Veritas NetBackup™ Troubleshooting Guide

UNIX, Windows, and Linux

Release 8.3
Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)  CustomerCare@veritas.com
Japan  CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

NB.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

## Contents

### Chapter 1 Introduction
- NetBackup logging and status code information ........................................ 9
- Troubleshooting a problem ........................................................................... 9
- Problem report for Technical Support .......................................................... 12
- About gathering information for NetBackup-Java applications ..................... 13

### Chapter 2 Troubleshooting procedures
- 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 ................. 25
- Troubleshooting installation problems ...................................................... 28
- Troubleshooting configuration problems ............................................... 29
- Device configuration problem resolution .................................................. 31
- Testing the master server and clients ....................................................... 34
- Testing the media server and clients ......................................................... 38
- Resolving network communication problems with UNIX clients .............. 41
- Resolving network communication problems with Windows clients ......... 46
- Troubleshooting vnetd proxy connections ............................................... 50
  - vnetd proxy connection requirements .................................................. 50
  - Where to begin to troubleshoot vnetd proxy connections ...................... 52
- Verify that the vnetd process and proxies are active .................................. 52
- Verify that the host connections are proxied .......................................... 53
- Test the vnetd proxy connections ............................................................ 53
- Examine the log files of the connecting and accepting processes .............. 56
  - Viewing the vnetd proxy log files ....................................................... 56
- Troubleshooting security certificate revocation ......................................... 57
  - Troubleshooting cloud provider’s revoked SSL certificate issues .......... 58
  - Troubleshooting cloud provider’s CRL download issues ....................... 59
  - How a host’s CRL affects certificate revocation troubleshooting ............ 59
Chapter 4  Disaster recovery ................................. 186
   About disaster recovery ........................................ 187
   About disaster recovery requirements ...................... 188
   Disaster recovery packages ........................................ 189
   About disaster recovery settings ........................... 189
   Recommended backup practices .................................. 190
   About disk recovery procedures for UNIX and Linux ........ 193
      About recovering the master server disk for UNIX and Linux 193
      About recovering the NetBackup media server disk for UNIX 199
      Recovering the system disk on a UNIX client workstation 199
   About clustered NetBackup server recovery for UNIX and Linux 200
      Replacing a failed node on a UNIX or Linux cluster .... 200
      Recovering the entire UNIX or Linux cluster .......... 202
   About disk recovery procedures for Windows .................. 203
      About recovering the master server disk for Windows .... 204
      About recovering the NetBackup media server disk for Windows 210
          Recovering a Windows client disk .......................... 210
   About clustered NetBackup server recovery for Windows ...... 213
      Replacing a failed node on a Windows VCS cluster .... 213
      Recovering the shared disk on a Windows VCS cluster 214
      Recovering the entire Windows VCS cluster ........ 215
   Generating a certificate on a clustered master server after disaster recovery installation ........................................ 217
   About restoring disaster recovery package .................... 218
   About the DR_PKG_MARKER_FILE environment variable ...... 218
   Restoring disaster recovery package on Windows ............... 219
   Restoring disaster recovery package on UNIX ................. 222
   About