> report for errors. Then follow the suggested actions for the appropriate status code.  |

## Resolving network communication problems with UNIX clients

The following procedure is for resolving NetBackup communications problems, such as those associated with NetBackup status codes 25, 54, 57, and 58. This

procedure consists of two variations: one for UNIX clients and another for Windows clients.

---

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

---

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

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

| Step   | Action  | Description   |
|--------|---|---|
| Step 1 | Create debug log directories.                       | <p>During communication retries, the debug logs provide detailed debug information, which can help you analyze the problem.</p> <p>Create the following directories:</p> <ul style="list-style-type: none"> <li>■ <code>bpcd</code> (on the master server and clients)</li> <li>■ <code>vnetd</code> (on the master server and clients)</li> <li>■ <code>bprd</code> (on the master server)</li> </ul> <p>Use the <code>bprd</code> log directory to debug client to master server communication, not client to media server communication problems.</p>  |
| Step 2 | Test a new configuration or modified configuration. | <p>If this configuration is a new or a modified configuration, do the following:</p> <ul style="list-style-type: none"> <li>■ Check any recent modifications to ensure that they did not introduce the problem.</li> <li>■ Ensure that the client software was installed and that it supports the client operating system.</li> <li>■ Check the client names, server names, and service entries in your NetBackup configuration as explained in the following topic:<br/>See <a href="#">“Verifying host name and service entries in NetBackup”</a> on page 53.</li> </ul> <p>You can also use the <code>hostname</code> command on the client to determine the host name that the client sends with requests to the master server. Check the <code>bprd</code> debug log on the master server to determine what occurred when the server received the request.</p> |

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

| Step   | Action                       | Description   |
|--------|------------------------------|---|
| Step 3 | Verify name resolution.      | <p>To verify name resolution, run the following command on the master server and the media servers:</p> <pre># bpclntcmd -hn <i>client name</i></pre> <p>If the results are unexpected, review the configuration of these name resolution services: <i>nsswitch.conf</i> file, <i>hosts</i> file, <i>ipnodes</i> file, and <i>resolv.conf</i> file.</p> <p>Also run the following on the client to check forward and reverse name lookup of the master server and media server that perform the backup:</p> <pre># bpclntcmd -hn <i>server name</i> # bpclntcmd -ip <i>IP address of server</i></pre>   |
| Step 4 | Verify network connectivity. | <p>Verify network connectivity between client and server by pinging the client from the server.</p> <pre># ping <i>clientname</i></pre> <p>Where <i>clientname</i> is the name of the client as configured in the NetBackup policy configuration.</p> <p>For example, to ping the policy client that is named <i>ant</i>:</p> <pre># 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</pre> <p>A successful ping verifies connectivity between the server and client. If the ping fails and ICMP is not blocked between the hosts, resolve the network problem outside of NetBackup before you proceed.</p> <p>Some forms of the ping command let you ping the <i>bpcd</i> port on the client as in the following command:</p> <pre># ping ant 13782</pre> <p>Ping 1556 (<i>PBX</i>), 13724 (<i>vnetd</i>), and 13782 (<i>bpcd</i>) in sequence, the same sequence that NetBackup tries by default. You then know which ports are closed so that you can open them or adjust the Connect Options for more efficient connection tries.</p> |

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

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

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

| Step   | Action   | Description   |
|--------|--|---|
| Step 6 | Connect to the client through telnet.            | <p>On the client, telnet to 1556 (PBX), 13724 (vnetd), and 13782 (bpcd). Check all three ports to make sure that a connection is made on at least one of them, then modify the NetBackup configuration accordingly. If the telnet connection succeeds, keep the connection until after you perform step 8, then terminate it with Ctrl-c.</p> <pre>telnet clientname 1556 telnet clientname 13724 telnet clientname 13782</pre> <p>Where <i>clientname</i> is the name of the client as configured in the NetBackup policy configuration.</p> <p>For example,</p> <pre># 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. <p>Repeat the procedure on the master server(s) and media server(s), to test communication to the client.</p> </pre>  |
| Step 7 | Identify the outbound socket on the server host. | <p>On the master server(s) and media server(s): Use the following command to identify the outbound socket that is used for the telnet command from step 6. Specify the appropriate IP address to which the server resolves the policy client. Note the source IP (10.82.105.11), the source port (45856) and the destination port (1556).</p> <pre># netstat -na   grep '&lt;client_IP_address&gt;'   egrep '1556 13724 13782 ' 10.82.105.11.45856 10.82.104.99.1556 49152 0 49152 0 ESTABLISHED</pre> <p>If telnet is still connected and a socket is not displayed: Remove the port number filtering and observe the port number to which the site has mapped the service name. Check that process listens on the port number in step 5.</p> <pre>\$ netstat -na   grep '&lt;client_IP_address&gt;' 10.82.105.11.45856 10.82.104.99.1234 49152 0 49152 0 ESTABLISHED</pre> <p>If the socket is in a SYN_SENT state instead of an ESTABLISHED state, the server host is trying to make the connection. However, a firewall blocks the outbound TCP SYN from reaching the client host or blocks the return bound TCP SYN+ACK from reaching the server host.</p> |

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

| Step   | Action   | Description  |
|--------|--|--|
| Step 8 | Confirm that the telnet connection reaches this client host.   | <p>On the master server(s) and media server(s), to confirm that the telnet connection reaches this client host, run the following command:</p> <pre>\$ netstat -na   grep '&lt;source_port&gt;'</pre> <pre>10.82.104.99.1556 10.82.105.11.45856 49152 0 49152 0 ESTABLISHED</pre> <p>One of the following conditions occurs:</p> <ul style="list-style-type: none"> <li>■ If telnet is connected but the socket is not present: The telnet reached some other host that incorrectly shares the same IP address as the client host.</li> <li>■ If the socket is in a SYN_RCVD state instead of an ESTABLISHED state, then the connection reached this client host. However, a firewall blocks the return of the TCP SYN+ACK to the server host.</li> </ul>  |
| Step 9 | Verify communication between the client and the master server. | <p>To verify client to master server communications, use the <code>bpclntcmd</code> utility. When <code>-pn</code> and <code>-sv</code> run on a NetBackup client, they initiate inquiries to the NetBackup master server (as configured in the client <code>bp.conf</code> file). The master server then returns information to the requesting client. More information is available about <code>bpclntcmd</code>.</p> <p>See <a href="#">“About the bpclntcmd utility”</a> on page 62.</p> <p>If you confirm connectivity from the server host to the client host through PBX (port 1556) or to both <code>bpccd</code> (port 13782) and <code>vnetd</code> (port 13724), note: The PBX, <code>bpccd</code>, or <code>vnetd</code> debug logs should provide details on the nature of any remaining failure.</p> |

## Resolving network communication problems with Windows clients

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

---

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

---

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

### To resolve network communication problems

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

- Increase the logging level on the client (see the *NetBackup Administrator's Guide, Volume I*, under "Client Settings properties").
  - On the NetBackup master server, create a `bprcd` debug log directory and on the clients create a `bpcd` debug log.
  - On the NetBackup server, set the **Verbose** level to 1.  
See the [NetBackup Logging Reference Guide](#) for help changing the logging level.
- 2 If this client is new, verify the client and the server names in your NetBackup configuration.  
See "[Verifying host name and service entries in NetBackup](#)" on page 53.
- 3 Verify network connectivity between client and server by pinging from the server to the client and vice versa. Use the following command:

```
# ping hostname
```

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

- NetBackup policy configuration
- WINS
- DNS (if applicable).
- `hosts` file in system directory `%SystemRoot%\system32\drivers\etc\hosts` (Windows 2003 or 2008)

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

If `ping` fails, you have a network problem outside of NetBackup that must be resolved before you proceed. As a first step, verify that the workstation is turned on. A workstation that is not turned on is a common source of connection problems with workstations.

- 4 On Microsoft Windows clients, ensure that the NetBackup Client service is active by checking the logs. Use the Services application in the Control Panel to verify that the NetBackup Client service is running. Start it if necessary.
- Check the `bpcd` debug logs for problems or errors. See the *NetBackup Logging Reference Guide* on how to enable and use these logs.
  - Verify that the same NetBackup client service (`bpcd`) port number is specified on both the NetBackup client and server (by default, 13782). Do one of the following:

Windows

Check the NetBackup client service port number.

Start the **Backup, Archive, and Restore** interface on the client. On the **File** menu, click **NetBackup Client Properties**. In the **NetBackup Client Properties** dialog box on the **Network** tab, check the NetBackup client service port number.

Verify that the setting on the **Network** tab matches the one in the services file. The `services` file is located in:

```
%SystemRoot%\system32\drivers\etc\services
(Windows)
```

The values on the **Network** tab are written to the `services` file when the NetBackup client service starts.

UNIX NetBackup servers

The `bpcd` port number is in the `/etc/services` file. On Windows NetBackup servers, see the Client Properties dialog box in the **Host Properties** window.

See [“Using the Host Properties window to access configuration settings”](#) on page 64.

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

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

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

|                           |   |
|---------------------------|---|
| Windows clients           | <p>Check the NetBackup client service port number.</p> <p>Start the <b>Backup, Archive, and Restore</b> interface on the client. On the <b>File</b> menu, click <b>NetBackup Client Properties</b>. In the <b>NetBackup Client Properties</b> dialog box on the <b>Network</b> tab, check the NetBackup client service port number.</p> <p>Verify that the setting on the <b>Network</b> tab matches the one in the services file. The <code>services</code> file is located in:</p> <pre style="margin-left: 20px;">%SystemRoot%\system32\drivers\etc\services (Windows)</pre> <p>The values on the <b>Network</b> tab are written to the <code>services</code> file when the NetBackup client service starts.</p> |
| UNIX NetBackup servers    | <p>The <code>bprd</code> port number is in the <code>/etc/services</code> file.</p> <p>See <a href="#">“Using the Host Properties window to access configuration settings”</a> on page 64.</p>  |
| Windows NetBackup servers | <p>Set these numbers in the <b>Client Properties</b> dialog box in the <b>Host Properties</b> window.</p> <p>See <a href="#">“Using the Host Properties window to access configuration settings”</a> on page 64.</p>  |

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

|              |  |
|--------------|--|
| Windows 2003 | <code>%SystemRoot%\system32\drivers\etc\hosts</code> |
| UNIX         | <code>/etc/hosts</code>                              |

- 7 Verify client-to-server connectability by means of `ping` or its equivalent from the client (step 3 verified the server-to-client connection).
- 8 If the client’s TCP/IP transport allows `telnet` and `ftp` from the server, try these services as additional connectivity checks.

- 9 Use the `bpcIntcmd` utility to verify client to master server communications. When the `-pn` and `-sv` options run on a client, they initiate inquiries to the master server (configured in the server list on the client). The master server then returns information to the requesting client.  
 See “About the `bpcIntcmd` utility” on page 62.
- 10 Use the `bptestbpcd` utility to try to establish a connection from a NetBackup server to the `bpcd` daemon on another NetBackup system. If successful, it reports information about the sockets that are established.  
 A complete description of `bptestbpcd` is in the [NetBackup Commands Reference Guide](#).
- 11 Verify that the client operating system is one of those supported by the client software.

## About troubleshooting networks and host names

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

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

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

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

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

Connection from host *peername* *ipaddress* ...

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

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

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

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

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

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

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

These comparisons are recorded 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/opensv/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. The second output line is the server's response in the following order:

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

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

- Browse client
- Requesting client
- Destination client

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

See the [NetBackup Administrator's Guide, Volume I](#).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
key hostname_from_client client_as_known_by_server
```

The following describes the preceding variables:

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

This following is an example:

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

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

- The client's `gethostname()` function returns `danr`.
- The master server's network services `gethostbyname()` function did not recognize the name `danr`.
- The client was configured and named in the NetBackup configuration as `danr.eng.aaa.com` and this name is also known to network services on the master server.

## Verifying host name and service entries in NetBackup

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

For more information on host names, see the [NetBackup Administrator's Guide, Volume II](#).

See ["About troubleshooting networks and host names"](#) on page 49.

### To verify the host name and service entries in NetBackup

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

On Windows servers  
and Windows clients

Do the following:

- On the **Server to use for backups and restores** drop-down list, ensure that a server entry exists for the master server and each media server.  
 Start the **Backup, Archive, and Restore** interface on the client. On the **File** menu, click **Specify NetBackup Machines and Policy Type**. In the **Specify NetBackup Machines and Policy Type** dialog box, click the **Server to use for backups and restores** drop-down list.  
 On Windows computers, 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 the **General** tab, verify that the client name setting is correct and matches what is in the policy client list on the master server.  
 Start the **Backup, Archive, and Restore** interface on the client. On the **File** menu, click **NetBackup Client Properties**. In the **NetBackup Client Properties** dialog box, click the **General** tab.
- On a master or a media server, ensure that a server entry exists for each Windows administrative client to use to administer that server.
- Ensure that host names are spelled correctly in the `bp.conf` file (UNIX) or in the servers list (Windows) on the master server. If a host name is misspelled or cannot be resolved with `gethostbyname`, the following error messages are logged on the NetBackup error log:

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

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

See [“Using the Host Properties window to access configuration settings”](#) on page 64.

On UNIX NetBackup servers and clients and Macintosh clients

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

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

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

UNIX client users 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/opensv/netbackup/bp.conf`.

On the master server

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

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

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

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

The following examples show the default port numbers.

See [“Example of host name and service entries on UNIX master server and client”](#) on page 57.

See [“Example of host name and service entries on UNIX master server and media server”](#) on page 58.

See [“Example of host name and service entries on UNIX PC clients”](#) on page 59.

See [“Example of host name and service entries on UNIX server that connects to multiple networks”](#) on page 60.

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

- 3 On NetBackup servers, check the services files to ensure that they have entries for the following:
  - `bpcd` and `bprd`

- vmd
- bpdbm
- Processes for configured robots (for example, `t18cd`).  
 See the [NetBackup Device Configuration Guide](#).

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

On UNIX clients      Check the `bprd` and the `bpcd` entries in the `/etc/services` file.

On Microsoft Windows clients      Verify that the NetBackup Client Service Port number and NetBackup Request Service Port number match settings in the `services` file by doing the following:

Start the Backup, Archive, and Restore interface on the client. On the **File** menu, click **NetBackup Client Properties**. In the **NetBackup Client Properties** dialog box on the **Network** tab, select the following: The NetBackup Client Service Port number and NetBackup Request Service Port number.

The values on the **Network** tab are written to the `services` file when the NetBackup Client service starts.

The `services` file is in the following location:

```
%SystemRoot%\system32\drivers\etc\services
```

- 4 On UNIX servers and clients, ensure that the `bpcd -standalone` process is running.
- 5 On Windows servers and clients, verify that the NetBackup Client service is running.
- 6 If you use NIS in your network, update those services to include the NetBackup information that is added to the `/etc/services` file.
- 7 NIS, WINS, or DNS host name information must correspond to what is in the policy configuration and the name entries. On Windows NetBackup servers and Microsoft Windows clients, do the following:
  - Check the **General** tab:  
 Start the **Backup, Archive, and Restore** interface on the client. On the **File** menu, click **NetBackup Client Properties**. In the **NetBackup Client Properties** dialog box, click the **General** tab.
  - Check the **Server to use for backups and restores** drop-down list:

Start the **Backup, Archive, and Restore** interface on the client. On the **File** menu, click **Specify NetBackup Machines and Policy Type**. In the **Specify NetBackup Machines and Policy Type** dialog box, click the **Server to use for backups and restores** drop-down list.

- The `bp.conf` file on UNIX servers and clients and Macintosh clients.
  - Verify that reverse DNS addressing is configured.
- 8 Use the `bpclntcmd` utility to confirm the setup of the IP addresses and host names in DNS, NIS, and local hosts files on each NetBackup node.

---

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

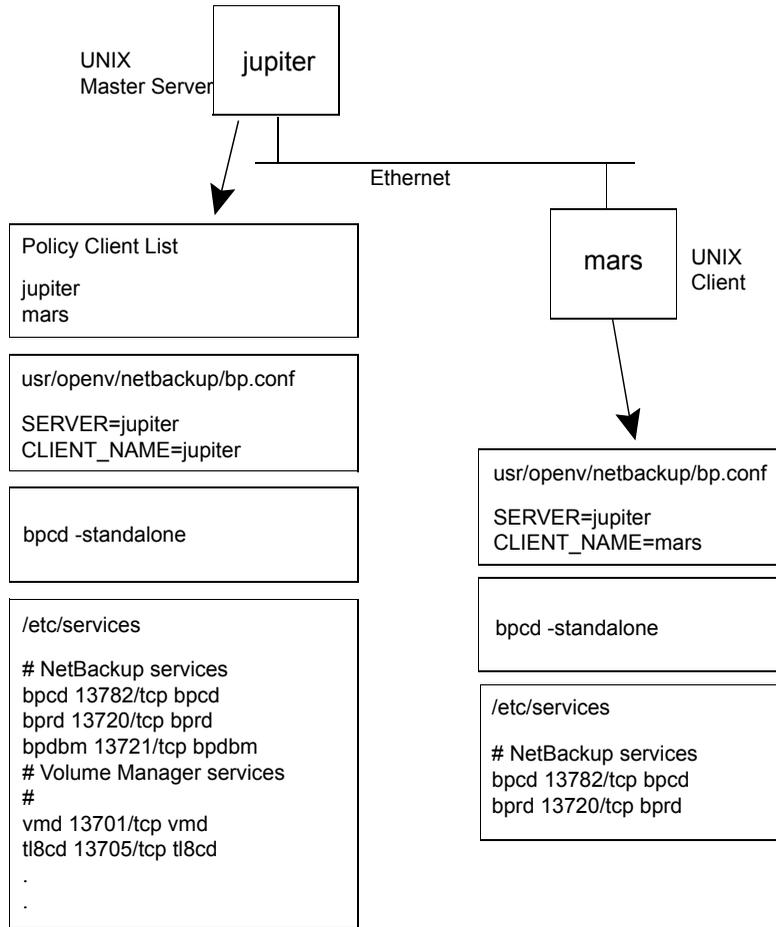
---

See [“About the bpclntcmd utility”](#) on page 62.

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

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

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



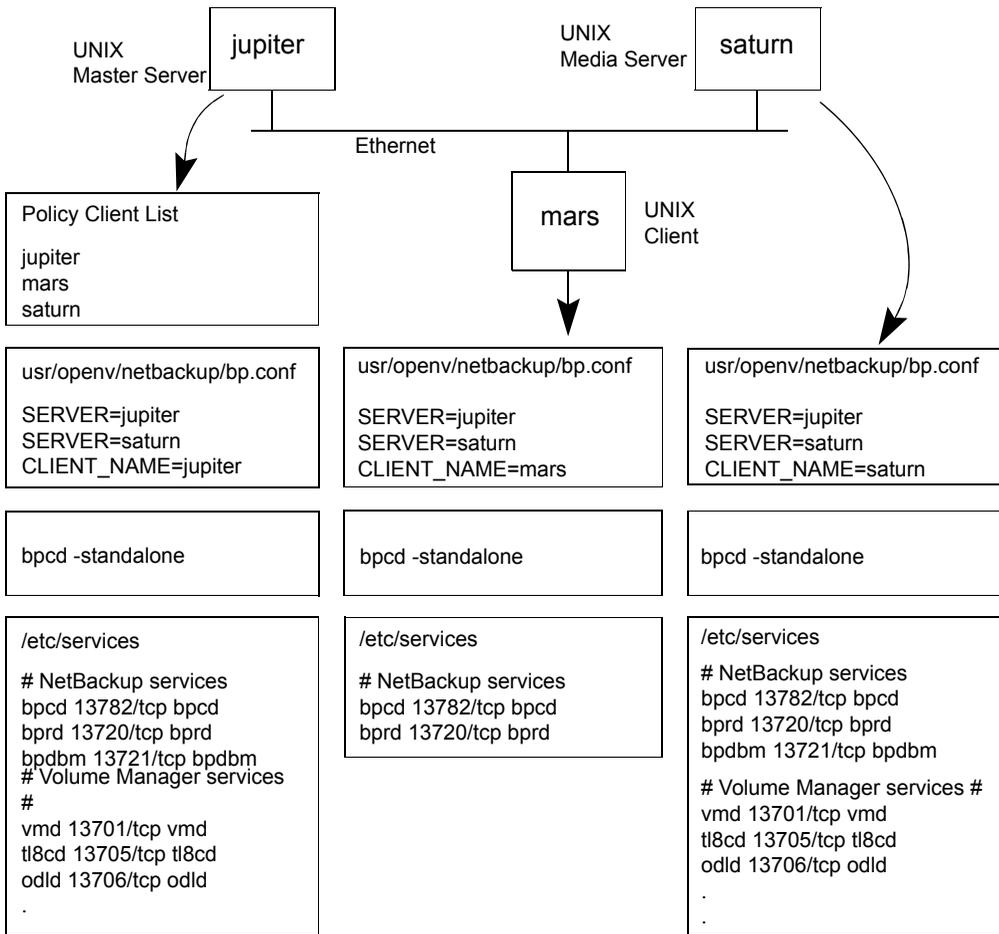
Consider the following about [Figure 2-1](#):

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

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

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

Figure 2-2 UNIX master and media servers



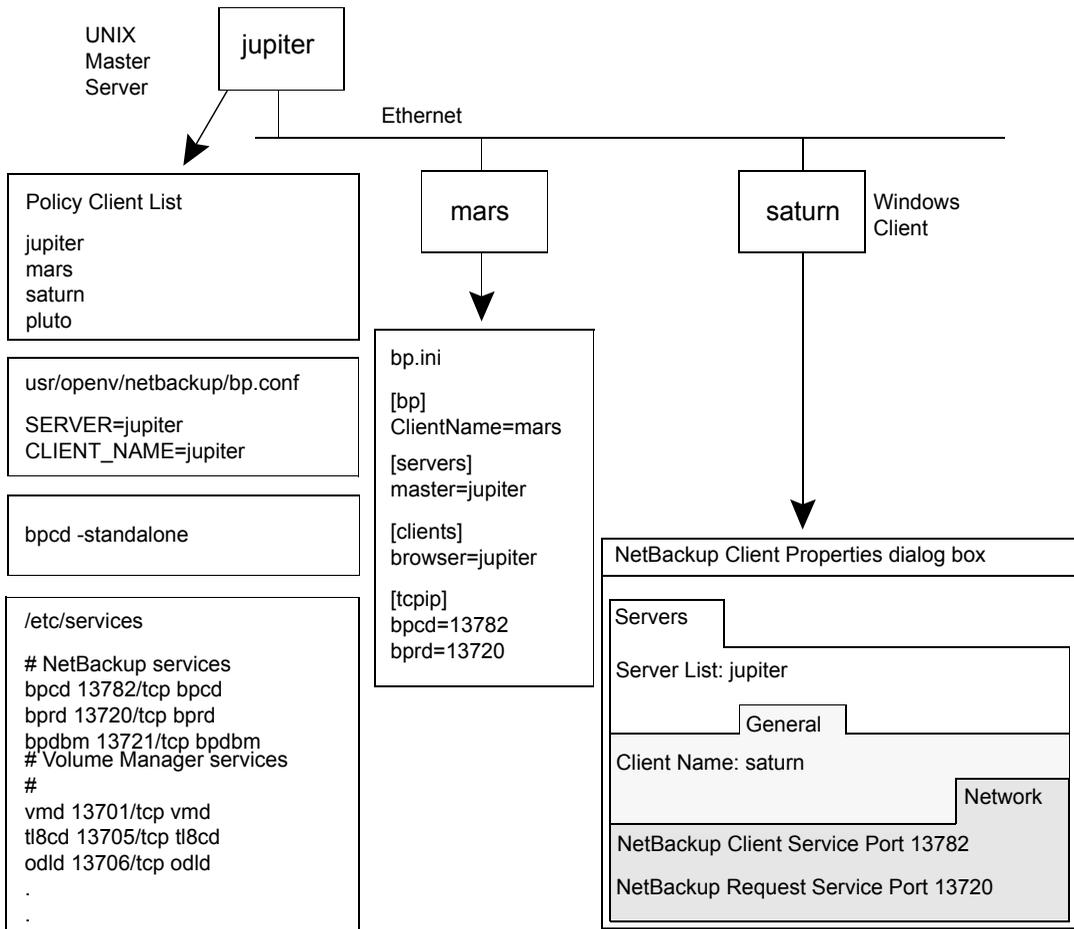
Consider the following about [Figure 2-2](#):

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

## Example of host name and service entries on UNIX PC clients

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

Figure 2-3 UNIX PC clients



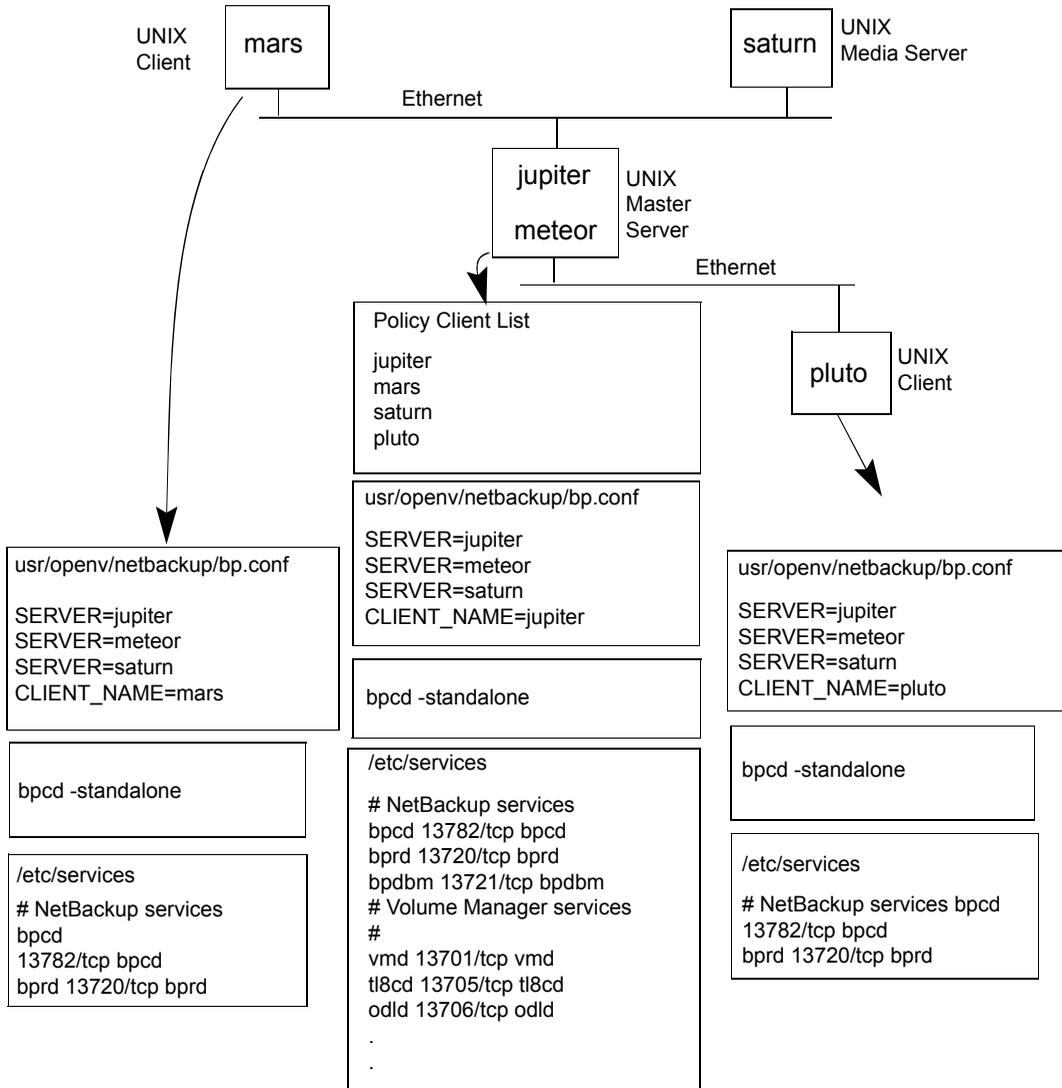
Consider the following about [Figure 2-3](#):

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

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

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

**Figure 2-4** UNIX server connects to multiple networks



Consider the following about [Figure 2-4](#):

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

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

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

The NetBackup server list for the other computers 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 computer 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.

## About the bpcIntcmd utility

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

|         |   |
|---------|---|
| Windows | <code>install_path\NetBackup\bin</code> |
| UNIX    | <code>/usr/opensv/netbackup/bin</code>  |

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

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

`-ip`      `bpcIntcmd -ip IP_Address`

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

`-hn`      `bpcIntcmd -hn Hostname`

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

`-sv`      `bpcIntcmd -sv`

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

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

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

The following is true of this command example:

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

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

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

- On the NetBackup server, use `bpcIntcmd -hn` to verify the following: The operating system can resolve the host name of the NetBackup client (as configured in the client list for the policy) to an IP address. The IP address is

then used in the node's routing tables to route a network message from the NetBackup server.

- On the NetBackup client, use `bpcIntcmd -ip` to verify that the operating system can resolve the IP address of the NetBackup server. (The IP address is in the message that arrives at the client's network interface.)

---

**Note:** The `bpcIntcmd` command logs messages to the `usr/opensv/netbackup/logs/bpcIntcmd` directory (UNIX) or the `install_path\NetBackup\logs\bpcIntcmd` (Windows). For earlier versions of NetBackup, `bpcIntcmd` logs are sent to the `bplist` directory, not the `bpcIntcmd` directory.

---

## Using the Host Properties window to access configuration settings

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

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

### To use the Host Properties window to access configuration settings

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

# Resolving full disk problems

If NetBackup is installed on a disk or a file system that fills up, such as with logging files, a number of problems can result. NetBackup may become unresponsive. For example, NetBackup jobs may remain queued for long periods, even though all NetBackup processes and services are running.

## To resolve the full disk problems that are caused by NetBackup log files

- 1 Clear up disk space in the directory where NetBackup is installed by doing the following:
  - You may need to delete log files manually, reduce logging levels, and adjust log retention to have log files automatically deleted sooner.  
See the [NetBackup Logging Reference Guide](#) for more information about logging levels, log file retention, and how to configure unified logging.
  - Consider moving the NetBackup unified logging files to a different file system.

- 2 Use the Activity Monitor to verify that the NetBackup relational database service is running.

This service is the `NB_dbdrv` daemon on UNIX and the NetBackup Relational Database Manager 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.

- 4 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.

## To resolve full disk problems on the NBDB file system

- 1 Shut down the NetBackup daemons.
- 2 Compress the staging directory and put a copy in a safe location.

UNIX: `/usr/opensv/db/staging`

Windows: `install_path\VERITAS\NetBackupDB\staging`

This copy is a backup of the database as of the last catalog backup.

**3 Run a validation on the database:**

**UNIX:** `/usr/opensv/db/bin/nbdb_admin -validate -full -verbose`

**Windows:** `install_path\VERITAS\NetBackup\bin\ nbdb_admin -validate -full -verbose`

If validation fails, contact Veritas Support.

**4 If validation succeeds, run a database rebuild:**

**UNIX:** `/usr/opensv/db/bin/ >nbdb_unload -rebuild -verbose`

**Windows:** `install_path\VERITAS\NetBackup\bin\ >nbdb_unload -rebuild -verbose`

If the rebuild fails, contact Veritas Support.

**5 If the rebuild succeeded, run the validation on the database again (step 3).**

If this validation fails, contact Veritas Support.

**6 Start the NetBackup daemons.**

**7 As soon as possible, add additional space to the file system that contains NBDB.**

**To resolve full disk problems on other file systems (such as binaries, root, or image catalog)**

- 1 Shut down the NetBackup daemons.
- 2 Determine the cause for the full file system and take corrective actions.
- 3 Start the NetBackup daemons.
- 4 Verify that the NetBackup daemons run without abnormal termination or errors.  
If errors occur, contact Veritas Support.

## Frozen media troubleshooting considerations

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

When troubleshooting frozen media, be aware of the following:

- Use the `bpmedialist` command to access the `MediaDB` information including the media status (Frozen, Full, or Active).
- To unfreeze the media, use the `bpmedia` command. Specify the media server that contains that frozen record in the command syntax. Unfreeze the media one at a time.

- Frozen media does not necessarily mean that the media is defective. NetBackup may freeze media as a safety measure to prevent further errors, drive damage, or data loss.
- Investigate any patterns to the media IDs, tape drives, or media servers that are involved when media is frozen.

## Logs for troubleshooting frozen media

The following logs are useful when you troubleshoot frozen media:

- |         |   |
|---------|---|
| UNIX    | <ul style="list-style-type: none"> <li>■ The <code>bptm</code> log from the media servers that froze the media:<br/><br/><code>/usr/opensv/netbackup/logs/bptm</code></li> <li>■ The Admin messages or syslog from the operating system.</li> </ul>   |
| Windows | <ul style="list-style-type: none"> <li>■ The <code>bptm</code> log from the media servers that froze the media:<br/><br/><code>install_dir\VERITAS\NetBackup\logs\bptm</code></li> <li>■ The Windows Event Viewer System Log</li> <li>■ The Windows Event Viewer Application Log</li> </ul> |

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

See [“Frozen media troubleshooting considerations”](#) on page 66.

See [“About the conditions that cause media to freeze”](#) on page 67.

## About the conditions that cause media to freeze

The following conditions can cause media to freeze:

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

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

The causes and the resolutions for this problem include:

|  |  |
|--|--|
| Dirty drives   | Clean the drives that are freezing the media according to the manufacturer's suggestions. Frozen media is one of the first symptoms of a dirty drive.  |
| The drive itself   | Check for the tape device errors that the operating system logs or the device driver reports. If any are found, follow the hardware manufacturer's recommendations for this type of error.   |
| Communication issues at the SCSI or host bus adapter (HBA) level | Check for SCSI or HBA device errors the operating system logs or the device driver reports. If any are found, follow the hardware manufacturer's recommendations for this type of error.   |
| Drive not supported  | Ensure that the tape drives appear on the hardware compatibility list as supported for NetBackup. This list is located on the following Symantec Support website:<br><br><a href="http://www.symantec.com/business/support/overview.jsp?pid=15143">http://www.symantec.com/business/support/overview.jsp?pid=15143</a> |
| Media not supported  | Ensure that the media is supported for use with the tape drive by the tape drive vendor.   |

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

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

The following conditions can cause this error:

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

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

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

These library tapes may have been written outside of NetBackup. By default, NetBackup only writes to a blank media or other NetBackup media. Other media types (DBR, TAR, CPIO, ANSI, MTF1, and recycled Backup Exec BE-MTF1 media) are frozen as a safety measure. Change this behavior by using the following procedure:

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

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

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

On Windows On the **NetBackup Administration Console**, proceed to **Host Properties > Media Server**

Open the properties for the media server in question.

Select the **Media** tab.

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

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

For more details about each media type, see the [NetBackup Device Configuration Guide](#).

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

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

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

- The media is intentionally frozen. You can use the `bpmedia` command to manually freeze media for a variety of administrative reasons. If no record exists of a specific job freezing the media, the media may have been frozen manually.
- The media is physically write protected. If the media has a write-protect notch that is set for write protection, NetBackup freezes the media.

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

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

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

```
# bpmedialist -m div008
```

```
Server Host = denton
```

| ID    | rl images | allocated  | last updated     | density          | kbytes | restores |   |
|-------|-----------|------------|------------------|------------------|--------|----------|---|
|       | vimages   | expiration | last read        | <-----           | STATUS | ----->   |   |
| DIV08 | 1         | 1          | 04/22/2014 10:12 | 04/22/2014 10:12 | hcart  | 35       | 5 |
|       |           | 1          | 05/06/2014 10:12 | 04/22/2014 10:25 | FROZEN |          |   |

## Resolving PBX problems

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

### To resolve PBX problems

- 1 Check that the PBX is properly installed. If PBX is not installed, NetBackup is unresponsive. Refer to the following procedure:  
 See [“Checking PBX installation”](#) on page 71.
- 2 Check that PBX is running, and initiate PBX if necessary by using the following procedure:  
 See [“Checking that PBX is running”](#) on page 71.

- 3 Check that PBX is correctly configured. If PBX is incorrectly configured, NetBackup is unresponsive. Refer to the following procedure:  
 See [“Checking that PBX is set correctly”](#) on page 72.
- 4 Access and check the PBX logs by using the following procedure:  
 See [“Accessing the PBX logs”](#) on page 73.
- 5 Check the PBX security and correct any problem by using the following procedure:  
 See [“Troubleshooting PBX security”](#) on page 74.
- 6 Check that the required NetBackup daemon or service is running. If necessary, start the needed daemon or service by using the following procedure:  
 See [“Determining if the PBX daemon or service is available”](#) on page 76.

## Checking PBX installation

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

See the [NetBackup Installation Guide](#).

If you uninstall PBX, you must reinstall it.

### To check PBX installation

- 1 Look for the following directory on the NetBackup master server:
  - On Windows: `install_path\VxPBX`
  - On UNIX: `/opt/VRTSspb`
- 2 To check the version of PBX, enter the following:
  - On Windows: `install_path\VxPBX\bin\pbxcfg -v`
  - On UNIX: `/opt/VRTSspb/bin/pbxcfg -v`

## Checking that PBX is running

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

### To see if PBX is running

- 1 On UNIX, check for the PBX process:

```
ps | grep pbx_exchange
```

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

```
/opt/VRTSspbx/bin/vxpbx_exchanged start
```

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

## Checking that PBX is set correctly

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

### To check that PBX is set correctly

- 1 To display the current PBX settings, do one of the following:
  - On Windows, type the following:

```
install_path\VxPBX\bin\pbxcfg -p
```

Example output:

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

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

- On UNIX, type the following:

```
/opt/VRTSspbx/bin/pbxcfg -p
```

Example output:

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

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

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

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

```
/opt/VRTSpx/bin/pbxcfg -a -u root
```

- To set Secure Mode to false:

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

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

## Accessing the PBX logs

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

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

The unified logging originator number for PBX is 103. See the [NetBackup Logging Reference Guide](#) for more information on unified logging.

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

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

### To access the PBX logs

- 1 Use the `vxlogview` command to view PBX and other unified logs. The originator ID for PBX is 103. For more information, see the `vxlogview` man page.

See also the [NetBackup Logging Reference Guide](#) for topics on unified logging.

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

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

where *debug\_level* is a number from 0 to 10, where 10 is the most verbose (the default).

To check the current verbosity, enter the following:

```
pbxcfg -p
```

PBX may log messages by default to the UNIX system logs

(`/var/adm/messages` or `/var/adm/syslog`) or to the Windows Event Log. As a result, the system logs may fill up with unnecessary PBX log messages, since the messages are also written to the PBX logs:

UNIX: `/opt/VRTSspbx/log`

Windows: `<install_path>\VxPBX\log`

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

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

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

## Troubleshooting PBX security

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

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

### To troubleshoot PBX security

- 1 Verify that PBX `Secure Mode` is set to `false` (the default):

- On Windows:

```
install_path\VxPBX\bin\pbxcfg -p
```

- On UNIX:

```
/opt/VRTSspbx/bin/pbxcfg -p
```

**2** If necessary, set `Secure Mode` to `false` by entering the following:

- On Windows:

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

- On UNIX:

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

**3** Stop NetBackup:

- On Windows:

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

- On UNIX:

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

**4** Stop PBX:

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

```
/opt/VRTSspbx/bin/vxpbx_exchanged stop
```

**5** Start PBX:

- On UNIX:

```
/opt/VRTSspbx/bin/vxpbx_exchanged start
```

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

**6** Start NetBackup:

- On Windows:

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

- On UNIX:

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

## Determining if the PBX daemon or service is available

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

When a NetBackup service is not running and another process tries to connect to it, messages similar to the following appear in `/opt/VRTSspbx/log` (UNIX) or `install_path\VxPBX\log` (Windows). The unified logging originator for PBX is 103 and the product ID is 50936.

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

### To determine if the PBX daemon or service is available

- 1 Start the needed service.

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

- 2 If necessary, stop and restart all NetBackup services.

- On Windows:

```
install_path\NetBackup\bin\bpdwn
install_path\NetBackup\bin\bpup
```

- On UNIX:

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

# About troubleshooting Auto Image Replication

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

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

---

**Note:** If replicating to specific targets (targeted AIR), you must create the Import SLP before creating the Auto Image Replication SLP in the originating domain. You may then choose the appropriate import SLP.

---

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

## Troubleshooting Auto Image Replication

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

---

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

---

Auto Image Replication operates like any duplication job except that its job contains no write side. The job must run on a media server that runs NetBackup 7.1 or higher. It also must consume a read resource from the disk volume on which the source

images reside. If no media server is available with NetBackup 7.1 or higher, the job fails with status 800.

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

The following procedure is based on NetBackup that operates in an OpenStorage configuration. This configuration communicates with a Media Server Deduplication Pool (MSDP) that uses Auto Image Replication.

## To troubleshoot Auto Image Replication jobs

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

```
# bpstsinfo -lsuinfo -stype PureDisk -storage_server
storage_server_name
```

### Example output:

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

This output shows the logical storage unit (LSU) flags **STS\_LSUF\_REP\_ENABLED** and **STS\_LSUF\_REP\_SOURCE** for **PureDiskVolume**. **PureDiskVolume** is enabled for Auto Image Replication and is a replication source.

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

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

The **ReplicationSource** flag confirms that NetBackup recognizes the LSU flags.

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

```
# nbdevconfig -previewdv -stype PureDisk -storage_server
storage_server_name -media_server media_server_name

V7.0 DiskVolume < "PureDiskVolume" "PureDiskVolume" 46068048064
46058373120 0 0 0 16 1 >
V7.0 ReplicationTarget < "bayside:PureDiskVolume" >
```

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

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

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

This listing shows that disk volume `PureDiskVolume` is configured in disk pool `PDpool`, and that NetBackup recognizes the replication capability on the source side. A similar `nbdevquery` command on the target side should display `ReplicationTarget` for its disk volume.

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

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

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

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

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

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

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

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

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

```
# tpconfig -dsh -all_hosts
=====
Media Server:                ssl.acme.com
Storage Server:              ssl.acme.com
User Id:                      root
    Storage Server Type:     BasicDisk
    Storage Server Type:     SnapVault
    Storage Server Type:     PureDisk
=====
```

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

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

```
nbstl woodridge2bayside -L
                                Name: woodridge2bayside
                                Data Classification: (none specified)
                                Duplication job priority: 0
                                State: active
                                Version: 0
Destination 1                   Use for: backup
                                Storage: PDstu
                                Volume Pool: (none specified)
                                Server Group: (none specified)
                                Retention Type: Fixed
                                Retention Level: 1 (2 weeks)
                                Alternate Read Server: (none specified)
                                Preserve Multiplexing: false
                                Enable Automatic Remote Import: true
                                State: active
                                Source: (client)
                                Destination ID: 0
Destination 2                   Use for: 3 (replication to remote master)
                                Storage: Remote Master
                                Volume Pool: (none specified)
                                Server Group: (none specified)
                                ...
                                Preserve Multiplexing: false
                                Enable Automatic Remote Import: false
                                State: active
                                Source: Destination 1 (backup:PDstu)
                                Destination ID: 0
```

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

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

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

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

**10 To show the status for completed replication copies, run the following command:**

```

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

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

Replication Destination:
Source Master Server: ssl.acme.com
Backup ID           : woodridge_1287610477
Copy Number         : 102

```

```

Target Machine      : bayside
Target Info        : PureDiskVolume
Remote Master      : (none specified)

```

## About troubleshooting automatic import jobs

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

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

See the [NetBackup Administrator's Guide, Volume I](#).

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

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

```

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

```

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

Copy:

Master Server : bayside.min.veritas.com  
 Backup ID : gdwinlin04\_1280299412  
 Copy Number : 1  
 Copy Type : 4  
 Expire Time : 0 (Wed Dec 31 18:00:00 1969)  
 Expire LC Time : 0 (Wed Dec 31 18:00:00 1969)  
 Try To Keep Time : 0 (Wed Dec 31 18:00:00 1969)  
 Residence : (none specified)  
 Copy State : 1 (NOT\_STARTED)  
 Job ID : 0  
 Retention Type : 0 (FIXED)  
 MPX State : 0 (FALSE)  
 Source : 0  
 Destination ID :  
 Last Retry Time : 0

Fragment:

Master Server : bayside.min.veritas.com  
 Backup ID : gdwinlin04\_1280299412  
 Copy Number : 1  
 Fragment Number : -2147482648  
 Resume Count : 0  
 Media ID : @aaaab  
 Media Server : bayside.min.veritas.com  
 Storage Server : bayside.min.veritas.com  
 Media Type : 0 (DISK)  
 Media Sub-Type : 0 (DEFAULT)  
 Fragment State : 1 (ACTIVE)  
 Fragment Size : 0  
 Delete Header : 1  
 Fragment ID : gdwinlin04\_1280299412\_C1\_IM

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

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

| <b>Action</b>   | <b>Condition</b>   |
|---|--|
| Automatic import jobs never start (copy stays at storage lifecycle state 1)   | <ul style="list-style-type: none"> <li>■ The storage lifecycle policy is inactive.</li> <li>■ The storage lifecycle policy import destination is inactive.</li> <li>■ The storage lifecycle policy is between sessions.</li> <li>■ The image has exceeded the extended retry count and the extended retry time has not passed.</li> </ul>  |
| Automatic import event is discarded and the image is ignored  | <ul style="list-style-type: none"> <li>■ The event specifies a backup ID that already exists in this master server catalog.</li> <li>■ The event specifies a disk volume that is not configured in NetBackup for this storage server.</li> </ul>   |
| Automatic import job is started but the image is expired and deleted to clean up disk space in some cases. The event logs an error in the Problems Report or berror output. An import job runs, but the import for this image fails showing a status code in the range 1532–1535. | <ul style="list-style-type: none"> <li>■ The storage lifecycle policy that is specified in the event does not contain an import destination.</li> <li>■ The storage lifecycle policy that is specified in the event has an import destination with a residence that does not include the disk volume that is specified by the event.</li> <li>■ The storage lifecycle policy that is specified does not exist. By default, the <b>Storage Lifecycle Policies</b> utility automatically creates a storage lifecycle policy with the correct name. Ensure that a storage lifecycle policy with the same case-sensitive name exists in the target master server.<br/><br/>More information is available for the storage lifecycle policy configuration options. See the <a href="#">NetBackup Administrator's Guide, Volume I</a>.</li> </ul> |

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

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

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

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

```
# nbstlutil list -copy_type import -U -copy_state 3 -U
Master Server           : bayside.min.veritas.com
Backup ID               : woodridge_1287610477
Client                  : woodridge
Backup Time             : 1287610477 (Wed Oct 20 16:34:37 2010)
Policy                  : two-hop-with-dup
Client Type             : 0
Schedule Type           : 0
Storage Lifecycle Policy : woodridge2bayside2pearl_withdup
Storage Lifecycle State  : 3 (COMPLETE)
Time In Process         : 1287610714 (Wed Oct 20 16:38:34 2010)
Data Classification ID  : (none specified)
Version Number          : 0
OriginMasterServer      : woodridge.min.veritas.com
OriginMasterServerID    : f5cec09a-da74-11df-8000-f5b9412d8988
Import From Replica Time : 1287610672 (Wed Oct 20 16:37:52 2010)
Required Expiration Date : 1290288877 (Sat Nov 20 15:34:37 2010)
Created Date Time       : 1287610652 (Wed Oct 20 16:37:32 2010)
```

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

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

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

# Troubleshooting network interface card performance

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

---

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

---

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

## To troubleshoot network interface card performance

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

```
ifconfig -a
```

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

The following is an example output from a NAS filer:

```
e0: flags=1948043<UP,BROADCAST,RUNNING,MULTICAST,TCPCSUM> 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,TCPCSUM> mtu 1500
ether 00:07:e9:3e:ca:b4 (auto-unknown-cfg_down) flowcontrol full
e9b: flags=108042<BROADCAST,RUNNING,MULTICAST,TCPCSUM> mtu 1500
ether 00:07:e9:3e:ca:b5 (auto-unknown-cfg_down) flowcontrol full
```

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

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

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

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

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

## About SERVER entries in the bp.conf file

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

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

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

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

---

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

---

## About unavailable storage unit problems

NetBackup jobs sometimes fail because storage units are unavailable, due to the disk drives or tape drives that are down or have configuration errors. The NetBackup processes log messages to the NetBackup error log that may help pinpoint and resolve these types of issues.

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

- The resources that the job requests

- The granted (allocated) resources.

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

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

## Resolving a NetBackup Administration operations failure on Windows

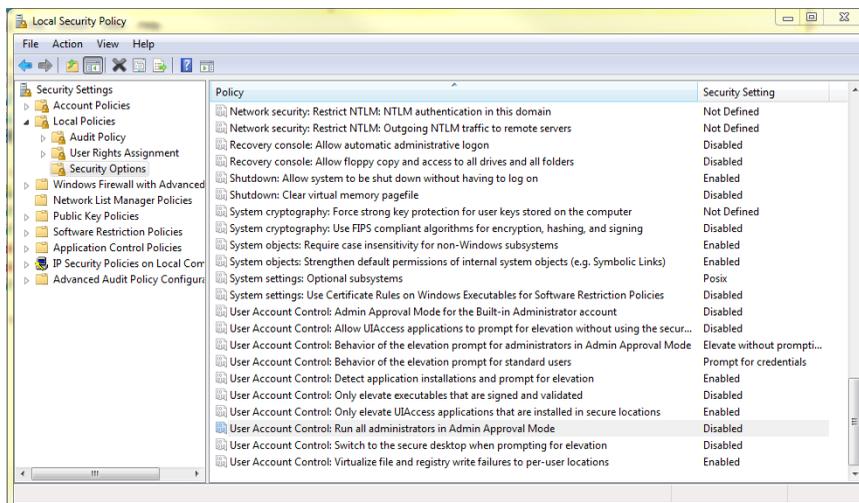
When a user who is part of the Administrator’s group tries to execute some NetBackup operations, the operation may fail with the following error, where *command* is a NetBackup administrator command:

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

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

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

**Figure 2-5** Local Security Policy panel



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

## Resolving garbled text displayed in NetBackup Administration Console on a UNIX computer

Perform the following steps if you see garbled text or if you cannot see non-English text in the **NetBackup Administration Console** on a UNIX computer:

1. On the command prompt, enter **locale**.
2. Ensure that `LC_CTYPE` is set to the value corresponding to the locale that you want to display.

For example, if `LC_CTYPE` is set to `en_US.UTF-8`, the text is displayed in US English in the console.

If `LC_CTYPE` is set to `fr_FR.UTF8`, the text is displayed in French in the console.

# Using NetBackup utilities

This chapter includes the following topics:

- [About NetBackup troubleshooting utilities](#)
- [About the analysis utilities for NetBackup debug logs](#)
- [About the Logging Assistant](#)
- [About network troubleshooting utilities](#)
- [About the NetBackup support utility \(nbsu\)](#)
- [About the NetBackup consistency check utility \(NBCC\)](#)
- [About the NetBackup consistency check repair \(NBCCR\) utility](#)
- [About the nbclogs utility](#)
- [About the robotic test utilities](#)

## About NetBackup troubleshooting utilities

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

**Table 3-1** Troubleshooting utilities

| Utility                                     | Description  |
|---|--|
| Analysis utilities for NetBackup debug logs | They enhance NetBackup's existing debug capabilities by providing a consolidated view of a job debug log.<br><br>See <a href="#">“About the analysis utilities for NetBackup debug logs”</a> on page 93. |

**Table 3-1** Troubleshooting utilities (*continued*)

| Utility  | Description  |
|--|--|
| Logging Assistant                                  | <p>It simplifies the gathering of evidence for support cases.</p> <p>For more information, see the following:</p> <ul style="list-style-type: none"> <li>■ <i>NetBackup Administrator's Guide, Volume I</i>, and the online Help for the NetBackup Administration Console.</li> <li>■ The <i>Symantec Logging Assistant FAQ</i>:<br/> <a href="http://www.symantec.com/docs/TECH204256">http://www.symantec.com/docs/TECH204256</a></li> </ul> |
| Network troubleshooting utilities                  | <p>They verify various aspects of the network configuration inside and outside NetBackup to ensure that there is no misconfiguration.</p> <p>See “<a href="#">About network troubleshooting utilities</a>” on page 97.</p>   |
| NetBackup support utility (nbsu)                   | <p>It queries the host and gathers appropriate diagnostic information about NetBackup and the operating system.</p> <p>See “<a href="#">About the NetBackup support utility (nbsu)</a>” on page 98.</p>  |
| NetBackup consistency check utility (NBCC)         | <p>It analyzes the integrity of portions of the NetBackup configuration and catalog and database information as they pertain to tape media.</p> <p>See “<a href="#">About the NetBackup consistency check utility (NBCC)</a>” on page 105.</p>   |
| NetBackup consistency check repair (NBCCR) utility | <p>It processes database-catalog repair actions and automates the application of approved suggested repair actions.</p> <p>See “<a href="#">About the NetBackup consistency check repair (NBCCR) utility</a>” on page 113.</p>   |
| nbcplogs utility                                   | <p>It simplifies the gathering of logs to deliver to Symantec technical support.</p> <p>See “<a href="#">About the nbcplogs utility</a>” on page 115.</p>  |
| Robotic test utilities                             | <p>They communicate directly with robotic peripherals.</p> <p>See “<a href="#">About the robotic test utilities</a>” on page 116.</p>  |

## About the analysis utilities for NetBackup debug logs

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

NetBackup jobs span multiple processes that are distributed across servers.

To trace a NetBackup job you must view and correlate messages in multiple log files on multiple hosts. The log analysis utilities provide a consolidated view of the job debug logs. The utilities scan the logs for all processes that are traversed or run for the job. The utilities can consolidate job information by client, job ID, start time for the job, and policy that is associated with the job.

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

---

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

---

**Table 3-2** Analysis utilities for NetBackup debug logs

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

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

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

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

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

The analysis utilities have the following limitations:

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

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

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

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

---

**Note:** For the processes that use unified logging, log directories are automatically created.

---

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

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

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

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

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

## About the Logging Assistant

For help on a NetBackup issue, you can use the Logging Assistant to gather evidence for Symantec Technical Support. You are not required to sift through NetBackup debug logs for clues or explanations on your own. Debug logs are for Symantec Technical Support to analyze.

Extensive information on the Logging Assistant is available in the following Symantec documents:

- *NetBackup Administrator's Guide, Volume I*, and in the online Help for the NetBackup Administration Console.
- The *Symantec Logging Assistant FAQ*:  
<http://www.symantec.com/docs/TECH204256>

## About network troubleshooting utilities

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

Network configuration broadly falls into the following categories:

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

**Table 3-3** Network troubleshooting utilities

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

## About the NetBackup support utility (nbsu)

The NetBackup support utility (`nbsu`) is a command line tool. It queries the host and gathers appropriate diagnostic information about NetBackup and the operating system. `nbsu` provides a wide range of control over the types of diagnostic information gathered. For instance, you can obtain information about NetBackup

configuration settings, about specific troubleshooting areas, or about NetBackup or media management job status codes.

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

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

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

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

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

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

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

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

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

To redirect the nbsu error messages to standard output (STDOUT)

Enter the following:

- UNIX  
`/usr/opensv/netbackup/bin/support/nbsu 2>&1`
- Windows  
`install_path\NetBackup\bin\support\nbsu.exe 2>&1`

To send all nbsu screen output including error messages to a file

Enter the following:

```
nbsu 2>&1 > file_name
```

Where `2>&1` directs standard error into standard output, and `file_name` directs standard output into the designated file.

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

```
# nbsu -debug
```

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

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

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

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

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

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

## Output from the NetBackup support utility (nbsu)

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

```
UNIX      /usr/opensv/netbackup/bin/support/output/nbsu
          /hostname_timestamp
```

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

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

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

The following are the actual commands and output after the header.

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
```

The following is an example of part of the `nbsu` output file for the `bpgetconfig` command.

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 -----
# /usr/opensv/netbackup/bin/admincmd/bpgetconfig -g nbmedia00 -L
Client/Master = Media Host
NetBackup Client Platform = Linux, RedHat2.6.18
```

```
NetBackup Client Protocol Level = 7.7.0
Product = NetBackup
Version Name = 7.7
Version Number = 770000
NetBackup Installation Path = /usr/opensv/netbackup/bin
Client OS/Release = Linux 2.6.18-194.el5
```

```
----- Command Used -----
# /usr/opensv/netbackup/bin/admincmd/bpgetconfig
SERVER = nbmaster00
SERVER = nbmedia00
TRUSTED_MASTER
KNOWN_MASTER
MASTER_OF_MASTERS
USEMAIL =
BPBACKUP_POLICY = any
BPBACKUP_SCHED = any
```

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

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

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

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

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

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

```
/usr/opensv/netbackup/bin/support/output/nbsu/host1_master_yyyymmdd_
164443/host1_master_20060814_164443.tar.gz
```

where `host1` is the name of the host on which `nbsu` ran, and `master` indicates that the host is a NetBackup master server. The date is embedded in the file name in the `yyymmdd` format.

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

---

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

---

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

A complete description of `nbsu` is in the [NetBackup Commands Reference Guide](#).

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

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

See the [Status Codes Reference Guide](#) for more about the topics that describe the status codes.

A complete description of `nbsu` is in the [NetBackup Commands Reference Guide](#).

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

To gather diagnostic information about status code 25      Enter `nbsu -nbu_e 25`.

This command runs only the diagnostic commands that are related to NetBackup status code 25. Since fewer commands are run, the result may be a smaller set of output files.

To determine what information `nbsu` can collect for a particular status code      Enter `nbsu -l -nbu_e 25`.

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

See [“Output from the NetBackup support utility \(nbsu\)”](#) on page 100.

---

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

---

A complete description of `nbsu` is in the [NetBackup Commands Reference Guide](#).

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

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

```
C:\Program Files\VERITAS\NetBackup\bin\support>nbsu
1.0 Determining initial nbsu settings
1.1 Determining OS environment
1.2 Determining OS host services
1.3 Determining identified network interface hostnames
1.4 Determining NetBackup environment
2.0 Querying nbsu diagnostic lists
2.1 Determining nbsu diagnostics to run
3.0 Executing nbsu diagnostics
    Executing diagnostic DEV_scsi_reg
    Registry query of HKEY_LOCAL_MACHINE\hardware\DeviceMap\Scsi\

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

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

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

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

A complete description of `nbsu` is in the [NetBackup Commands Reference Guide](#).

## About the NetBackup consistency check utility (NBCC)

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

NBCC does the following:

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

NBCC resides in the following location:

UNIX `/usr/opensv/netbackup/bin/support/NBCC`

Windows `install_path\NetBackup\bin\support\NBCC.exe`

Symantec recommends that you run NBCC in the following circumstances:

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

The following items can help you run the NBCC utility:

- The use of NBCC without options gathers all data and reports, and is recommended for most customers. For additional information, NBCC description, examples, and instructions for gathering NetBackup catalog and database information to send to technical support, use the `NBCC -help` command.
- NBCC is designed to be run on NetBackup master servers.
- In some cases, a non-functioning operating system or NetBackup process or service can prevent NBCC from running properly or completing. As NBCC

progresses through the interrogation of various operating system or NetBackup components, it outputs what processes to STDOUT. As NBCC processes catalog and database components, it displays how many records have been processed. The number of records that are processed is in direct relationship to the size of the catalog and database being processed. If NBCC detects a failure, related information is output to STDERR. Information to STDOUT or STDERR are also output to the `nbcc-info.txt` file (if available).

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

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

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

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

This information indicates the processing that NBCC has done.

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

See “[Example of an NBCC progress display](#)” on page 107.

A complete description of NBCC is in the [NetBackup Commands Reference Guide](#).

## Output from the NetBackup consistency check utility (NBCC)

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

```
UNIX and Linux    /usr/opensv/netbackup/bin/support/output  
                  /nbcc/hostname_NBCC_timestamp
```

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

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

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

```
/usr/opencv/netbackup/bin/support/output/NBCC/host1_NBCC_20060814_164443/host1_NBCC_20060814_164443.tar.gz
```

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

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

A complete description of NBCC is in the [NetBackup Commands Reference Guide](#).

## Example of an NBCC progress display

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

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

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

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

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

2.0 Gathering required NetBackup configuration information
2.1 Determining the date format to use with NetBackup commands...
```

```

    Using the date format /mm/dd/yyyy
2.2 Building EMM host configuration information...
    Detected the EMM Server hostname
        lidabl11
    Detected the EMM master server hostname
        lidabl11
    Detected the EMM Virtual Machine entry
        pamb111vm3
    Detected the EMM NDMP Host entry
        fas3240a
    ...
2.3 Obtaining EMM server aliases...
    EMM aliases for detected EMM Server
        server1
            lidabl11.rmnus.sen.symantec.com
    EMM aliases for detected master server
        server1
            lidabl11.rmnus.sen.symantec.com
    EMM aliases for detected media server
        server4
    ...
2.4 Obtaining Storage Server information...
    Detected FalconStor OST direct copy to tape Storage Server
        falconstorvt15
2.5 Building NetBackup storage unit list...
    Detected Storage Unit for NetBackup for NDMP media server
        reab13
    and NDMP Host
        falconstorvt15
    Detected disk media storage unit host
        lidabl11
    Detected Disk Pool
        lidabl11_pdde_pool
    ...
2.6 Obtaining Disk Pool information...
    Detected Disk Pool
        lidabl11_pdde_pool
        host
            lidabl11
    Detected Disk Pool lidabl11_pdde_pool member
        lidabl11
    ...
2.7 Obtaining tpconfig Storage credential information...

```

```

Detected the master server hostname
  lidabl11
and associated Storage server hostname
  lidabl11
...
2.8 Obtaining tpconfig NDMP configuration information...
    Detected the EMM NDMP Host hostname
      fas3240a
    Detected the EMM NDMP Host hostname
      fas3240b
...
2.9 Analyzing EMM master and/or media servers and configured
Storage Units...
    The following EMM server entries do not have configured
Storage Units or Disk Pools:

    Media server - lidabl14

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

```

```

Reading Image number 3000
Reading Image number 4000
Found 4014 images in the Image database
3.6 Building EMM database Media and Device configuration
attribute lists
Obtaining the EMM database Media attribute list for disk
virtual server
lidabl11 ...
There were 0 bpmedialist records detected for media server
lidabl11
Getting device configuration data from server
lidabl11 ...
...
3.7 Building EMM database Unrestricted Sharing Media attribute lists
Found 0 Unrestricted Sharing media records in the EMM database
3.8 Building the EMM database Volume attribute list...
Getting the EMM database Volume attributes from EMM server
mlbnbu ...
Found 43 Volume attribute records in the EMM database
3.9 Building NetBackup volume pool configuration list
EMM Server lidabl11
3.10 Building NetBackup scratch pool configuration list
EMM Server lidabl11
3.11 Gathering NetBackup EMM merge table list
Found 0 EMM merge table records

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

Catalog data gathering took 189 seconds to complete

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

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

07/07/2011 09:43 AM 2,211,811 nbcc-bpimagelist-1
...

```

```
4.0 Verifying required catalog components were gathered

5.0 Beginning NetBackup catalog consistency check
    Start time = 2013-02-27 09:44:18
5.1 There were no tape media involved in active NetBackup jobs
5.3 Processing EMM database Volume attribute records, pass 1 (of 2),
    4 records to be processed
    Processed 4 EMM database Volume attribute records.
5.4 Checking for duplicate EMM server host names in Volume
    attribute data
5.5 Processing Image DB, pass 1 (of 2),
    3751 images to be processed
    3751 images processed on pass 1
    There were 0 images with at least one copy on hold detected.
5.6 Processing EMM database Media attribute records, pass 1 (of 3),
    2 records to be processed
    Processed 2 EMM database Media attribute records.
    There were 0 tape media detected that are on hold.
5.8 Check for duplicate media server names in the EMM database
    Media attribute data
5.9 Processing EMM database Media attribute records, pass 2 (of 3),
    2 records to be processed
5.10 Processing Image DB, pass 2 (of 2),
    3751 images to be processed
CONSISTENCY_ERROR Oper_7_1

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

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

    Summary of NBCC EMM Server processing
    Summary of NBCC EMM Server processing
+++++
+ Primary hostname:                                     +
+ lidabl11                                             +
+ Alias hostnames:                                     +
+ lidabl11                                             +
+ Sources:                                             +
+ nbemncmd vmopr cmd                                   +
+ EMM Server = yes                                     +
```

```
+ EMM NetBackup version = 7.6 +
+ NBCC NetBackup version = 7.6 +
+++++
```

Summary of NBCC Master server processing

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

Summary of NBCC Media server processing

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

...

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

Report complete, closing the

```
.\output\nbcc\lidabl11_NBCC_20130227_094057\nbcc-info.txt  
output file.
```

A complete description of NBCC options is in the [NetBackup Commands Reference Guide](#).

## About the NetBackup consistency check repair (NBCCR) utility

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

The NBCCR utility executes each repair action in several stages.

**Table 3-4** Stages of repair

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

NBCCR resides in the following location:

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

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

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

**Input file** NBCCR accepts as input the Suggested Repair Action (SRA) file named `mastername_NBCCA_timestamp.txt`. Technical Support analyzes the NBCC support package and generates this file which is sent to the end-user. This file is placed in the following directory for NBCCR processing:

On UNIX:

`/usr/opensv/netbackup/bin/support/input/nbccr/SRA`

On Windows:

`install_path\NetBackup\bin\support\input\nbccr\SRA`

**Output files** NBCCR automatically creates a separate directory for each SRA file processed. The file name is based on the contents of the SRA file. The name of the directory is as follows:

On UNIX: `/usr/opensv/netbackup/bin/support/output/nbccr/mastername_nbccr_timestamp`

On Windows: `install_path\NetBackup\bin\support\output\nbccr\mastername_nbccr_timestamp`.

After repair processing is complete, NBCCR relocates the SRA file to the same directory.

NBCCR also creates the following output files and places them in the same directory.

- NBCCR creates `NBCCR.History.txt`, which is a history file of all the repair actions attempted.
- NBCCR creates `NBCCR.output.txt`.

**Temporary file** While it runs, the NBCCR utility uses `KeepOnTruckin.txt`, which appears in the same location as the output files described in this table.

To terminate NBCCR while it processes repairs, delete this file. This action causes NBCCR to complete the current repair, then shut down. Any other interruption causes undetermined results.

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

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

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

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

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

A complete description of `NBCCR` is in the [NetBackup Commands Reference Guide](#).

## About the `nbcplogs` utility

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

By default, `nbcplogs` (NetBackup log uploader) now runs the `nbsu` utility and uploads `nbsu` information for the host system. This capability saves time and keystrokes in gathering information. The utility also gathers additional log information for clusters and pack history information.

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

On Windows:

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

On UNIX:

In `/bin/sh`, enter the following:

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

In `/bin/bash`, enter the following:

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

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

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

This utility supports the following types of search algorithms as options on the `nbcplogs` command.

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

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

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

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

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

A complete description of `nbcplogs` is in the [NetBackup Commands Reference Guide](#).

## About the robotic test utilities

Each of the robotic software packages includes a robotic test utility for communicating directly with robotic peripherals. The tests are for diagnostic purposes: 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 NBDB), start the robotic test utility by using the `robtest` command. This action saves time, since robotic and drive device paths are passed to the test utility automatically. The procedure is as follows:

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

- Execute the following command:

```
/usr/opensv/volmgr/bin/robtest
```

The test utility menu appears.

- Select a robot and click **Enter**.

The test starts.

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

|     |  |
|-----|--|
| ACS | <code>/usr/opensv/volmgr/bin/acstest -r ACSLS_hostpath</code><br>for <code>acstest</code> to work on UNIX and Linux, <code>acssel</code> and <code>acsssi</code> must be running |
| ODL | <code>/usr/opensv/volmgr/bin/odltest -r roboticpath</code>   |
| TL4 | <code>/usr/opensv/volmgr/bin/tl4test -r roboticpath</code>   |
| TL8 | <code>/usr/opensv/volmgr/bin/tl8test -r roboticpath</code>   |
| TLD | <code>/usr/opensv/volmgr/bin/tldtest -r roboticpath</code>   |
| TLH | <code>/usr/opensv/volmgr/bin/tlhstest -r robotic_library_path</code>   |
| TLM | <code>/usr/opensv/volmgr/bin/tlmtest -r DAS_host</code>  |
| TSH | <code>/usr/opensv/volmgr/bin/tshtest -r roboticpath</code>   |

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

See the [NetBackup Device Configuration Guide](#).

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

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

## Robotic tests on Windows

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

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

- Execute the following command:

```
install_path\Volmgr\bin\robtest.exe
```

The test utility menu appears.

- Select a robot and press Enter.

The test starts.

---

**Note:** If the robot is not configured, you cannot use `robtest`. You must execute the command that applies to the robot you want to test (see following list).

---

|     |   |
|-----|---|
| ACS | <code><i>install_path</i>\Volmgr\bin\acstest -r ACSLS_HOST</code>                       |
| TL4 | <code><i>install_path</i>\Volmgr\bin\tl4test -r <i>roboticpath</i></code>               |
| TL8 | <code><i>install_path</i>\Volmgr\bin\tl8test -r <i>roboticpath</i></code>               |
| TLD | <code><i>install_path</i>\Volmgr\bin\tldtest -r <i>roboticpath</i></code>               |
| TLH | <code><i>install_path</i>\Volmgr\bin\tlhstest -r<br/><i>robotic_library_name</i></code> |
| TLM | <code><i>install_path</i>\Volmgr\bin\tlmtest -r DAS_Hostname</code>                     |

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

See the [NetBackup Device Configuration Guide](#).

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

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

Usage is:

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

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

# Disaster recovery

This chapter includes the following topics:

- [About disaster recovery](#)
- [Recommended backup practices](#)
- [About disk recovery procedures for UNIX and Linux](#)
- [About clustered NetBackup server recovery for UNIX and Linux](#)
- [About disk recovery procedures for Windows](#)
- [About clustered NetBackup server recovery for Windows](#)
- [About recovering the NetBackup catalog](#)

## About disaster recovery

Data backup is essential to any data protection strategy, especially a strategy that is expected to assist in disaster recovery. Regularly backing up data and therefore being able to restore that data within a specified time frame are important components of recovery. Regardless of any other recovery provisions, backup protects against data loss from complete system failure. And off-site storage of backup images protects against damage to your on-site media or against a disaster that damages or destroys your facility or site.

To perform recovery successfully, the data must be tracked. Knowing at what point in time the data was backed up allows your organization to assess the information that cannot be recovered. Configure your data backup schedules to allow your organization to achieve its recovery point objective (RPO). The RPO is the point in time before which you cannot accept lost data. If your organization can accept one day's data loss, your backup schedule should be at least daily. That way you can achieve an RPO of one day before any disaster.

Your organization also may have a recovery time objective (RTO), which is the expected recovery time or how long it takes to recover. Recovery time is a function of the type of disaster and of the methods that are used for recovery. You may have multiple RTOs, depending on which services your organization must recover when.

High availability technologies can make the recovery point very close or even identical to the point of failure or disaster. They also can provide very short recovery times. However, the closer your RTO and RPO are to the failure point, the more expensive it is to build and maintain the systems that are required to achieve recovery. Your analysis of the costs and benefits of various recovery strategies should be part of your organization's recovery planning.

Effective disaster recovery requires procedures specific to an environment. These procedures provide detailed information regarding preparation for and recovering from a disaster. Use the disaster recovery information in this chapter as a model only; evaluate and then develop your own disaster recovery plans and procedures.

---

**Warning:** Before you try any of the disaster recovery procedures in this chapter, Symantec recommends that you contact technical support.

This topic provides information about NetBackup installation and (if necessary), catalog recovery after a system disk failure. Symantec assumes that you recover to the original system disk or one configured exactly like it.

---

**Warning:** NetBackup may not function properly if you reinstall and recover to a different partition or to one that is partitioned differently due to internal configuration information. Instead, configure a replacement disk with partitioning that is identical to the failed disk. Then reinstall NetBackup on the same partition on which it was originally installed.

---

The specific procedures that replace failed disks, build partitions and logical volumes, and reinstall operating systems can be complicated and time consuming. Such procedures are beyond the scope of this manual. Appropriate vendor-specific information should be referenced.

## Recommended backup practices

The following backup practices are recommended:

|   |   |
|---|---|
| Selecting files to back up                    | <p>In addition to backing up files on a regular basis, it is important to select the correct files to back up. Include all files with records that are critical to users and the organization. Back up system and application files, so you can quickly and accurately restore a system to normal operation if a disaster occurs.</p> <p>Include all Windows system files in your backups. In addition to the other system software, the Windows system directories include the registry, which is needed to restore the client to its original configuration. If you use a NetBackup exclude list for a client, do not specify any Windows system files in that list.</p> <p>Do not omit executables and other application files. You may want to save tape by excluding these easy-to-reinstall files. However, backing up the entire application ensures that it is restored to its exact configuration. For example, if you have applied software updates and patches, restoring from a backup eliminates the need to reapply them.</p> |
| Bare Metal Restore                            | <p>NetBackup Bare Metal Restore (BMR) protects client systems by backing them up with a policy configured for BMR protection. A complete description of BMR backup and recovery procedures is available.</p> <p>See the <i>NetBackup Bare Metal Restore Administrator's Guide</i>:<br/><a href="http://www.symantec.com/docs/DOC5332">http://www.symantec.com/docs/DOC5332</a></p>  |
| Critical policies                             | <p>When you configure a policy for online catalog backup, designate certain NetBackup policies as critical. Critical policies back up systems and data deemed critical to end-user operation. During a catalog recovery, NetBackup verifies that all of the media that is needed to restore critical policies are available.</p>  |
| Full backup after catalog recovery            | <p>If the configuration contains Windows clients that have incremental backup configurations set to <b>Perform Incrementals Based on Archive Bit</b>, run a full backup of these clients as soon as possible after a catalog recovery. The archive bit resets on the files that were incrementally backed up after the catalog backup that was used for the catalog recovery. If a full backup of these clients is not run after a catalog recovery, these files could be skipped and not backed up by subsequent incremental backups.</p>  |
| Online catalog backups                        | <p>Online, hot catalog backup is a policy-driven backup that supports tape-spanning and incremental backups. It allows for restoring catalog files from the Backup, Archive, and Restore interface. Online catalog backups may be run while other NetBackup activity occurs, which provides improved support for environments in which continual backup activity is typical.</p>  |
| Online catalog backup disaster recovery files | <p>Symantec recommends saving the disaster recovery files that are created by the online catalog backup to a network share or removable device. Do not save the disaster recovery files to the local computer. Catalog recovery from an online catalog backup without the disaster recovery image file is a more complex procedure and time-consuming procedure.</p>  |

|  |   |
|--|---|
| Automated recovery                                 | <p>The catalog disaster recovery file (created during an online catalog backup) is intended to automate the process of NetBackup recovery. If you recover a system other than the one that originally made the backups, it should be identical to the original system. For example, the system that performs the recovery should include NetBackup servers with identical names to those servers where the backups were made. If not, the automated recovery may not succeed.</p>   |
| Online catalog disaster recovery information email | <p>Configure the online catalog backup policy to email a copy of the disaster recovery information to a NetBackup administrator in your organization. Configure this policy as part of every catalog backup. Do not save the disaster recovery information emails to the local computer. Catalog recovery without the disaster recovery image file or the disaster recovery information email available is exceedingly complex, time consuming, and requires assistance.</p> <p>NetBackup emails the disaster recovery file when the following events occur:</p> <ul style="list-style-type: none"><li>■ The catalog is backed up.</li><li>■ A catalog backup is duplicated or replicated.</li><li>■ The primary catalog backup or any copy of a catalog backup expires automatically or is expired manually.</li></ul> <p>You may tailor the disaster recovery email process by using the <code>mail_dr_info</code> notify script. More details are available.</p> <p>See the <i>NetBackup Administrator's Guide, Volume II</i>:<br/><a href="http://www.symantec.com/docs/DOC5332">http://www.symantec.com/docs/DOC5332</a></p> |
| Identifying the correct catalog backup             | <p>Ensure that you identify and use the appropriate catalog backup for your recovery. For example, if you recover from your most recent backups, use the catalog from your most recent backups. Similarly, if you recover from a specific point in time, use the catalog backup from that specific point in time.</p>   |
| Catalog recovery time                              | <p>System environment, catalog size, location, and backup configuration (full and incremental policy schedules) all help determine the time that is required to recover the catalog. Carefully plan and test to determine the catalog backup methods that result in the desired catalog recovery time.</p>  |
| Master and media server backups                    | <p>The NetBackup catalog backup protects your configuration data and catalog data. Set up backup schedules for the master servers and media servers in your NetBackup installation. These schedules protect the operating systems, device configurations, and other applications on the servers.</p> <p>Master or media server recovery procedures when the system disk has been lost assume that the servers are backed up separately from the catalog backup. Backups of master and media servers should not include NetBackup binaries, configuration or catalog files, or relational database data.</p>   |

# About disk recovery procedures for UNIX and Linux

The three different types of disk recovery for UNIX and Linux are as follows:

- Master server disk recovery procedures  
See “[Recovering the master server disk for UNIX and Linux](#)” on page 124.
- Media server disk recovery procedures  
See “[About recovering the NetBackup media server disk for UNIX](#)” on page 129.
- Client disk recovery procedures  
See “[Recovering the system disk on a UNIX client workstation](#)” on page 130.

The disk-based images that reside on AdvancedDisk or on OpenStorage disks cannot be recovered by means of the NetBackup catalog. These disk images must be recovered by means of the NetBackup import feature. For information on import,

See the topic on importing NetBackup images in the *NetBackup Administrator's Guide, Volume I*:

<http://www.symantec.com/docs/DOC5332>

When the disk image is imported, NetBackup does not recover the original catalog entry for the image. Instead, a new catalog entry is created.

## Recovering the master server disk for UNIX and Linux

Two procedures explain how to recover data if the system disk fails on a UNIX or Linux NetBackup master server, as follows:

- The root file system is intact. The operating system, NetBackup software and some (if not all) other files are assumed to be lost.  
See “[Recovering the master server when root is intact](#)” on page 125.
- The root file system is lost along with everything else on the disk. This situation requires a total recovery. This recovery reloads the operating system to an alternate boot disk and boots from this disk during recovery. This operation lets you recover the root partition without risking a crash that is caused by overwriting the files that the operating system uses during the restore.  
See “[Recovering the master server when the root partition is lost](#)” on page 127.

For NetBackup master and media servers, the directory locations of the NetBackup catalog become an integral part of NetBackup catalog backups. Any recovery of the NetBackup catalog requires identical directory paths or locations be created during the NetBackup software reinstallation. Disk partitioning, symbolic links, and NetBackup catalog relocation utilities may be needed.

NetBackup Bare Metal Restore (BMR) protects client systems by backing them up with a policy configured for BMR protection. Information is available that describes BMR backup and recovery procedures.

See the *NetBackup Bare Metal Restore System Administrator's Guide*:

<http://www.symantec.com/docs/DOC5332>

## Recovering the master server when root is intact

The following procedure recovers the master server by reloading the operating system, restoring NetBackup, and then restoring all other files.

### To recover the master server when root is intact

- 1 Verify that the operating system works, that any required patches are installed, and that specific configuration settings are made. Take corrective action as needed.
- 2 Reinstall NetBackup software on the server you want to recover.

See the *NetBackup Installation Guide* for instructions:

<http://www.symantec.com/docs/DOC5332>

- 3 Install any NetBackup patches that had been previously installed. See the documentation that was included with the patch software.

---

**Note:** Symantec does not support the recovery of a catalog image that was backed up using an earlier version of NetBackup.

---

- 4 If any of the default catalog directories have changed that may be reflected in the NetBackup catalog backups, recreate those directories before the catalog recovery.

The following are examples:

- Use of symbolic links as part of the NetBackup catalog directory structure.
  - Use of the NetBackup `nbbdb_move` command to relocate parts of the NetBackup relational database catalog.
- 5 If the recovery scenario involves restoring policy or catalog backups, the appropriate recovery device(s) must be configured, which may involve the following tasks:
    - Install and configure the robotic software for the devices that read backups of the NetBackup catalog and regular backups of the disk being restored. If a non-robotic drive is available that can read these backups, then no robot

is required. Although manual intervention is required if multiple pieces of media are required.

See the *NetBackup Device Configuration Guide*:

<http://www.symantec.com/docs/DOC5332>

- Use the **NetBackup Device Configuration** Wizard to discover and configure the recovery device in NetBackup.

See the *NetBackup Administrator's Guide, Volume I*:

<http://www.symantec.com/docs/DOC5332>

- Use the NetBackup `tpautoconf` command to discover and configure the recovery device in NetBackup.

See the *NetBackup Commands Reference Guide*:

<http://www.symantec.com/docs/DOC5332>

- Update the device mapping files.

See the *NetBackup Administrator's Guide, Volume I*:

<http://www.symantec.com/docs/DOC5332>

- 6 If you must restore from the policy backups or catalog backups that were done to media, the appropriate media may have to be configured in NetBackup

See the *NetBackup Administrator's Guide, Volume I*:

<http://www.symantec.com/docs/DOC5332>

Configuring the media may require some or all of the following tasks:

- Manually load the required media into a standalone recovery device.
- Use the NetBackup utilities such as `robtest` or vendor-specific robotic control software to load media into the required recovery device or devices.
- Use the NetBackup Volume Configuration Wizard to inventory the media contents of a robotic device.
- Use the vendor-specific robotic control software to load the media into the required recovery device(s).

- 7 Recover the NetBackup catalogs to the server you are recovering.

The NetBackup catalogs can be recovered only to the same directory structure from which they were backed up (alternate path recovery is not allowed).

- 8 Stop and restart all NetBackup daemons. Use the following NetBackup commands, or use the **Activity Monitor** in the NetBackup Administration Console.

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

- 9 Start the NetBackup Backup, Archive, and Restore interface (or the `bp` command) and restore other files to the server as desired. When the files are restored, you are done.

## Recovering the master server when the root partition is lost

The following procedure assumes that the root file system is lost along with everything else on the disk. This procedure reloads the operating system to an alternate boot disk and boots from that disk during recovery. This operation lets you recover the root partition without risking a crash that is caused by overwriting the files that the operating system uses during the restore

### To recover the master server when the root partition is lost

- 1 Load the operating system on an alternate boot disk, using the same procedure as you would normally use for the server type.
- 2 On the alternate disk, create the partition and directory where NetBackup, its catalogs (if applicable), and databases resided on the original disk. By default, they reside under the `/usr/opensv` directory.
- 3 Verify that the operating system works, that any required patches are installed, and that specific configuration settings are made. Take corrective action as needed.
- 4 Install NetBackup on the alternate disk. Install only the robotic software for the devices that are required to read backups of the NetBackup catalogs and regular backups of the disk being restored. If a non-robotic drive can read these backups, no robot is required.
- 5 Install any NetBackup patches that had been previously installed. See the documentation that was included with the patch software.
- 6 If the catalog directories differ from those in the NetBackup catalog backups, recreate that directory structure on disk before you recover the catalog.

Examples of those directories are the following:

- Use of symbolic links as part of the NetBackup catalog directory structure.
- Use of the NetBackup `nbdb_move` command to relocate parts of the NetBackup relational database catalog.

- 7 If the recovery scenario involves restoring policy or catalog backups, the appropriate recovery device(s) must be configured.

Device configuration may include the following tasks:

- Install and configure the robotic software for the devices that read backups of the NetBackup catalog and regular backups of the disk being restored. If a non-robotic drive is available that can read these backups, then no robot is required. Although manual intervention is required if multiple pieces of media are required.

See the *NetBackup Device Configuration Guide*:

<http://www.symantec.com/docs/DOC5332>

- Use the **NetBackup Device Configuration** Wizard to discover and configure the recovery device in NetBackup.

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

<http://www.symantec.com/docs/DOC5332>

- Use the NetBackup `tpautoconf` command to discover and configure the recovery device in NetBackup.

See the *NetBackup Commands Reference Guide* manual:

<http://www.symantec.com/docs/DOC5332>

- Update the device mapping files.

See the *NetBackup Administrator's Guide, Volume I*:

<http://www.symantec.com/docs/DOC5332>

- 8 If you must restore from the policy backups or catalog backups that were done to media, the appropriate media may have to be configured in NetBackup.

See the *NetBackup Administrator's Guide, Volume I*:

<http://www.symantec.com/docs/DOC5332>

Configuring the media may require some or all of the following tasks:

- Manually load the required media into a standalone recovery device.
- Use the NetBackup utilities such as `robtest` or vendor-specific robotic control software to load media into the required recovery device or devices.
- Use the NetBackup Volume Configuration Wizard to inventory the media contents of a robotic device.
- Use the vendor-specific robotic control software to load the media into the required recovery device(s).

- 9 Recover the NetBackup catalogs to the alternate disk.

See [“About recovering the NetBackup catalog”](#) on page 146.

The catalogs can be recovered only to the same directory structure from which they were backed up (alternate path recovery is not allowed).

- 10 Start the NetBackup Backup, Archive, and Restore interface (or the `bp` command). Restore the latest backed up version of all files.

You restore these files from the backup of the master server, not from the NetBackup catalog backup. Be sure to specify the disk that you recover as the alternate recovery location.

---

**Warning:** Do not restore files to the `/usr/opensv/var`, `/usr/opensv/db/data`, or `/usr/opensv/volmgr/database` directories (or relocated locations) or the directories that contain NetBackup database data. This data was recovered to the alternate disk in step 9 and is copied back to the recovery disk in step 12.

---

- 11 Stop all NetBackup processes that you started from NetBackup on the alternate disk. Use the **Activity Monitor** in the NetBackup Administration Console or the following:

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

- 12 Maintaining the same directory structure, copy the NetBackup catalogs from the alternate disk to the disk that you recover. These are the catalogs recovered in step 9.
- 13 Make the recovered disk the boot disk again and restart the system.
- 14 Start and test the copy of NetBackup on the disk that you have recovered.

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

Try the NetBackup Administration utilities. Also, try some backups and restores.

- 15 When you are satisfied that the recovery is complete, delete the NetBackup files from the alternate disk. Or, unhook that disk, if it is a spare.

## About recovering the NetBackup media server disk for UNIX

NetBackup 6.0 and later media servers store information in the NetBackup relational database. If you need to recover the system disk on a NetBackup media server, the recommended procedure is similar to disk recovery for the client.

See [“Recovering the system disk on a UNIX client workstation”](#) on page 130.

## Recovering the system disk on a UNIX client workstation

The following procedure recovers the client by reloading the operating system, installing NetBackup client software, and then restoring all other files. The procedure assumes that the host name does not change.

### To recover the system disk on a client workstation

- 1 Install the operating system as you normally would for a client workstation of that type.
- 2 Install NetBackup client software and patches.
- 3 Use the NetBackup Backup, Archive, and Restore interface to select and restore user files.

## About clustered NetBackup server recovery for UNIX and Linux

NetBackup server clusters do not protect against catalog corruption, loss of the shared disk, or loss of the whole cluster. Regular catalog backups must be performed. More information is available about configuring catalog backups and system backup policies in a clustered environment.

See the *NetBackup High Availability Guide*:

<http://www.symantec.com/docs/DOC5332>

The following table describes the failure scenarios and points to the recovery procedures.

---

**Warning:** Before attempting any of the recovery procedures in this topic, contact technical support.

---

**Table 4-1** Cluster failure and recovery scenarios

| Scenario            | Procedure   |
|---------------------|---|
| Node failure        | See “ <a href="#">Replacing a failed node on a UNIX or Linux cluster</a> ” on page 131. |
| Shared disk failure | See “ <a href="#">Recovering the entire UNIX or Linux cluster</a> ” on page 132.        |
| Cluster failure     | See “ <a href="#">Recovering the entire UNIX or Linux cluster</a> ” on page 132.        |

## Replacing a failed node on a UNIX or Linux cluster

Cluster technology-specific information is available about how to bring the NetBackup resource group online and offline. Also, information about how to freeze and unfreeze (that is, disable and enable monitoring for) the NetBackup Resource group.

Refer to topics about configuring NetBackup in the *NetBackup High Availability Guide*:

<http://www.symantec.com/docs/DOC5332>

The following procedure applies when the shared disk and at least one configured cluster node remain available.

### To replace a failed node on a UNIX or Linux cluster

- 1 Configure the hardware, system software, and cluster environment on the replacement node.
- 2 Verify that the device configuration matches that of the surviving nodes.
- 3 Ensure that the NetBackup Resource group is offline on all nodes before installing NetBackup on the replacement node.
- 4 Ensure that the NetBackup shared disks are not mounted on the node on which NetBackup is to be installed.
- 5 Freeze the NetBackup service.
- 6 Reinstall NetBackup on the new node or replacement node. Be sure to use the NetBackup Virtual Name as the name of the NetBackup server. Follow the instructions for installing the NetBackup server software.

Refer to the *NetBackup Installation Guide*:

<http://www.symantec.com/docs/DOC5332>

- 7 Install any Maintenance Packs and patches that are required to bring the newly installed node to the same patch level as the other cluster nodes.
- 8 Bring the NetBackup Resource group online on a node other than the freshly installed node.
- 9 Log onto the node on which the NetBackup resource group is online and run the following command:

```
/usr/opensv/netbackup/bin/cluster/cluster_config -s nbu -o  
add_node -n node_name
```

*node\_name* is the name of the freshly installed node.

- 10 Switch the NetBackup resource group to the replacement node.
- 11 Freeze the NetBackup group.

- 12 Ensure that the appropriate low-level tape device and robotic control device configuration necessary for your operating system has been performed. Information is available for your operating system.  
Refer to the *NetBackup Device Configuration Guide*:  
<http://www.symantec.com/docs/DOC5332>
- 13 Run the **Device Configuration Wizard** to configure the devices. You do not have to rerun the device configuration on the pre-existing nodes. Configuration information on your particular cluster is available.  
See the *NetBackup Administrator's Guide, Volume I*:  
<http://www.symantec.com/docs/DOC5332>
- 14 Check that the robot numbers and robot drive numbers for each robot are consistent across all nodes of the cluster. Repeat for any other servers that are connected to that robot and correct if necessary.  
See the *NetBackup Administrator's Guide, Volume 1*:  
<http://www.symantec.com/docs/DOC5332>
- 15 Test the ability of NetBackup to perform restores using the configured devices on the replacement node.
- 16 Unfreeze the NetBackup resource group.

## Recovering the entire UNIX or Linux cluster

The following procedure applies to the clustered NetBackup server environment that must be re-created from scratch.

Before you proceed, ensure that you have valid online catalog backups.

### To recover the entire UNIX or Linux cluster

- 1 Configure the hardware, system software, and cluster environment on the replacement cluster.
- 2 Ensure that the appropriate low-level tape device and robotic control device configuration necessary for your operating system has been performed.

Refer to the *NetBackup Device Configuration Guide*:

<http://www.symantec.com/docs/DOC5332>

- 3 Reinstall NetBackup on each of the cluster nodes. Be sure to use the NetBackup Virtual Name as the name of the NetBackup server. Follow the instructions for installing NetBackup server software.

Refer to the *NetBackup Installation Guide*:

<http://www.symantec.com/docs/DOC5332>

- 4 Configure the clustered NetBackup server.

Refer to the *NetBackup High Availability Guide*:

<http://www.symantec.com/docs/DOC5332>

- 5 Install any Maintenance Packs and patches that are required to bring the newly installed NetBackup server to the same patch level as the server being replaced

- 6 Configure required devices and media and recover the NetBackup catalogs.

See “[Recovering the master server when root is intact](#)” on page 125.

- 7 Bring the NetBackup resource group on each node in turn and run the **Device Configuration** Wizard to configure the devices.

Configuration information on your particular cluster is available.

Refer to the *NetBackup High Availability Guide*:

<http://www.symantec.com/docs/DOC5332>

## About disk recovery procedures for Windows

The three different types of disk recovery for Windows are as follows:

- Master server disk recovery procedures  
See “[About recovering the master server disk for Windows](#)” on page 134.
- Media server disk recovery procedures  
See “[About recovering the NetBackup media server disk for Windows](#)” on page 139.
- Client disk recovery procedures  
See “[Recovering a Windows client disk](#)” on page 140.

The disk-based images that reside on AdvancedDisk or on OpenStorage disks cannot be recovered by means of the NetBackup catalog. These disk images must be recovered by means of the NetBackup import feature. For information on import, refer to the section on importing NetBackup images in the following manual:

See *NetBackup Administrator's Guide, Volume I*:

<http://www.symantec.com/docs/DOC5332>

---

**Note:** When the disk image is imported, NetBackup does not recover the original catalog entry for the image. Instead, a new catalog entry is created.

---

## About recovering the master server disk for Windows

The procedure in this section explains how to recover data if one or more disk partitions are lost on a Windows NetBackup master server.

The following two scenarios are covered:

- Windows is intact and not corrupted. The system still starts Windows, but some or all other partitions are lost. NetBackup software is assumed to be lost. See “[Recovering the master server with Windows intact](#)” on page 134.
- All disk partitions are lost. Windows must be reinstalled, which is a total recovery. These procedures assume that the NetBackup master disk was running a supported version of Windows and that the defective hardware has been replaced. See “[Recovering the master server and Windows](#)” on page 136.

For NetBackup master and media servers, the directory locations of the NetBackup catalog become an integral part of NetBackup catalog backups. Any recovery of the NetBackup catalog requires the identical directory paths or locations be created before the catalog recovery.

### Recovering the master server with Windows intact

This procedure shows how to recover the NetBackup master server with the Windows operating system intact.

#### To recover the master server with Windows intact

- 1 Determine the *install\_path* in which NetBackup is installed. By default, NetBackup is installed in the `C:\Program Files\VERITAS` directory.
- 2 Determine if any directory paths or locations need to be created for NetBackup catalog recovery.
- 3 Partition any disks being recovered as they were before the failure (if partitioning is necessary). Then reformat each partition as it was before the failure.
- 4 Reinstall NetBackup software on the server.  
Refer to the *NetBackup Installation Guide*:  
<http://www.symantec.com/docs/DOC5332>
- 5 Install any NetBackup patches that had been previously installed. See the documentation that was included with the patch software.

- 6 If the catalog directories differ from those in the NetBackup catalog backups, recreate that directory structure on disk before you recover the catalog. For example, use the NetBackup `nbdb_move` command to relocate parts of the NetBackup relational database catalog.
- 7 If the recovery scenario involves restoring policy or catalog backups, the appropriate recovery devices must be configured.

You may have to do some or all of the following:

- Install and configure the robotic software for the devices that read backups of the NetBackup catalog and regular backups of the disk being restored. If a non-robotic drive is available that can read these backups, then no robot is required. Although manual intervention is required if multiple pieces of media are required.  
See the *NetBackup Device Configuration Guide*:  
<http://www.symantec.com/docs/DOC5332>
  - Use the **NetBackup Device Configuration Wizard** to discover and configure the recovery device in NetBackup.  
See the *NetBackup Administrator's Guide, Volume I*:  
<http://www.symantec.com/docs/DOC5332>
  - Use the NetBackup `tpautoconf` command to discover and configure the recovery device in NetBackup.  
See the *NetBackup Commands Reference Guide* manual:  
<http://www.symantec.com/docs/DOC5332>
  - Update the device mapping files.  
See the *NetBackup Administrator's Guide, Volume I*:  
<http://www.symantec.com/docs/DOC5332>
- 8 If the recovery scenario involves restoring the policy backups or catalog backups that were done to media, the appropriate recovery device(s) must be configured.  
Configuring the media may involve the following actions:
    - Manually load the required media into a standalone recovery device.
    - Use NetBackup utilities such as `robtest` or vendor-specific robotic control software to load media into the required recovery devices.
    - Use the NetBackup Volume Configuration Wizard to inventory the media contents of a robotic device.
    - Use the vendor-specific robotic control software to load the media into the required recovery device(s).

9 Recover the NetBackup catalogs.

See “[About recovering the NetBackup catalog](#)” on page 146.

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
```

---

**Warning:** In step 11, do not restore files to the `install_path\NetBackup\db`, `install_path\NetBackupDB`, `install_path\NetBackup\var`, or `install_path\Volmgr\database` directories. The catalogs were recovered in step 9 and overwriting them with regular backups leave them in an inconsistent state.

---

If the NetBackup relational database files were relocated using `nbdb_move` from `install_path\NetBackupDB\data`, they are recovered in step 9 and should not be restored in step 11.

11 To restore all other files, do the following actions in the order shown:

- Start the NetBackup Administration interface on the master server.
- Start the Backup, Archive, and Restore utility.
- Browse for restores and select only the partitions that were lost. Select the system directory (typically `C:\Windows`), which ensures that all registry files are restored.
- Deselect the `install_path\NetBackup\db`, `install_path\NetBackupDB`, `install_path\NetBackup\var`, and `install_path\Volmgr\database` directories (see the caution in step 10).
- If you reinstall Windows, select the **Overwrite existing files** option, which ensures that existing files are replaced with the backups.
- Start the restore.

12 Restart the system, which replaces any files that were busy during the restore. When the boot process is complete, the system is restored to the state it was in at the time of the last backup.

## Recovering the master server and Windows

This procedure assumes that all disk partitions in Windows are lost.

### To recover the master server and Windows

- 1 Install a minimal Windows operating system (perform the Express install).
  - Install the same type and version of Windows software that was used previously.
  - Install Windows in the same partition that was used before the failure.
  - Install any required patches. Take corrective action as needed.
  - Specify the default workgroup. Do not restore the domain.
  - Install and configure special drivers or other software that is required to get the hardware operational (for example, a special driver for the disk drive).
  - Install SCSI or other drivers as needed to communicate with the tape drives on the system.
  - Follow any hardware manufacturer's instructions that apply, such as loading SSD on a Compaq system.
  - Restart the system when Windows installation is complete.
- 2 Determine the *install\_path* in which NetBackup is installed. By default, NetBackup is installed in the `C:\Program Files\VERITAS` directory.
- 3 Determine if any directory paths or locations need to be created for NetBackup catalog recovery.
- 4 If necessary, partition any disks being recovered as they were before the failure. Then reformat each partition as it was before the failure.
- 5 Reinstall NetBackup software on the server being recovered. Do not configure any NetBackup policies or devices at this time.
- 6 Install any NetBackup patches that had been previously installed. See the documentation that was included with the patch software.
- 7 If the catalog directories differ from those in the NetBackup catalog backups, recreate that directory structure on disk before you recover the catalog. For example, use the NetBackup `nbdb_move` command to relocate parts of the NetBackup relational database catalog.
- 8 If the recovery scenario involves restoring policy or catalog backups, the appropriate recovery device or devices have to be configured.

You may have to do all or some of the following tasks:

  - Install and configure the robotic software for the devices that read backups of the NetBackup catalog and regular backups of the disk being restored. If a non-robotic drive is available that can read these backups, then no robot

is required. Although manual intervention is required if multiple pieces of media are required.

See the *NetBackup Device Configuration Guide*:

<http://www.symantec.com/docs/DOC5332>

- Use the NetBackup **Device Configuration** Wizard to discover and configure the recovery device in NetBackup.

See the *NetBackup Administrator's Guide, Volume I*:

<http://www.symantec.com/docs/DOC5332>

- Use the NetBackup command `tpautoconf` to discover and configure the recovery device in NetBackup.

See the *NetBackup Commands Reference Guide* manual:

<http://www.symantec.com/docs/DOC5332>

- Update the device mapping files.

See the *NetBackup Administrator's Guide, Volume I*:

<http://www.symantec.com/docs/DOC5332>

- 9 If you must restore from the policy backups or catalog backups that were done to media, the appropriate media may have to be configured in NetBackup.

See the *NetBackup Administrator's Guide, Volume I*:

<http://www.symantec.com/docs/DOC5332>

When you configure the media, you may have to do some or all of the following:

- Manually load the required media into a standalone recovery device.
- Use the NetBackup utilities such as `robtest` or vendor-specific robotic control software to load media into the required recovery devices.
- Use the NetBackup Volume Configuration Wizard to inventory the media contents of a robotic device.
- Use the vendor-specific robotic control software to load the media into the required recovery devices.

- 10 Recover the NetBackup catalogs.

See “[About recovering the NetBackup catalog](#)” on page 146.

- 11 When catalog recovery is complete, stop and restart the NetBackup services. Use the following `bpdown` and `bpup` commands, the **Activity Monitor** in the **NetBackup Administration Console**, or the Services application in the Windows Control Panel.

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

---

**Warning:** In step 12, do not restore files to the `install_path\NetBackup\db`, `install_path\NetBackupDB`, `install_path\NetBackup\var`, or `install_path\Volmgr\database` directories. These directories were recovered in step 10 and overwriting them with regular backups leaves the catalogs in an inconsistent state. If the relational database files were relocated using `nbdb_move` from `install_path\NetBackupDB\data`, they are recovered in step 10 and should not be restored in step 12.

---

- 12 To restore all other files, do the following steps in the order presented:
  - Start the NetBackup Administration interface on the master server.
  - Start the Backup, Archive, and Restore client interface.
  - Browse for restores and select only the partitions that were lost. Select the system directory (typically `C:\Windows`), which ensures that all registry files are restored.
  - Deselect the `install_path\NetBackup\db`, `install_path\NetBackupDB` (or relocated NetBackup relational database path), `install_path\NetBackup\var`, or `install_path\Volmgr\database` directories.  
See the caution in this procedure.
  - If you reinstall Windows, select the **Overwrite existing files** option, which ensures that existing files are replaced with the backups.
  - Start the restore.
- 13 Restart the system, which replaces any files that were busy during the restore. When the boot process is complete, the system is restored to the state it was in at the time of the last backup.

## About recovering the NetBackup media server disk for Windows

NetBackup media servers store their information in the NetBackup relational database. If you need to recover the system disk on a NetBackup media server, the recommended procedure is similar to disk recovery for the client.

See “[Recovering a Windows client disk](#)” on page 140.

## Recovering a Windows client disk

The following procedure explains how to perform a total recovery of a Windows NetBackup client in the event of a system disk failure.

NetBackup Bare Metal Restore (BMR) protects client systems by backing them up with a policy configured for BMR protection. A complete description of BMR backup and recovery procedures is available.

See the *Bare Metal Restore System Administrator's Guide*:

<http://www.symantec.com/docs/DOC5332>

This procedure assumes that the Windows operating system and NetBackup are reinstalled to boot the system and perform a restore.

The following are additional assumptions:

- The NetBackup client was running a supported Microsoft Windows version.
- The NetBackup client was backed up with a supported version of NetBackup client and server software.
- The NetBackup master server to which the client sent its backups is operational. You request the restore from this server.
- The backups included the directory where the operating system and its registry resided.

If the backups excluded any files that resided in the directory, you may not be able to restore the system identically to the previous configuration.

- Defective hardware has been replaced.

Before starting, verify that you have the following:

- Windows system software to reinstall on the NetBackup client that being restored. Reinstall the same type and version of software that was previously used.
- NetBackup client software to install on the client that being restored.
- Special drivers or other software that is required to make the hardware operational (for example, a special driver for the disk drive).
- IP address and host name of the NetBackup client.
- IP address and host name of the NetBackup master server.
- The partitioning and the formatting scheme that was used on the system to be restored. You must duplicate that scheme during Windows installation.

**To recover a Windows client disk**

- 1 Install a minimal Windows operating system (perform the Express install).  
During the installation, do the following tasks:
  - Partition the disk as it was before the failure (if partitioning is necessary). Then, reformat each partition as it was before the failure.
  - Install the operating system in the same partition that was used before the failure.
  - Specify the default workgroup. Do not restore to the domain.
  - Follow any hardware manufacturers' instructions that apply.
- 2 Reboot the system when the installation is complete.
- 3 Configure the NetBackup client system to re-establish network connectivity to the NetBackup master server.

For example, if your network uses DNS, the configuration on the client must use the same IP address that was used before the failure. Also, it must specify the same name server (or another name server that recognizes both the NetBackup client and master server). On the client, configure DNS in the **Network** dialog, accessible from the Windows Control Panel.

- 4 Install NetBackup client software.  
Ensure that you specify the correct names for the client server and master server.
  - To specify the client name, start the Backup, Archive, and Restore interface on the client and click **NetBackup Client Properties** on the **File** menu. Enter the client name on the **General** tab of the **NetBackup Client Properties** dialog.
  - To specify the server name, click **Specify NetBackup Machines and Policy Type** on the **File** menu.

Refer to the *NetBackup Installation Guide* for instructions:

<http://www.symantec.com/docs/DOC5332>

- 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\bpinstd
```

NetBackup creates logs in these directories.

- 7 Stop and restart the NetBackup Client service.  
This action enables NetBackup to start logging to the `bpineted` debug log.
- 8 Use the NetBackup Backup, Archive, and Restore interface to restore the system files and user files to the client system.  
For example, if all files are on the `C` drive, restoring that drive restores the entire system.  
To restore files, you do not need to be the administrator, but you must have restore privileges. For instructions, refer to the online Help or refer to the following:  
See the *NetBackup Backup, Archive, and Restore Getting Started Guide*:  
<http://www.symantec.com/docs/DOC5332>  
NetBackup restores the registry when it restores the Windows system files. For example, if the system files are in the `C:\Winnt` directory, NetBackup restores the registry when it restores that directory and its subordinate subdirectories and files.
- 9 Check for ERR or WRN messages in the log files that are in the directories you created in step 6.  
If the logs indicate problems with the restore of Windows system files, resolve those problems before proceeding.
- 10 Stop the NetBackup Client service and verify that the `bpineted` program is no longer running.
- 11 Restart the NetBackup client system.  
When the boot process is complete, the system is restored to the state it was in at the time of the last backup.

## About clustered NetBackup server recovery for Windows

NetBackup server clusters do not protect against catalog corruption, loss of the shared disk, or loss of the whole cluster. Regular catalog backups must be performed. More information is available about configuring catalog backups and system backup policies in a clustered environment.

Refer to topics about configuring NetBackup in the *NetBackup High Availability Guide*:

<http://www.symantec.com/docs/DOC5332>

---

**Warning:** Contact technical support before you try these recovery procedures.

---

## Replacing a failed node on a Windows VCS cluster

Cluster technology-specific information is available about how to bring the NetBackup resource group online and offline. Also, it is available on how to freeze and unfreeze (disable and enable the monitoring for) the resource group.

Refer to topics about configuring NetBackup in the *NetBackup High Availability Guide*:

<http://www.symantec.com/docs/DOC5332>

Check the following conditions before you proceed with this procedure:

- The hardware, system software, and cluster environment on the replacement node have been configured.
- The reconfigured node or replacement node has been made a member of the cluster and has the same name as the failed node.

The following procedure applies when the shared disk and at least one configured cluster node remain available.

### To replace a failed node on a Windows cluster using VCS

- 1 Freeze the NetBackup service.
- 2 Ensure that the NetBackup shared disks are not mounted on the node on which NetBackup is to be installed.
- 3 Reinstall NetBackup on the new node or replacement node. Be sure to use the NetBackup Virtual Name as the name of the NetBackup server. Follow the instructions for installing the NetBackup server software.

Refer to the *NetBackup Installation Guide*:

<http://www.symantec.com/docs/DOC5332>

- 4 Ensure that the node is a member of an existing cluster and that it performs the necessary configuration automatically.
- 5 Install any Maintenance Packs and patches that are required to bring the newly installed node to the same patch level as the other cluster nodes.
- 6 Unfreeze the NetBackup service and verify that it can be brought up on the replacement node.

## Recovering the shared disk on a Windows VCS cluster

The following procedure is applicable in situations where the configured cluster nodes remain available but the NetBackup catalog, database files, or both on the shared disk have been corrupted or lost.

Check the following conditions before you proceed with this procedure:

- The shared storage hardware is restored to a working state, so that the shared disk resource can be brought online with an empty shared directory.
- Valid online catalog backups exist.

### To recover the shared disk on a Windows cluster that uses VCS

- 1 Clear the faulted NetBackup resource group, disable monitoring, and bring up the shared disk and virtual name resources on a functioning node.
- 2 Ensure that all NetBackup shared disks are assigned the same drive letters that were used when NetBackup was originally installed and configured.
- 3 To reconfigure NetBackup for the cluster, initialize the database by running the following commands in sequence on the active node:

```
bpclusterutil -ci  
tpext  
bpclusterutil -online
```

- 4 Use the appropriate NetBackup catalog recovery procedure to restore the NetBackup catalog information on the shared disk.  
See [“Recovering the master server and Windows”](#) on page 136.
- 5 If the clustered NetBackup server is a media server, verify that the restored `vm.conf` file contains the correct host-specific `MM_SERVER_NAME` configuration entry for the active node. If `MM_SERVER_NAME` is different from the local host name, edit the file and change the server name to the local host name:  
`MM_SERVER_NAME=<local host name>`
- 6 Use NetBackup to restore any data on the shared disks. Details are available on how to perform a restore.  
Refer to the *NetBackup Backup, Archive, and Restore Getting Started Guide*:  
<http://www.symantec.com/docs/DOC5332>
- 7 Configure required devices and media and recover the NetBackup catalogs.
- 8 Manually shut down and restart NetBackup on the active node.

- 9 Re-enable monitoring of the NetBackup resource group.
- 10 Verify that the NetBackup server can now be brought online on all configured nodes.

## Recovering the entire Windows VCS cluster

The following procedure applies to the clustered NetBackup server environment that must be re-created from scratch.

Before you proceed, ensure that you have valid online catalog backups.

### To recover the entire Windows VCS cluster

- 1 Configure the hardware, system software, and cluster environment on the replacement cluster.
- 2 Ensure that the appropriate low-level tape device and robotic control device configuration necessary for your operating system has been performed.  
Refer to the *NetBackup Device Configuration Guide*:  
<http://www.symantec.com/docs/DOC5332>
- 3 Reinstall NetBackup on each of the cluster nodes. Be sure to use the NetBackup Virtual Name as the name of the NetBackup server. Follow the instructions for installing NetBackup server software.  
Refer to the *NetBackup Installation Guide*:  
<http://www.symantec.com/docs/DOC5332>
- 4 Configure the clustered NetBackup server.  
Refer to the *NetBackup High Availability Guide*:  
<http://www.symantec.com/docs/DOC5332>
- 5 Install any Maintenance Packs and patches that are required to bring the newly installed NetBackup server to the same patch level as the server that is being replaced.
- 6 Configure required devices and media and recover the NetBackup catalogs.  
See “[Recovering the master server and Windows](#)” on page 136.
- 7 Bring the NetBackup resource group on each node in turn and run the **Device Configuration** Wizard to configure the devices.  
Configuration information on your cluster (MSCS or VCS) is available.  
Refer to the *NetBackup High Availability Guide*:  
<http://www.symantec.com/docs/DOC5332>

# About recovering the NetBackup catalog

Before you recover the NetBackup catalog, ensure that NetBackup is running in the recovery environment. Ensure that the recovery devices are configured in NetBackup. Ensure that the media on which the catalog backups exist are available to NetBackup. If the NetBackup master server is part of a cluster, ensure that the cluster is functional.

The NetBackup catalog consists of several parts. How you recover the catalog depends on which part or parts of the catalog you want to recover, as follows:

**Table 4-2** Catalog recovery options

| Recovery option   | Description   |
|---|---|
| Recover the entire catalog                              | <p>Symantec recommends that you recover the entire catalog. Doing so helps ensure consistency among the various parts of the catalog. This method is most useful for recovering a catalog to the same environment from which it was backed up.</p> <p>See <a href="#">“About recovering the entire NetBackup catalog”</a> on page 152.</p>  |
| Recover the catalog image files and configuration files | <p>The image database contains information about the data that has been backed up. The configuration files (<code>databases.conf</code> and <code>server.conf</code>) are the flat files that contain instructions for the SQL Anywhere daemon.</p> <p>This type of recovery also restores the NetBackup relational database (NBDB) to the staging directory so that it is available for further processing if required.</p> <p>See <a href="#">“About recovering the NetBackup catalog image files”</a> on page 163.</p>   |
| Recover the relational database files                   | <p>The NetBackup database (NBDB) is also known as the Enterprise Media Manager (EMM) database. It contains information about volumes and the robots and drives that are in NetBackup storage units. The NetBackup relational database also contains the NetBackup catalog images files. The images files contain the metadata that describes the backups.</p> <p>Recover the relational database if it is corrupt or lost but the catalog image files exist and are valid.</p> <p>See <a href="#">“About recovering the NetBackup relational database”</a> on page 176.</p> |

Recovery of the entire catalog or the catalog image files relies on the disaster recovery information. That information is saved in a file during the catalog backup. The location of the disaster recovery file is configured in the catalog backup policy.

See [“NetBackup disaster recovery email example”](#) on page 149.

If you do not have the disaster recovery file, you still can recover the catalog. However, the process is much more difficult and time-consuming.

See [“Recovering the NetBackup catalog without the disaster recovery file”](#) on page 186.

---

**Note:** After a catalog recovery, NetBackup freezes the removeable media that contains the catalog backup. This operation prevents a subsequent accidental overwrite action on the final catalog backup image on the media. This final image pertains to the actual catalog backup itself, and its recovery is not part of the catalog recovery. You can unfreeze the media.

See [“Unfreezing the NetBackup online catalog recovery media”](#) on page 191.

---

Other procedures exist for special use cases.

See [“Recovering the NetBackup catalog when NetBackup Access Control is configured”](#) on page 184.

Other topics provide more information about catalog recovery.

See [“About NetBackup catalog recovery on Windows computers”](#) on page 147.

See [“About NetBackup catalog recovery from disk devices”](#) on page 147.

See [“About NetBackup catalog recovery and OpsCenter”](#) on page 148.

## About NetBackup catalog recovery on Windows computers

On Windows computers, the NetBackup media server host names are stored in the Windows registry. (They also are stored in the NetBackup catalog.)

If you install NetBackup during a catalog recovery scenario, ensure that you enter your media server names during the installation. Doing so adds them to the registry. Your catalog recovery and any subsequent backups that use the existing media servers and storage devices then function correctly.

## About NetBackup catalog recovery from disk devices

In a catalog recovery, the disk media IDs in the recovery environment may differ from the disk media IDs in the backup environment. They may differ in the following uses cases:

- The storage devices are the same but the NetBackup master server installation is new. A master server host or disk failure may require that you install NetBackup. Configuring the devices in NetBackup may assign different disk media IDs to the disk volumes than were assigned originally.
- The disk storage devices are different than those to which the catalog backups were written. It may be in the same environment after storage hardware failure or replacement. It may be at another site to which you replicate the catalog backups and the client backups. Regardless, the catalog backups and the client backups reside on different hardware. Therefore, the disk media IDs may be different .

In these scenarios, NetBackup processes the disk media IDs so that the catalog may be recovered. The processing maps the disk media IDs from the backup environment to the disk media IDs in the recovery environment.

This processing occurs when the catalog backup resides on one of the following storage types:

- An AdvancedDisk disk pool
- A **Media Server Deduplication Pool (MSDP)**
- An OpenStorage device

## About NetBackup catalog recovery and symbolic links

When you recover the NetBackup catalog, you must account for any symbolic links in the NetBackup catalog directory structure, as follows:

`db/images` directory    If the NetBackup `db/images` directory resides on the storage that is the target of a symbolic link, that symbolic link must exist in the recovery environment. The symbolic link also must have the same target in the recovery environment.

`db/images/client` directories    If any of the client subdirectories under the `db/images` directory are symbolic links, they also must exist in the recovery environment. The symbolic links also must have the same targets in the recovery environment.

Catalog recovery of clustered master server    To recover the NetBackup catalog from a clustered master server to a single master server at a disaster recovery site, you must create the following symbolic links on the recovery host before you recover the catalog:

```
/usr/opensv/netbackup/db -> /opt/VRTSnbu/netbackup/db  
/usr/opensv/db/staging -> /opt/VRTSnbu/db/staging
```

On Solaris systems only, you also must create the following symbolic links before you recover the catalog:

```
/usr/opensv -> /opt/opensv
```

If the symbolic links and their targets do not exist, catalog recovery fails.

## About NetBackup catalog recovery and OpsCenter

When the NetBackup catalog is recovered, NetBackup resets the job ID to 1. NetBackup starts assigning job numbers beginning with 1.

If you use NetBackup OpsCenter to monitor NetBackup activity, you may see duplicate job IDs in OpsCenter after a catalog recovery. To prevent duplicate job IDs, you can specify the job ID from which NetBackup should number jobs after the recovery.

See [“Specifying the NetBackup job ID number after a catalog recovery”](#) on page 149.

## Specifying the NetBackup job ID number after a catalog recovery

You can specify the NetBackup job ID number after a catalog recovery. If you use OpsCenter to monitor NetBackup activity, doing so prevents duplicate job ID numbers in OpsCenter.

See [“About NetBackup catalog recovery and OpsCenter”](#) on page 148.

### To specify the NetBackup job ID number after a catalog recovery

- 1 If necessary, restore the OpsCenter database from a backup.
- 2 Determine the last job ID number that is recorded in OpsCenter.
- 3 Edit the NetBackup `jobid` file and set the value to one higher than the number from step 2. The following is the pathname to the `jobid` file:
  - UNIX: `/usr/opensv/netbackup/db/jobs/jobid`
  - Windows: `install_path\Veritas\NetBackup\db\jobs\jobid`

Because the recovery consumes job numbers, you must specify the number before the catalog recovery.

- 4 Recover the NetBackup catalog.

## NetBackup disaster recovery email example

A catalog backup policy can send a disaster recovery email upon completion of a catalog backup. To configure a catalog backup policy, see the *NetBackup Administrator's Guide, Volume I*:

<http://www.symantec.com/docs/DOC5332>

The following is an example of a disaster recovery email after a successful catalog backup:

```
From: Netbackup.master.example.com
Sent: Monday, January 2, 2012 1:26 PM
To: NetBackup Administrator
Subject: NetBackup Catalog Backup successful on host master.example.com status 0
```

Server

master.example.com

NetBackup Version

7.6.1

Date

Thur Jan 1 13:05:44 2015

Policy

cat

Catalog Backup Status

the requested operation was successfully completed (status 0).

DR image file:

/backup/dr/cat\_1305655567\_FULLL

To ensure that the NetBackup catalog data is protected through Thur Jan 15 13:05:44 2015, retain a copy of the attached file, and the media or files listed below:

Catalog Recovery Media

| Media Server        | Disk Image Path                                 | Image File Required  |
|---------------------|---|----------------------|
| * media.example.com | /backup/nb/master.example.com_1305655547_C1_F1  | cat_1305655547_FULLL |
| * media.example.com | /backup/nb/master.example.com_1305655567_C1_F1  | cat_1305655567_FULLL |
| * media.example.com | /backup/nb/master.example.com_1305655567_C1_TIR | cat_1305655567_FULLL |

DR file written to

/backup/dr/cat\_1305655567\_FULLL

\* - Primary Media

Catalog Recovery Procedure for the Loss of an Entire Catalog

You should create a detailed disaster recovery plan to follow should it become necessary to restore your organization's data in the event of a disaster. A checklist of required tasks can be a tremendous tool in assisting associates in triage. For example, after the facility is safe for data to be restored, the power and data infrastructure need to be verified. When these tasks are completed, the following scenarios will 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 (If using OpenStorage disk pools, refer to the Shared Storage Guide to configure the disk pools instead of step 2 and 3 below):

1. Install NetBackup.
2. Configure the devices necessary to read the media listed above.
3. Inventory the media.
4. Run:  
`bpimport -create_db_info [-server name] -id /backup/nb`
5. Run:  
`cat_export -client master.example.com`
6. Go to the following directory to find the DR image file  
`cat_1305655567_FULL:`  
`/usr/opensv/netbackup/db.export/images/master.example.com/1305000000`
7. Open `cat_130655567_FULL` file and find the `BACKUP_ID` (for example: `master.example.com_1305655567`).
8. Run:  
`bpimport [-server name] -backupid master.example.com_1305655567`
9. Run:  
`bprestore -T -w [-L progress_log] -C master.example.com -t 35`

- ```
-p cat -X -s 1305655567 -e 1305655567 /
```
10. Run the BAR user interface to restore the remaining image database if the DR image is a result of an incremental backup.
  11. To recover the NetBackup relational database, run:  

```
bprecover -r -nbdb
```
  12. Stop and Start NetBackup
  13. Configure the devices if any device has changed since the last backup.
  14. To make sure the volume information is updated, inventory the media to update the NetBackup database.

See [“About recovering the NetBackup catalog”](#) on page 146.

## About recovering the entire NetBackup catalog

Symantec recommends that you recover the entire catalog. Doing so helps ensure consistency among the various parts of the catalog.

Recovery includes the catalog image files and configuration files that are in the catalog backups that are identified by the disaster recovery file, as follows:

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Full backup        | The NetBackup relational database files identified by the DR file are restored. The images and configuration files that are identified by the disaster recovery file are restored.                                                                                                                                                                                                                                           |
| Incremental backup | The NetBackup relational database files identified by the DR file are restored. All catalog backup image files back to the last full catalog backup are automatically included in an incremental catalog backup. Therefore, only catalog images and configuration files that changed since the last full backup are restored. You can then use the Backup, Archive, and Restore user interface to restore all backup images. |

You can use either of the following methods to recover the entire catalog:

- The **Catalog Recovery Wizard** in the **NetBackup Administration Console**. See [“Recovering the entire NetBackup catalog using the Catalog Recovery Wizard”](#) on page 153.
- The text-based wizard launched by the `bprecover -wizard` command and option. See [“Recovering the entire NetBackup catalog using bprecover -wizard”](#) on page 159.

The relational database transaction log is not applied during full catalog recovery.

<http://www.symantec.com/docs/DOC5332>

## Recovering the entire NetBackup catalog using the Catalog Recovery Wizard

This procedure describes how to recover the entire catalog using the **Catalog Recovery Wizard**. The relational database transaction log is not applied during full catalog recovery.

See [“About recovering the NetBackup catalog”](#) on page 146.

---

**Note:** Full catalog recovery restores the device and the media configuration information in the catalog backup. If you must configure storage devices during the recovery, Symantec recommends that you recover only the NetBackup image files.

See [“About recovering the NetBackup catalog image files”](#) on page 163.

---

You must have root (administrative) privileges.

You must be logged on to the master server on which you want to recover the catalog. The **Catalog Recovery Wizard** does not work after you perform a change server operation.

---

**Note:** During the catalog recovery process, NetBackup may shut down and restart services. If NetBackup is configured as a highly available application (cluster or global cluster), freeze the cluster before you begin the recovery process. Doing so prevents a failover. Then, unfreeze the cluster after the recovery process is complete.

---

**Warning:** Do not run any client backups before you recover the NetBackup catalog.

---

### To recover the entire catalog by using the Catalog Recovery Wizard

- 1 If NetBackup is not running, start all of the NetBackup services by entering the following:
  - On UNIX and Linux:  

```
/usr/opensv/netbackup/bin/bp.start_all
```
  - On Windows:  

```
install_path\NetBackup\bin\bpup
```
- 2 Start the **NetBackup Administration Console**.

- 3 If the catalog backup and the recovery devices are not available, do the following:
  - a Configure the necessary recovery device in NetBackup.

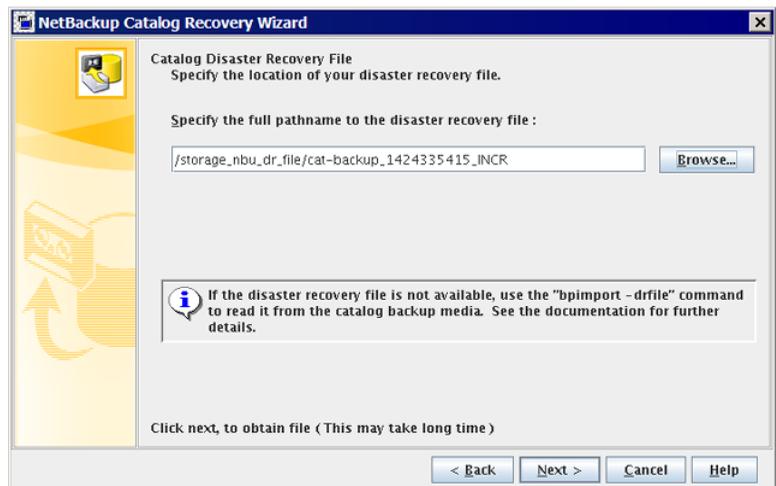
For tape storage or **BasicDisk** storage, see the *NetBackup Administrator's Guide, Volume I*. For disk storage types, see the guide that describes the option. See the following website for NetBackup documentation:  
<http://www.symantec.com/docs/DOC5332>
  - b Make available to NetBackup the media that contains the catalog backup: Inventory the robot or the disk pool, add the media for standalone drives, configure the storage server and disk pool, or so on.

For tape storage or **BasicDisk** storage, see the *NetBackup Administrator's Guide, Volume I*. For disk storage types, see the guide that describes the option. See the following website for NetBackup documentation:  
<http://www.symantec.com/docs/DOC5332>
- 4 In the **NetBackup Administration Console** window, click **NetBackup Management** in the left pane and then **Recover the catalogs** in the right pane. The **Catalog Recovery Wizard Welcome** panel appears.
- 5 Click **Next** on the **Welcome** panel to display the **Catalog Disaster Recovery File** panel.

- 6 On the **Catalog Disaster Recovery File** panel, specify where the disaster recovery file is stored. You can browse to select the file or enter the full pathname to the disaster recovery file.

In most cases, you specify the most recent disaster recovery information file available. If the most recent catalog backup is an incremental backup, use the disaster recovery file from the incremental backup. (There is no need to first restore the full backup and then follow with the incremental backup.)

If some form of corruption has occurred, you may want to restore to an earlier state of the catalog.



Click **Next** to continue. The **Retrieving Disaster Recovery File** panel appears

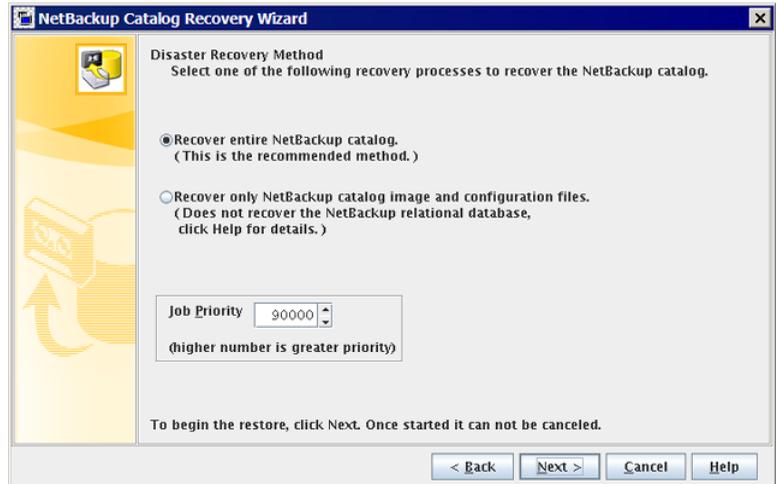
- 7 The wizard searches for the media that are required to recover the catalog, and **Retrieving Disaster Recovery File** panel informs you of the progress. It informs you if the necessary backup ID of the disaster recovery image is located. If the media is not located, the wizard lists which media is needed to update the database.



If necessary, follow the wizard instructions to insert the media that is indicated and run an inventory to update the NetBackup database. The information that is displayed on this panel depends on whether the recovery is from a full backup or an incremental backup.

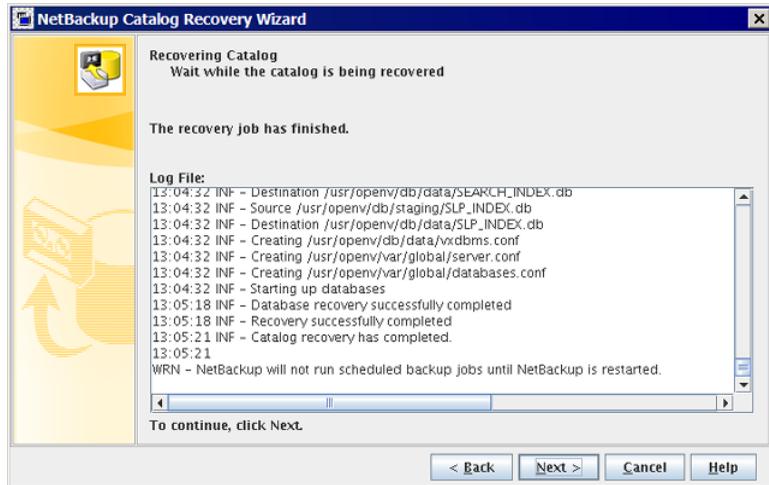
When the required media sources are all found, click **Next** to display the **Disaster Recovery Method** panel.

- 8 By default, the **Recover entire NetBackup catalog** option is selected on the **Disaster Recovery Method** panel.



Select a **Job Priority** if desired and then click **Next** to initiate the recovery of the entire NetBackup catalog. The **Recovering Catalog** panel appears.

- 9 The **Recovering Catalog** panel displays the progress of recovering the various catalog components, as follows:
- NBDB database (including the EMM database)
  - BMR database (if applicable)
  - NetBackup policy files
  - Backup image files to their proper image directories
  - Other configuration files



Your action depends on the outcome of the recovery, as follows:

- |                |                                                                                                                                       |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Not successful | Consult the log file messages for an indication of the problem. Click <b>Cancel</b> , fix the problem, and then run the wizard again. |
| Successful     | Click <b>Next</b> to continue to the final wizard panel.                                                                              |

**10** On the panel that informs you that the recovery is complete, click **Finish**.

**11** Before you continue, be aware of the following points:

- If you recovered the catalog from removable media, NetBackup freezes the catalog media.  
See [“Unfreezing the NetBackup online catalog recovery media”](#) on page 191.
- Before you restart NetBackup, Symantec recommends that you freeze the media that contains the backups more recent than the date of the catalog from which you recovered.
- NetBackup does not run scheduled backup jobs until you stop and then restart NetBackup.  
You can submit backup jobs manually before you stop and restart NetBackup. However, if you do not freeze the media that contains the backups more recent than the date of the catalog from which you recovered, NetBackup may overwrite that media.

**12** Stop and restart NetBackup services on all of the servers, as follows:

- On UNIX and Linux:

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

- On Windows:

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

If the **NetBackup Administration Console** is active on any of the hosts, the command that stops the NetBackup services shuts it down.

- 13 If the catalog recovery is part of a server recovery procedure, complete the remaining steps in the appropriate recovery procedure.

Recovery can include the following:

- Importing the backups from the backup media into the catalog.
- Write protecting the media.
- Ejecting the media and setting it aside.
- Freezing the media.

## Recovering the entire NetBackup catalog using `bprecover -wizard`

The `bprecover -wizard` command is an alternative to using the **NetBackup Administration Console** wizard. You must have root (administrative) privileges to perform this procedure.

The relational database transaction log is not applied during full catalog recovery.

You must have root (administrative) privileges to perform these procedures.

You must be logged on to the master server on which you want to recover the catalog.

---

**Note:** During the catalog recovery process, services may be shut down and restarted. If NetBackup is configured as a highly available application (cluster or global cluster), freeze the cluster before starting the recovery process to prevent a failover. Then unfreeze the cluster after the recovery process is complete.

---

---

**Note:** Full catalog recovery restores the device and the media configuration information in the catalog backup. If you must configure storage devices during the recovery, Symantec recommends that you recover only the NetBackup image files.

See [“About recovering the NetBackup catalog image files”](#) on page 163.

---

**Warning:** Do not run any client backups before you recover the NetBackup catalog.

---

### To recover the entire catalog by using `bprecover -wizard`

- 1 If recovering the catalog to a new NetBackup installation, such as at a disaster recovery site, do the following:
  - Install NetBackup.
  - Configure the devices that are required for the recovery.
  - Add the media that are required for the recovery to the devices.

- 2 Start NetBackup.

The following are the commands to start NetBackup:

- UNIX and Linux:  
`/usr/opensv/netbackup/bin/bp.start_all`
- Windows:  
`install_path\NetBackup\bin\bpup.exe`

- 3 Start the `bprecover` wizard by entering the following command:

- UNIX and Linux:  
`/usr/opensv/netBbckup/bin/admincmd/bprecover -wizard`
- Windows:  
`install_path\Veritas\NetBackup\bin\admincmd\bprecover.exe  
-wizard`

The following is displayed:

```
Welcome to the NetBackup Catalog Recovery Wizard!
```

```
Please make sure the devices and media that contain catalog  
disaster recovery data are available  
Are you ready to continue?(Y/N)
```

- 4 Enter **Y** to continue. The following prompt appears:

```
Please specify the full pathname to the catalog disaster recovery
file:
```

- 5 Enter the fully qualified pathname to the disaster recovery file for the backup that you want to restore. For example:

```
/mnt/hdd2/netbackup/dr-file/Backup-Catalog_1318222845_FULL
```

If the most recent catalog backup was an incremental backup, use the disaster recovery file from the incremental backup. (There is no need to first restore the full backup and then follow with the incremental backup.) Alternately, you can recover from earlier version of the catalog.

If the pathname is to a valid DR file, a message similar to the following is displayed:

```
vm2.example.com_1318222845
All media resources were located
Do you want to recover the entire NetBackup catalog? (Y/N)
```

If the DR file or the pathname is not valid, the command-line wizard exits.

- 6 Enter **Y** to continue. The following is displayed:

```
Do you want to startup the NetBackup relational database (NBDB)
after the recovery?(Y/N)
```

The image file is restored to the proper image directory and the NetBackup relational databases (NBDB and optionally BMRDB) are restored and recovered.

## 7 Enter **Y** or **N** to continue.

The following is displayed while the restore is in progress:

```
Catalog recovery is in progress. Please wait...
```

```
Beginning recovery of NBDB. Please wait...
```

```
Completed successful recovery of NBDB on vm2.example.com
```

```
INF - Catalog recovery has completed.
```

```
WRN - NetBackup will not run scheduled backup jobs until NetBackup  
is restarted.
```

For more information, please review the log file:

```
/usr/opensv/netbackup/logs/user_ops/root/logs/Recover1318344410.log
```

When the recovery job is finished, each image file is restored to the proper image directory, and the NetBackup relational databases (NBDB and optionally BMRDB) have been restored and recovered.

## 8 Before you continue, be aware of the following points:

- If you recovered the catalog from removable media, NetBackup freezes the catalog media.  
See [“Unfreezing the NetBackup online catalog recovery media”](#) on page 191.
- Before you restart NetBackup, Symantec recommends that you freeze the media that contains the backups more recent than the date of the catalog from which you recovered.
- NetBackup does not run scheduled backup jobs until you stop and then restart NetBackup.  
You can submit backup jobs manually before you stop and restart NetBackup. However, if you do not freeze the media that contains the backups more recent than the date of the catalog from which you recovered, NetBackup may overwrite that media.
- Because this operation is a partial recovery, you must recover the relational database portion of the catalog.  
See [“About recovering the NetBackup relational database”](#) on page 176.

## 9 Stop and restart NetBackup.

The following are the commands to stop and restart NetBackup:

- On UNIX and Linux:

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

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

- On Windows:

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

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

- 10 If the catalog recovery is part of a server recovery procedure, complete the remaining steps in the appropriate recovery procedure.

This procedure can include the following tasks:

- Importing the backups from the backup media into the catalog
- Write protecting the media
- Ejecting the media and setting it aside
- Freezing the media

## About recovering the NetBackup catalog image files

The catalog image files contain information about all the data that has been backed up. This information constitutes the largest part of the NetBackup catalog. This type of catalog recovery does the following:

- Recovers the image `.f` files.
- Recovers the configuration files (`databases.conf` and `server.conf`).
- Restores the NetBackup relational database (NBDB) to the staging directory so that it is available for further processing if required.  
See [“About processing the relational database in staging”](#) on page 183.
- Optionally, recovers the policy and the licensing data.

[Table 4-3](#) is a list of the files that are included in a partial recovery.

---

**Note:** Beginning with the NetBackup 7.5 release, the images files are now stored in the NetBackup relational database. The images files contain the metadata that describes the backups.

---

NetBackup supports recovery of the catalog image files and configuration files from a clustered environment to a non-clustered master server at a disaster recovery.

### Recovery recommendations

See [“About NetBackup catalog recovery and symbolic links”](#) on page 148.

Symantec recommends that you recover the catalog images files in the following scenarios:

- The NetBackup relational database is valid, but NetBackup policy, backup image, or configuration files are lost or corrupt.
- You want to restore part of the NetBackup catalog before you restore the entire catalog. This procedure recovers only the catalog images and configuration files.  
 After you recover the image files, you can recover the relational database. See [“About recovering the NetBackup relational database”](#) on page 176.
- You recover the catalog using different storage devices. It may be to the same environment after storage hardware failure or replacement. It may be another site to which you replicate the catalog backups and the client backups. Regardless, the catalog backups and the client backups reside on different hardware.  
 This recovery does not overwrite the new storage device configuration with the old, no longer valid storage device information from the catalog backup.

## Catalog recovery and backup types

Recovery includes the catalog image files and configuration files that are in the catalog backups listed in the disaster recovery file, as follows:

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Full backup        | The image files and configuration files that are listed in the disaster recovery file are recovered.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Incremental backup | <p>Two recover scenarios exist, as follows:</p> <ul style="list-style-type: none"> <li>■ The catalog contains <i>no</i> information about the corresponding full backup and other incremental backups.<br/>           NetBackup restores only the backup image .<i>if</i> files, configuration files, and NetBackup policy files that are backed up in that incremental backup.<br/>           However, all of the catalog backup image .<i>if</i> files up to the last full catalog backup are restored. Therefore, you can restore the rest of the policy, image .<i>if</i> files, and configuration files by using the Backup, Archive and Restore interface.</li> <li>■ The catalog <i>contains</i> information about the corresponding full backup and other incremental backups.<br/>           NetBackup restores all of the backup image .<i>if</i> files and the configuration files that were included in the related set of catalog backups.</li> </ul> |

## Catalog image files

[Table 4-3](#) lists the files that comprise a partial catalog recovery.

**Table 4-3** Catalog image files

| UNIX and Linux                                 | Windows                                                 |
|------------------------------------------------|---------------------------------------------------------|
| /usr/opensv/netbackup/bp.conf                  | Not applicable                                          |
| /usr/opensv/netbackup/db/*                     | <i>install_path</i> \NetBackup\db\*                     |
| /usr/opensv/netbackup/db/class/*<br>(optional) | <i>install_path</i> \NetBackup\db\class\*<br>(optional) |
| /usr/opensv/netbackup/vault/<br>sessions*      | <i>install_path</i> \NetBackup\vault\sessions\*         |
| /usr/opensv/var/* (optional)                   | <i>install_path</i> \NetBackup\var\*<br>(optional)      |
| /usr/opensv/volmgr/database/*                  | <i>install_path</i> \Volmgr\database\*                  |
| /usr/opensv/volmgr/vm.conf                     | <i>install_path</i> \Volmgr\vm.conf                     |

## Recovery methods

You can use either of the following methods to recover the catalog image files:

- The **Catalog Recovery Wizard** in the **NetBackup Administration Console**. See [“Recovering the entire NetBackup catalog using the Catalog Recovery Wizard”](#) on page 153.
- The text-based recovery wizard. The `bprecover -wizard` command and option start the text-based recovery wizard. See [“Recovering the entire NetBackup catalog using bprecover -wizard”](#) on page 159.

## Recovering the NetBackup catalog image files using the Catalog Recovery Wizard

This procedure describes how to recover the NetBackup catalog image files by using the **Catalog Recovery Wizard**. The relational database transaction log is applied during image file recovery.

See [“About recovering the NetBackup catalog image files”](#) on page 163.

You must have root (administrative) privileges to perform this procedure.

You must be logged on to the master server on which you want to recover the catalog. The **Catalog Recovery Wizard** does not work after you perform a change server operation.

---

**Note:** This wizard relies on the disaster recovery file that was generated during the catalog backup. The path to the disaster recovery file is specified in the catalog backup policy.

---

---

**Note:** During the catalog recovery process, NetBackup may shutdown and restart services. If NetBackup is configured as a highly available application (cluster or global cluster), freeze the cluster before you begin the recovery process to prevent a failover. Then, unfreeze the cluster after the recovery process is complete.

---

---

**Warning:** Do not run any client backups before you recover the NetBackup catalog.

---

See “About recovering the NetBackup catalog image files” on page 163.

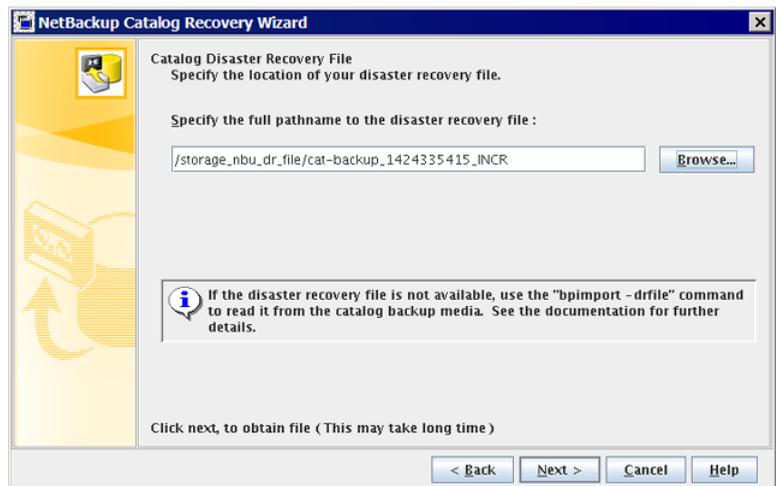
#### To recover the catalog image files using the Catalog Recovery Wizard

- 1 If NetBackup is not running, start all of the NetBackup services by entering the following:
  - On UNIX and Linux:  
`/usr/openv/netbackup/bin/bp.start_all`
  - On Windows:  
`install_path\NetBackup\bin\bpup`
- 2 If the catalog backup and the recovery devices are not available, do the following:
  - a Configure the necessary recovery device in NetBackup.  
  
For tape storage or **BasicDisk** storage, see the *NetBackup Administrator's Guide, Volume I*. For disk storage types, see the guide that describes the option. See the following website for NetBackup documentation:  
<http://www.symantec.com/docs/DOC5332>
  - b Make available to NetBackup the media that contains the catalog backup: Inventory the robot or the disk pool, add the media for standalone drives, configure the storage server and disk pool, or so on.  
  
For tape storage or **BasicDisk** storage, see the *NetBackup Administrator's Guide, Volume I*. For disk storage types, see the guide that describes the option. See the following website for NetBackup documentation:  
<http://www.symantec.com/docs/DOC5332>
  - c Create symbolic links to match those in the original environment.  
  
See “About NetBackup catalog recovery and symbolic links” on page 148.

- 3 In the **NetBackup Administration Console** window, click **NetBackup Management** in the left pane and then **Recover the catalogs** in the right pane. The **Catalog Recovery Wizard Welcome** panel appears.
- 4 Click **Next** on the **Welcome** panel to display the **Catalog Disaster Recovery File** panel.
- 5 On the **Catalog Disaster Recovery File** panel, specify where the disaster recovery file is stored. You can browse to select the file or enter the full pathname to the disaster recovery file.

In most cases, you specify the most recent disaster recovery information file available. If the most recent catalog backup is an incremental backup, use the disaster recovery file from the incremental backup. (There is no need to first restore the full backup and then follow with the incremental backup.)

If some form of corruption has occurred, you may want to restore to an earlier state of the catalog.



Click **Next** to continue. The **Retrieving Disaster Recovery File** panel appears.

- The wizard searches for the media that are required to recover the catalog, and **Retrieving Disaster Recovery File** panel informs you of the progress. It informs you if the necessary backup ID of the disaster recovery image is located. If the media is not located, the wizard lists which media is needed to update the database.

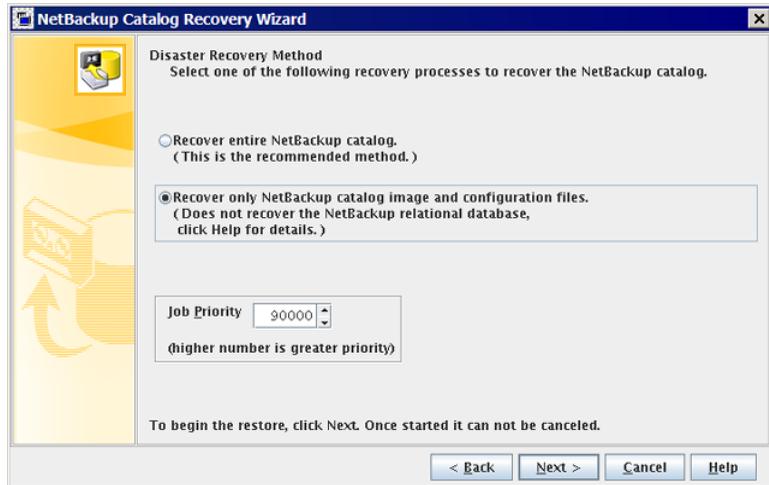


If necessary, follow the wizard instructions to insert the media that is indicated and run an inventory to update the NetBackup database. The information that is displayed on this panel depends on whether the recovery is from a full backup or an incremental backup.

When the required media sources are all found, click **Next** to display the **Disaster Recovery Method** panel.

The **Disaster Recovery Method** panel appears.

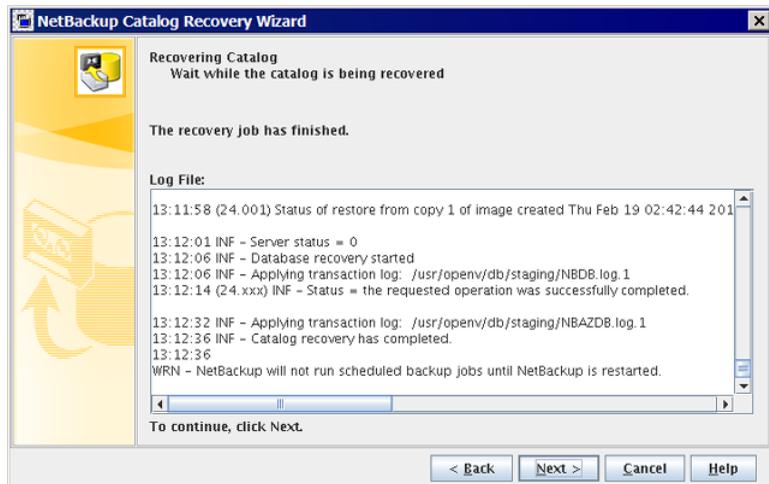
- On the **Disaster Recovery Method** panel, do the following:
  - Select **Recover only NetBackup catalog image and configuration files**.
  - Specify a job priority.



To continue, click **Next**.

The **Recovering Catalog** panel appears.

**8** The **Recovering Catalog** panel displays the recovery progress.



Your action depends on the outcome of the recovery, as follows:

- Not successful                      Consult the log file messages for an indication of the problem. Click **Cancel**, fix the problem, and then run the wizard again.
- Successful                              Click **Next** to continue to the final wizard panel.

9 On the final wizard panel, click **Finish**

When the recovery job is finished, each image file is restored to the proper image directory and the configuration files are restored.

10 Export the image metadata from the relational database in the staging directory, as follows:

```
cat_export -all -staging -source_master source-master-server-name
```

The export is required so that the image metadata can be imported into the relational database. A catalog image file recovery does not recover the relational database.

11 Import the image metadata into the relational database, as follows:

```
cat_import -all -replace_destination
```

12 If you recovered the catalog from a disk device, you may have to fix the disk media ID references in the image headers. The image headers were recovered from the catalog backup.

To fix the disk media IDs in the image headers, run the following command:

```
nbcatsync -backupid image_id -dryrun
```

Replace *image\_id* with the ID of the catalog backup. You can find the image ID of the catalog backup by examining the DR file.

13 Before you continue, be aware of the following points:

- If you recovered the catalog from removable media, NetBackup freezes the catalog media.  
See [“Unfreezing the NetBackup online catalog recovery media”](#) on page 191.
- Before you restart NetBackup, Symantec recommends that you freeze the media that contains the backups more recent than the date of the catalog from which you recovered.
- NetBackup does not run scheduled backup jobs until you stop and then restart NetBackup.  
You can submit backup jobs manually before you stop and restart NetBackup. However, if you do not freeze the media that contains the backups more recent than the date of the catalog from which you recovered, NetBackup may overwrite that media.
- Because this operation is a partial recovery, you must recover the relational database portion of the catalog.  
See [“About recovering the NetBackup relational database”](#) on page 176.

14 Stop and restart NetBackup on all the servers, as follows:

- On UNIX and Linux:

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

- On Windows:

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

15 If the catalog recovery is part of a server recovery procedure, complete the remaining steps in the appropriate recovery procedure.

Recovery can include the following:

- Importing the backups from the backup media into the catalog.
- Write protecting the media.
- Ejecting the media and setting it aside.
- Freezing the media.

## Recovering the NetBackup catalog image files using bprecover-wizard

You must have root (administrative) privileges to perform this procedure.

You must be logged on to the master server on which you want to recover the catalog. The **Catalog Recovery Wizard** does not work after you perform a change server operation.

---

**Note:** This wizard relies on the disaster recovery file that was generated during the catalog backup. The path to the disaster recovery file is specified in the catalog backup policy.

---

---

**Note:** During the catalog recovery process, services may be shut down and restarted. If NetBackup is configured as a highly available application (cluster or global cluster), freeze the cluster before starting the recovery process to prevent a failover. Then unfreeze the cluster after the recovery process is complete.

---

---

**Warning:** Do not run any client backups before you recover the NetBackup catalog.

---

See [“About recovering the NetBackup catalog image files”](#) on page 163.

**To recover the catalog image files using `bprecover -wizard`**

- 1 If recovering the catalog to a new NetBackup installation, such as at a disaster recovery site, do the following:
  - Install NetBackup.
  - Configure the devices that are required for the recovery.
  - Add the media that are required for the recovery to the devices.
  - Create symlinks to match those in the original environment.  
See [“About NetBackup catalog recovery and symbolic links”](#) on page 148.

- 2 If the EMM server is on a different host than the master server, start the NetBackup services on that host by entering the following command:

- On UNIX and Linux:  
`/usr/opensv/netbackup/bin/bp.start_all`

- On Windows:  
`install_path\NetBackup\bin\bpup`

- 3 Start the NetBackup services on the master server by entering the following command:

- On UNIX and Linux:  
`/usr/opensv/netbackup/bin/bp.start_all`

- On Windows:  
`install_path\NetBackup\bin\bpup`

- 4 Start the `bprecover wizard` by entering the following command:

```
bprecover -wizard
```

The following is displayed:

```
Welcome to the NetBackup Catalog Recovery Wizard!  
Please make sure the devices and media that contain catalog  
disaster recovery data are available  
Are you ready to continue?(Y/N)
```

- 5 Enter **Y** to continue. You are prompted to enter the full path name of the disaster recovery file, as follows:

```
Please specify the full pathname to the catalog disaster recovery  
file:
```

- 6 Enter the fully qualified path name to the disaster recovery file for the backup that you want to restore. For example:

```
/mnt/hdd2/netbackup/dr-file/Backup-Catalog_1318222845_FULL
```

If the most recent catalog backup was an incremental backup, use the disaster recovery file from the incremental backup. (There is no need to first restore the full backup and then follow with the incremental backup.) Alternately, you can recover from earlier version of the catalog.

If you specified a DR file for a full backup, a message similar to the following appears:

```
vm2.example.com_1318222845  
All media resources were located
```

```
Do you want to recover the entire NetBackup catalog? (Y/N)
```

If you specified a DR file for an incremental backup, a message similar to the following is displayed:

```
vm2.symantec.org_1318309224  
All media resources were located
```

The last catalog backup in the catalog disaster recovery file is an incremental.

If no catalog backup images exist in the catalog, a PARTIAL catalog recovery will only restore the NetBackup catalog files backed up in that incremental backup.

However, all of the catalog backup images up to the last full catalog backup are restored. Then you can restore the remaining NetBackup catalog files from the Backup, Archive, and Restore user interface. If catalog backup images already exist, all files that were included in the related set of catalog backups are restored.

```
Do you want to recover the entire NetBackup catalog? (Y/N)
```

- 7 Enter **N** to continue. The following is displayed:

A PARTIAL catalog recovery includes the images directory containing the dotf files and staging of the NetBackup relational database (NBDB) for further processing.

```
Do you also want to include policy data?(Y/N)
```

**8** Enter **Y** or **N** to continue. The following is displayed:

```
Do you also want to include licensing data?(Y/N)
```

**9** Enter **Y** or **N** to continue. The following is displayed:

```
Catalog recovery is in progress. Please wait...
```

```
Completed successful recovery of NBDB in staging directory on  
vm2.example.com
```

```
This portion of the catalog recovery has completed.  
Because this was a PARTIAL recovery of the NetBackup catalog,  
any remaining files included in the catalog backup can be restored  
using the Backup, Archive, and Restore user interface.
```

```
The image metadata that is stored in NBDB in the staging directory  
can be exported using "cat_export -staging", and, imported using  
"cat_import".
```

```
The "nbdb_unload -staging" command can be used to unload one or more  
database tables from NBDB in the staging directory.
```

```
The "nbdb_restore -recover -staging" command can be used to replace  
NBDB in the data directory with the contents from the staging  
directory.
```

```
WRN - NetBackup will not run scheduled backup jobs until NetBackup  
is restarted.
```

```
For more information, please review the log file:  
/usr/opensv/netbackup/logs/user_ops/root/logs/Recover1318357550.log
```

**10** When the recovery job is finished, each image file is restored to the proper image directory and the configuration files are restored. If you chose to recover the policy data and licensing data, it is restored also.**11** Export the image metadata from the relational database in the staging directory, as follows:

```
cat_export -all -staging -source_master source-master-server-name
```

The export is required so that the image metadata can be imported into the relational database. A catalog image file recovery does not recover the relational database.

- 12 Import the image metadata into the relational database, as follows:

```
cat_import -all -replace_destination
```

- 13 If you recovered the catalog from a disk device, you may have to fix the disk media ID references in the image headers. The image headers were recovered from the catalog backup.

See [“About NetBackup catalog recovery from disk devices”](#) on page 147.

To fix the disk media IDs in the image headers, run the following command:

```
nbcatsync -backupid image_id -prune_catalog
```

Replace *image\_id* with the ID of the catalog backup. The `bprecover` output contains the image ID of the catalog backup being restored. Alternatively, you can find the image ID of the catalog backup by examining the DR file.

- 14 Before you continue, be aware of the following points:

- If you recovered the catalog from removable media, NetBackup freezes the catalog media.  
See [“Unfreezing the NetBackup online catalog recovery media”](#) on page 191.
- Before you restart NetBackup, Symantec recommends that you freeze the media that contains the backups more recent than the date of the catalog from which you recovered.
- NetBackup does not run scheduled backup jobs until you stop and then restart NetBackup.  
You can submit backup jobs manually before you stop and restart NetBackup. However, if you do not freeze the media that contains the backups more recent than the date of the catalog from which you recovered, NetBackup may overwrite that media.
- Because this operation is a partial recovery, you must recover the relational database portion of the catalog.  
See [“About recovering the NetBackup relational database”](#) on page 176.

- 15 Stop and restart NetBackup on all the servers, as follows:

- On UNIX and Linux:

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

- On Windows:

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

**16** If the catalog recovery is part of a server recovery procedure, complete the remaining steps in the appropriate recovery procedure.

This procedure can include the following tasks:

- Importing the backups from the backup media into the catalog
- Write protecting the media
- Ejecting the media and setting it aside
- Freezing the media

## About recovering the NetBackup relational database

The NetBackup database (NBDB) is also known as the Enterprise Media Manager (EMM) database. It contains information about volumes and the robots and drives that are in NetBackup storage units. The NetBackup relational database also contains the NetBackup catalog images files. The images files contain the metadata that describes the backups.

You can recover the NetBackup relational databases independently of an entire catalog backup.

|                                    |                                                                                                    |
|------------------------------------|----------------------------------------------------------------------------------------------------|
| Recover from a backup              | See <a href="#">“Recovering NetBackup relational database files from a backup”</a> on page 176.    |
| Recover from the staging directory | See <a href="#">“Recovering the NetBackup relational database files from staging”</a> on page 180. |

## Recovering NetBackup relational database files from a backup

You can recover the NetBackup (NBDB) or Bare Metal Restore (BMRDB) relational database files from a backup. A valid database must exist before you can recover the catalog backup. Therefore, the steps that you follow to recover from a backup depend on the use case, as follows:

|                               |                                                                                                                                                                                                         |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The database is not corrupted | If the NBDB database is available and the SQL Anywhere server is running, you do not need to create a database. Do only step <a href="#">11</a> and step <a href="#">12</a> in the following procedure. |
| The database is corrupted     | Follow all of the steps in the procedure <i>only if</i> the NBDB database has been corrupted or does not exist. You must create a valid, empty database, which is included in the full procedure.       |

**To recover the NetBackup relational database files from a catalog backup**

- 1 If the NetBackup services are running, stop them as follows:

UNIX: `/usr/opensv/netbackup/bin/bp.kill_all`

Windows: `install_path\NetBackup\bin\bpdown`

- 2 Move the \*.db and \*.log files from the database file directories to a temporary directory. The following are the default locations for the database files:

UNIX: `/usr/opensv/db/data`

Windows: `C:\Program Files\Veritas\NetBackupDB\data`

- 3 Configure SQL Anywhere so that it does not try to start automatically when the host is started, as follows:

UNIX: `/usr/opensv/db/bin/nbdb_admin -auto_start NONE`

Windows: `install_path\NetBackup\bin\nbdb_admin -auto_start  
NONE`

- 4 Start the SQL Anywhere server, as follows:

UNIX: `/usr/opensv/netbackup/bin/nbdbms_start_stop start`

Windows: `install_path\NetBackup\bin\bpup -e SQLANYs_VERITAS_NB`

**5 Create the database. The command that you run depends on your scenario, as follows:**

**Normal scenario**                      **UNIX:** `/usr/opensv/db/bin/create_nbdb -drop`  
**Windows:** `install_path\NetBackup\bin\create_nbdb -drop`

**The database was relocated or the environment is clustered**                      **UNIX:** `/usr/opensv/db/bin/create_nbdb -data VXDBMS_NB_DATA -drop -staging VXDBMS_NB_STAGING`  
**Windows:** `install_path\NetBackup\bin\create_nbdb -data VXDBMS_NB_DATA -drop -staging VXDBMS_NB_STAGING`

**Obtain the values for `VXDBMS_NB_DATA` and `VXDBMS_NB_STAGING` from the `vxdbms.conf` file in the temporary directory that you created in step 2.**

**The database was relocated or the environment is clustered, and space constraints force you to create this temporary database in the final location**                      **UNIX:** `/usr/opensv/db/bin/create_nbdb -drop -data VXDBMS_NB_DATA -index VXDBMS_NB_INDEX -tlog VXDBMS_NB_TLOG -staging VXDBMS_NB_STAGING`  
**Windows:** `install_path\NetBackup\bin\create_nbdb -drop -data VXDBMS_NB_DATA -index VXDBMS_NB_INDEX -tlog VXDBMS_NB_TLOG -staging VXDBMS_NB_STAGING`

**Obtain the values for the option arguments from the `vxdbms.conf` file in the temporary directory that you created in step 2.**

**6 Start the NetBackup services, as follows:**

**UNIX:**                      `/usr/opensv/netbackup/bin/bp.start_all`

**Windows:**                      `install_path\NetBackup\bin\bpup`

**7 Load the default device protocols and settings into the NetBackup Enterprise Media Manager (EMM) database by running the following command:**

**UNIX:**                      `/usr/opensv/volmgr/bin/tpext -loadEMM`

**Windows:**                      `install_path\Volmgr\bin\tpext -loadEMM`

- 8 If you used the `nbdb_move` command to relocate the NetBackup database files, re-create the directories where the files were located when you backed up the catalog. The following are the default locations into which the `nbdb_move` command moves the database files:

UNIX: `/usr/opensv/db/data`

Windows: `install_path\NetBackupDB\data`

- 9 Start the NetBackup device manager on the NetBackup master server, as follows:

UNIX: `/usr/opensv/volmgr/bin/ltid -v`

Windows: Use Windows Computer Management to start the NetBackup Device Manager service (`ltid.exe`).

- 10 If the catalog backup and the recovery devices are not available, do the following:

- a Configure the necessary recovery device in NetBackup.

For tape storage or **BasicDisk** storage, see the *NetBackup Administrator's Guide, Volume 1*. For disk storage types, see the guide that describes the option. See the following website for NetBackup documentation:

<http://www.symantec.com/docs/DOC5332>

- b Make available to NetBackup the media that contains the catalog backup: Inventory the robot or the disk pool, add the media for standalone drives, configure the storage server and disk pool, or so on.

For tape storage or **BasicDisk** storage, see the *NetBackup Administrator's Guide, Volume 1*. For disk storage types, see the guide that describes the option. See the following website for NetBackup documentation:

<http://www.symantec.com/docs/DOC5332>

- c Import the catalog backup from the media on which it resides.

See the *NetBackup Administrator's Guide, Volume 1*:

<http://www.symantec.com/docs/DOC5332>

**11 Recover the catalog by running the following command on the master server:**

UNIX: `/usr/opensv/netbackup/bin/admincmd/bprecover -r -nbdb`

Windows: `install_path\NetBackup\bin\admincmd\bprecover -r -nbdb`

**12 Stop and restart NetBackup, as follows:**

UNIX: `/usr/opensv/netbackup/bin/bp.kill_all`  
`/usr/opensv/netbackup/bin/bp.start_all`

Windows: `install_path\NetBackup\bin\bpdown`  
`install_path\NetBackup\bin\bpup`

## Recovering the NetBackup relational database files from staging

During a catalog backup, NetBackup copies the relational database files to the staging directory. The recovery option that restores the image files and the configuration files also restores the relational database files to the staging directory.

See [“About recovering the NetBackup catalog image files”](#) on page 163.

You can recover the NetBackup NBDB relational database files from the staging directory. You can also use NetBackup commands process the NBDB relational database files further.

See [“About processing the relational database in staging”](#) on page 183.

When the relational database is recovered from staging, NetBackup also applies the current online transaction log during the recovery. Applying the transaction log ensures that the database is as consistent as possible with the current `db/images` directory.

Two recovery procedures from the staging directory exist, as follow:

The database is not corrupted      See [“To recover relational database files from staging if the database is corrupted”](#) on page 181.

The database is corrupted      See [“To recover relational database files from staging if the database is corrupted”](#) on page 181.

**To recover relational database files from staging if the database is not corrupted**

- 1 Run the following command on the master server to recover NBDB from staging:

UNIX: `/usr/opensv/netbackup/bin/nbdb_restore -dbn NBDB -recover -staging`

Windows: `install_path\NetBackup\bin\nbdb_restore -dbn NBDB -recover -staging`

- 2 Stop and restart NetBackup, as follows:

UNIX:

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

Windows:

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

**To recover relational database files from staging if the database is corrupted**

- 1 If the NetBackup services are running, stop them as follows:

UNIX: `/usr/opensv/netbackup/bin/bp.kill_all`

Windows: `install_path\NetBackup\bin\bpdown`

- 2 Move the \*.db and \*.log files from the following database file directories to a temporary directory:

UNIX: `/usr/opensv/db/data`

Windows: `C:\Program Files\Veritas\NetBackupDB\data`

- 3 Configure SQL Anywhere so that it does not try to start automatically when the host is started, as follows:

Linux: `/usr/opensv/db/bin/nbdb_admin -auto_start NONE`

Windows: `install_path\NetBackup\bin\nbdb_admin -auto_start NONE`

- 4 Start the SQL Anywhere server, as follows:

UNIX: `/usr/opensv/netbackup/bin/nbdbms_start_stop start`

Windows: `install_path\NetBackup\bin\bpup -e SQLANYs_VERITAS_NB`

- 5 Create an empty database, as follows:

UNIX: `/usr/opensv/db/bin/create_nbdb -drop`

Windows: `install_path\NetBackup\bin\create_nbdb -drop`

**6 Stop and restart NetBackup, as follows:****UNIX and Linux:**

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

**Windows:**

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

**7 Run the NetBackup `tpext` command to update the device mapping files, as follows:****UNIX:** `/usr/opensv/volmgr/bin/tpext -loadEMM`**Windows:** `install_path\Volmgr\bin\tpext -loadEMM`**8 If you used the `nbdb_move` command to relocate NetBackup database files, re-create the directories where the files were located when you backed up the catalog.****9 Start the NetBackup Device Manager, as follows:****UNIX:** `/usr/opensv/volmgr/bin/ltid -v`**Windows:** Start the device manager service.**10 Run the following command on the master server to recover NBDB from staging:****UNIX:** `/usr/opensv/netbackup/bin/nbdb_restore -dbn NBDB -recover -staging`**Windows:** `install_path\NetBackup\bin\nbdb_restore -dbn NBDB -recover -staging`**11 Stop and restart NetBackup, as follows:****UNIX:**

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

**Windows:**

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

## About processing the relational database in staging

A recovery of the NetBackup image files and configuration files also restores the NetBackup relational database (NBDB) to the staging directory. You can use the following NetBackup commands to further process the NBDB database if required:

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>cat_import</code>                | Use <code>cat_import</code> to import the image metadata that is in the legacy flat file format into an NBDB relational database. The NBDB database can be the actual production DB or an NBDB in a different NetBackup domain.                                                                                                                                                                                                                                                                     |
| <code>cat_export</code>                | Use <code>cat_export -staging</code> to extract the image metadata from the relational database. It writes the data to the <code>db.export</code> directory in the legacy flat file format. You can export all of the image metadata or a subset of the image metadata by client or backup ID. Then, you can use the <code>cat_import</code> command to insert the data into another NBDB database. <i>Another NBDB</i> can be the actual production DB or an NBDB in a different NetBackup domain. |
| <code>nbdb_restore<br/>-staging</code> | Use <code>nbdb_restore -staging</code> to recover the relational database from the staging directory.<br><br>See <a href="#">"Recovering the NetBackup relational database files from staging"</a> on page 180.                                                                                                                                                                                                                                                                                     |
| <code>nbdb_unload -staging</code>      | Use <code>nbdb_unload -staging</code> to unload the media table and related tables to a set of flat files. Then, you can use SQL tools to insert the subset of data into another NBDB. <i>Another NBDB</i> can be the actual production DB or an NBDB in a different NetBackup domain.                                                                                                                                                                                                              |

---

**Warning:** Symantec recommends that you manipulate or process the NetBackup relational database *only* when directed to do so by a Symantec Support Representative. For help with NetBackup domain merges and splits, contact the Symantec Information Management Consulting Services:

[http://www.symantec.com/business/services/consulting\\_services.jsp](http://www.symantec.com/business/services/consulting_services.jsp)

---

More information about the commands is available.

See the *NetBackup Commands Reference Guide*:

<http://www.symantec.com/docs/DOC5332>

## Recovering the NetBackup catalog when NetBackup Access Control is configured

If you have configured NetBackup Access Control (NBAC), the online, hot catalog backup automatically backs up your authentication information and authorization configuration information.

Both the Operate and Configure permission sets are required on the catalog object to successfully back up and recover NBAC authentication and authorization data.

Separate recovery procedures exist based on operating system, as follows:

- UNIX: [Table 4-4](#)
- Windows: [Table 4-5](#)

**Table 4-4** To recover the NetBackup catalog on UNIX when NetBackup Access Control is configured

| Step   | Task                                                                                                                                  | Procedure                                                                                                                                        |
|--------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | If recovering to a master server on which NBAC is configured and operational, disable NBAC (that is, set it to PROHIBITED mode).      | See the <i>NetBackup Security and Encryption Guide</i> : <a href="http://www.symantec.com/docs/DOC5332">http://www.symantec.com/docs/DOC5332</a> |
| Step 2 | Recover the NetBackup catalog from the online catalog backup using the Catalog Recovery Wizard or the <code>bprecover</code> command. | See “About recovering the entire NetBackup catalog” on page 152.                                                                                 |
| Step 3 | Configure NetBackup to use NBAC by setting it to AUTOMATIC or REQUIRED as per the security level desired.                             | See the <i>NetBackup Security and Encryption Guide</i> : <a href="http://www.symantec.com/docs/DOC5332">http://www.symantec.com/docs/DOC5332</a> |
| Step 4 | Restart NetBackup.                                                                                                                    | <code>/usr/opensv/netbackup/bin/bp.kill_all</code><br><code>/usr/opensv/netbackup/bin/bp.start_all</code>                                        |

**Table 4-5** To recover the NetBackup catalog on Windows when NetBackup Access Control is configured

| Step   | Task                                                                                                                             | Procedure                                                                                                                                        |
|--------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | If recovering to a master server on which NBAC is configured and operational, disable NBAC (that is, set it to PROHIBITED mode). | See the <i>NetBackup Security and Encryption Guide</i> : <a href="http://www.symantec.com/docs/DOC5332">http://www.symantec.com/docs/DOC5332</a> |
| Step 2 | Stop the NetBackup services.                                                                                                     | <code>install_path\Veritas\NetBackup\bin\bpdown.exe</code>                                                                                       |

**Table 4-5** To recover the NetBackup catalog on Windows when NetBackup Access Control is configured (*continued*)

| Step   | Task                                                                                                                                  | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | In Windows, change the startup type of the NetBackup Authentication Service and NetBackup Authorization Service to Disabled.          | Instructions for configuring Microsoft Windows are beyond the scope of the NetBackup documentation. Refer to the appropriate Microsoft documentation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 4 | Start the NetBackup services.                                                                                                         | <code>install_path\Veritas\NetBackup\bin\bpup.exe</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 5 | Recover the NetBackup catalog from the online catalog backup using the Catalog Recovery Wizard or the <code>bprecover</code> command. | See <a href="#">“About recovering the entire NetBackup catalog”</a> on page 152.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 6 | In Windows, change the startup type of the NetBackup Authentication Service and NetBackup Authorization Service to Automatic.         | Instructions for configuring Microsoft Windows are beyond the scope of the NetBackup documentation. Refer to the appropriate Microsoft documentation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 7 | Configure NetBackup to use NBAC.                                                                                                      | <p>The procedure depends on the environment, as follows:</p> <ul style="list-style-type: none"> <li>■ For a NetBackup master server in a Windows Server Failover Clustering environment, run the following command on the NetBackup master server on the active node:<br/> <code>bpnbaz -setupmaster</code><br/>                     This command provisions the Windows registry on all nodes with the required entries for NBAC.</li> <li>■ For recovery to a new installation, run the following command on the NetBackup master server:<br/> <code>bpnbaz -setupmaster</code></li> <li>■ For recovery in an existing environment, set NBAC to AUTOMATIC or REQUIRED as per the security level desired.</li> </ul> <p>See the <i>NetBackup Security and Encryption Guide</i>:<br/> <a href="http://www.symantec.com/docs/DOC5332">http://www.symantec.com/docs/DOC5332</a></p> |
| Step 8 | Restart NetBackup.                                                                                                                    | <code>install_path\Veritas\NetBackup\bin\bpdown.exe</code><br><code>install_path\Veritas\NetBackup\bin\bpup.exe</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

See [“About recovering the NetBackup catalog”](#) on page 146.

## Recovering the NetBackup catalog from a nonprimary copy of a catalog backup

By default, catalog backup can have multiple copies, and the catalog is recovered from the primary backup copy. The primary copy is the first or the original copy. However, you can recover from a copy other than the primary.

---

**Note:** You must be logged on to the master server on which you want to recover the catalog. You cannot change server while running the **NetBackup Administration Console** on a different host and then run the wizard.

---

---

**Note:** You must have root (administrative) privileges to perform these procedures.

---

### To recover the catalog from a non-primary copy

- 1 If the copy of the catalog backup is on a medium other than tape, do the following:

**BasicDisk** Make sure that the disk that contains the backup is mounted against the correct mount path (as displayed in the disaster recovery file).

Disk pool For a catalog backup file in a disk pool, do the following:

- Create the disk storage server for the storage by using the **Storage Server Configuration Wizard**.
- Create the disk pool for the storage by using the **Disk Pool Configuration Wizard**.
- Run the following command to synchronize the disaster recovery file to the new disk pool.

```
nbcatsync -sync_dr_file disaster_recovery_file
```

- 2 Run the following NetBackup command to recover the catalog:

```
bprecover -wizard -copy N
```

*N* is the number of the copy from which you want to recover.

## Recovering the NetBackup catalog without the disaster recovery file

If the disaster recovery file has been lost, consult the email that was sent to the administrator when the catalog was backed up. The disaster recovery file is written to the location you specify in the catalog backup policy and is appended to the backup stream itself.

**To recover the catalog without the disaster recovery file**

- 1 The email identifies the media that contains the disaster recovery file, and the media that was used to back up critical policies. Ensure that this media is available.
- 2 Follow the normal catalog recovery steps until the point where the **Catalog Recovery Wizard** or `bprecover` command is called for.
- 3 Run the following command to retrieve all disaster recovery files from the catalog backup media:

```
bpimport -drfile -id media_id -drfile_dest  
fully_qualified_dir_name
```

This command recovers all disaster recovery files from the specified media ID and places them in the specified directory. The ID can be either a tape media ID or the fully qualified location of a disk storage unit.

- 4 Verify that the correct disaster recovery file is available in the specified directory and that it is available from the NetBackup master server.
- 5 Continue with the normal catalog recovery procedure by running the **Catalog Recovery Wizard** or `bprecover` command, providing the disaster recovery file location when prompted.

Refer to the email as your primary source for recovery instructions, because they are the most current instructions for recovering your catalog. The instructions are sent when the catalog backup is completed, or when a catalog backup image is duplicated.

---

**Note:** If you restore catalog files directly by using `bprestore` on a Solaris system, use the following path: `/opt/openssl/netbackup/bin/bprestore`.

---

The name of the online catalog backup policy is **CatalogBackup**. The email is written to the following file:

```
/storage/DR/CatalogBackup_1123605764_FULLL.
```

The file name itself indicates if the backup was full or not.

See [“NetBackup disaster recovery email example”](#) on page 149.

## Recovering a NetBackup user-directed online catalog backup from the command line

This procedure recovers the catalog manually through the command line interface (CLI) without a Phase 1 import when the disaster recovery (DR) file is available. You must have root (administrative) privileges to perform this procedure.

---

**Note:** Use this procedure only if you want to restore the minimal NetBackup catalog information that lets you begin to recover critical data.

---

### To recover the user-directed online catalog from the command line interface

- 1 Verify the location of the disaster recovery files that are created from Full and Incremental Hot Catalog backups. These files can be stored in a specified path of the file system on the master server and in email attachments to the NetBackup administrator.
- 2 Set up each master server and media server in the same configuration as the configuration that is used during the last catalog backup. The master server and media servers have the following same properties as the backed up catalog configuration: name, NetBackup version, operating system patch level, and path to storage devices.

Configure any devices and volumes you may need for the recovery.

- 3 Locate the latest DR image file corresponding to the backups that are used for recovery. Open the file in an editor and find values for the following:

|                            |                                                                                                                 |
|----------------------------|-----------------------------------------------------------------------------------------------------------------|
| <code>master_server</code> | Use the exact name that is specified in NetBackup configuration for the master server .                         |
| <code>media_server</code>  | The location of the robot or disk storage unit that is used for catalog backup.                                 |
| <code>timestamp</code>     | The four most significant digits in the DR file name and six zeroes attached.                                   |
| <code>media</code>         | The location of the catalog backup media as specified by the disaster recovery file under the FRAGMENT keyword. |
| <code>backup_id</code>     | Found in the DR file under BACKUP_ID.                                                                           |

Example:

file: Hot\_Backup\_1122502016\_INCR

timestamp: 1122000000

#### 4 Create the DR recovery directory on the master server.

UNIX and Linux:

```
/usr/opensv/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 -assignto host media timestamp master_server
```

Example:

```
vmquery -assignto host DL005L 1122000000 klingon
```

#### 7 To recover the catalog .f file from the hot catalog backup, run a Phase II import on the media that is specified by the disaster recovery file .

```
bpimport -server master_server -backupid backup_id
```

#### 8 If your catalog backup was incremental, recover all the other catalog backup images up to and including the most recent Full Catalog backup.

- Open the Backup, Archive, and Restore client interface for NetBackup. Select NBU-Catalog as the policy type. Set the source clients and destination clients to your master server.
- Search the backups and restore all files that are located in the following directory:

```
install_path/netbackup/db/images/master_server
```

- Verify that all files are restored successfully on the master server.

- 9 Restore your critical data by using the Backup, Archive, and Restore client interface or the command line.
  - Restore the catalog backup images for each media server which requires data recovery.
  - To restore the backup images, select NBU-Catalog as the policy type. Source and destination clients should be your master server. Refresh your view in the BAR GUI. Traverse the file system for the master server to the following:

```
install_path/netbackup/db/images
```

Restore the images for each configured media server. Verify that your images are present by searching for them in the catalog.

- 10 Recover backup data from each media server in the previous step. Change the Policy Type, Source, and Destination client to match the client that is used to back up the desired data. Select the desired files from the Backup, Archive, and Restore client interface and restore them.
- 11 To recover the NetBackup relational database, run the following:

```
bprecover -r -nbdb
```

This command restores NetBackup media usage information, ensure that media containing backups are not overwritten, and restore the storage unit configuration.

You cannot recover the NetBackup relational database to a configuration that is not identical to the configuration on which the catalog was backed up. Instead, you must import each piece of backup media.

- 12 If your catalog recovery media is on tape, freeze the media that contains the catalog backup that is used for recovery. This action protects the media from being reused:

```
bpmmedia -freeze -m media -h master_server
```

Run `bpmmedialist` to verify that the media is frozen.

- 13 Recover your policies and configuration data on each master server and media server.

Before recovering NetBackup policy files, ensure that you have recovered all of your critical data, or protected the media that contains your critical data. When policy information is recovered, NetBackup starts to run the scheduled jobs that may overwrite the media that was written after the last catalog backup.

Open the Backup, Archive, and Restore client interface for NetBackup and select NBU-Catalog as the policy type.

For each server to be restored, set the source clients and destination clients to your server, starting with the master server.

Restore all files that are backed up by the hot catalog backup on each server.

- 14 Stop and restart the NetBackup services.

## Restoring files from a NetBackup online catalog backup

Because the online catalog backup uses the standard backup format, you may recover specific files using the NetBackup Backup, Archive, and Restore user interface. Restoring catalog files directly to their original location may cause inconsistencies in the NetBackup catalog or cause NetBackup to fail. Instead, you should restore catalog files to an alternate location.

### To restore files from an online catalog backup

- 1 From the **Specify NetBackup Machines and Policy Type** menu, select the **NBU-Catalog** policy type.
- 2 Specify the master server as the source client for the restore.
- 3 Select the catalog files to restore.

## Unfreezing the NetBackup online catalog recovery media

This procedure describes how to unfreeze your removable catalog recovery media.

See [“About recovering the NetBackup catalog”](#) on page 146.

### To unfreeze the online catalog recovery media

- 1 On the master server, for each removable media that is identified in the disaster recovery file or email, run the following command:

```
bpimport -create_db_info -server server_name -id media_id
```

- 2 On the master server, run the following command:

```
bpimport
```

- 3 On the master server, for each media that is identified in the disaster recovery file or email, run the following command:

```
bpmedia -unfreeze -m media_id -h server_name
```

# Index

## A

- acstest 118
- AdvancedDisk 124, 133
- Alternate client restores
  - host.xlate file 52
- archiving
  - for NBCC 107
  - for nbsu 102
- Auth User
  - for PBX 73
- auto-configuration problems 30

## B

- Bare Metal Restore 122, 125, 140
- bp.conf
  - SERVER entries 89
- bp.kill\_all 75–76
- bp.start\_all 76
- bpdown command 75–76, 136, 139
- bpps 23
- bpup command 76
- bundling
  - NBCC output 107
  - nbsu output 102

## C

- catalog recovery
  - catalog image files 163
  - clustered master server 163
- client
  - NetBackup
    - configured name 50
    - installation problems 28
    - multiple hostnames 49
    - peername 49
    - testing configuration 34, 37
- Client Properties dialog 64
- client, NetBackup
  - Windows disk recovery 140

- communications problems
  - PC clients 45
  - UNIX clients 41
- compression
  - for NBCC 107
  - for nbsu 102
- configuration problems 28

## D

- debug logs
  - analysis utilities 93
- debugging
  - NBCC 106
  - nbsu 99
- device configuration problems 30
- Device Configuration Wizard 135
- disaster recovery
  - preparing for disaster 120
- disk full 65
- disk recovery
  - Windows client 140
- duplex mode and performance 88

## E

- E-mail 123

## F

- full disk 65
- full duplex mode 88

## H

- Half duplex and poor performance 88
- host name entries
  - checking 53
- Host Properties 64
- host.xlate file 52

**I**

- ifconfig
  - for checking NIC duplex mode 88
- inetd 28
- Information E-mail 123
- installation
  - Linux 28
- installation problems 27
- ipconfig
  - for checking NIC duplex mode 88

**J**

- jobs
  - queued for long periods 65

**L**

- Linux 28
- log analysis utilities
  - debug logs 93
  - limitations 96
  - output format 97

**M**

- master server
  - test procedure 34, 37
- media server
  - test procedure 37

**N**

- NB\_dbsrv daemon 65
- NBCC
  - archiving and compression 107
  - does the following 105
  - introduction 105
  - location of 105
  - nbcc-info.txt file 106
  - Notes on running 105
  - output 106
  - progress display 107
  - troubleshooting 106
  - when to use 105
- nbcc-info.txt file 106
- nbdb\_move 135
- nbemm 23
- nbftclnt
  - and bp.conf 89
- nbjm 23
- nbpem 23
- nbrb 23, 65
- nbsu
  - and status codes 103
  - archiving and compression 102
  - bundling 102
  - creating xml output file 103
  - introduction 99
  - location of 99
  - nbsu\_info.txt file 100
  - output files 100
  - progress display 104
  - troubleshooting 99
  - when to use 99
- nbsu\_info.txt file 100
- NetBackup
  - if unresponsive 65
- NetBackup Authentication service
  - start and stop 25
- NetBackup Client Service
  - start and stop 25–26
- NetBackup CloudStore Service Container service
  - start and stop 25
- NetBackup Compatibility service
  - start and stop 25
- NetBackup consistency check
  - see NBCC 105
- NetBackup Database Manager service
  - start and stop 25
- NetBackup Deduplication Engine service
  - start and stop 26
- NetBackup Deduplication Manager service
  - start and stop 26
- NetBackup Device Manager service
  - start and stop 26
- NetBackup Discovery Framework service
  - start and stop 25
- NetBackup Enterprise Media Manager service
  - start and stop 25
- NetBackup Event Manager service
  - start and stop 25
- NetBackup Indexing Manager service
  - start and stop 25
- NetBackup Job Manager service
  - start and stop 25
- NetBackup Legacy Client Service
  - start and stop 26
- NetBackup Policy Execution Manager service
  - start and stop 25

- NetBackup Relational Database Manager 65
- NetBackup Relational Database Manager Service
  - start and stop 25
- NetBackup Remote Manager and Monitor Service
  - start and stop 25–26
- NetBackup Request Daemon service
  - start and stop 25
- NetBackup Resource Broker service
  - start and stop 25
- NetBackup Service Layer service
  - start and stop 25
- NetBackup Service Monitor service
  - start and stop 25
- NetBackup Storage Lifecycle Manager service
  - start and stop 25
- NetBackup Support Utility
  - see nbsu 99
- NetBackup Vault Manager service
  - start and stop 25
- NetBackup Volume Manager service
  - start and stop 25–26
- NetBackupDeduplication Multi-Threaded Agent service
  - start and stop 26
- network connections
  - multiple 49
- network interface cards 88
- network problems
  - PC clients 45
  - UNIX clients 41
- NIC cards and full duplex 88

## O

- odltest 117
- OpenStorage 124, 133

## P

- patches (installing during recovery) 141
- PBX
  - Auth User 73
  - logging 73
  - Secure Mode 73–74
  - starting 72
  - starting/stopping 75
  - troubleshooting 70
- pbx\_exchange 72
- pbxcfg 72
- preliminary troubleshooting procedure 20
- Private Branch Exchange (PBX) 70

- Private Branch Exchange service
  - start and stop 25–26
- procedures
  - recovery
    - Windows client disk 140
  - troubleshooting
    - communications problems 41, 45
    - host names and services 53
    - installation and configuration 27
    - introduction 18
    - master server and clients 34
    - media server and clients 37
    - preliminary 20

## Q

- queued jobs 65

## R

- recording information 12
- recovery procedures
  - Windows client disk 140
- RedHat 28
- relational database 65
- robotic test utility 116
  - acstest 118
  - odltest 117
  - tl4test 117–118
  - tl8test 117–118
  - tlctest 117–118
  - tlhtest 118
  - tshtest 117
- robtest 117–118

## S

- SAN client
  - and bp.conf 89
- Secure Mode
  - for PBX 73
- server
  - installation problems 27
  - test procedure for master 34, 37
  - test procedure for media server 37
- SERVER entries
  - bp.conf 89
- services entries
  - checking 53
- SharedDisk 124, 133
- slow performance and NIC cards 88

- starting NetBackup processes 76
- status codes
  - and nbsu 103
- stopping NetBackup processes 75–76
- storage units 89
- SuSE 28

## T

- test utility
  - robotic 116
- tl4test 117–118
- tl8test 117–118
- tlctest 117–118
- tlhtest 118
- tpautoconf 128
- traceroute 52
- tracert 52
- troubleshooting procedure
  - communication problems
    - PC clients 45
    - UNIX clients 41
  - general
    - master server and clients 34, 37
    - media server and clients 37
  - host name and services entries 53
  - installation 27
  - preliminary 20
- tshtest 117

## U

- unavailable 89
- utility
  - robotic test 116

## V

- Volume Configuration Wizard 135
- vxpbx\_exchanged 75

## X

- xinetd 28
- xml
  - for nbsu 103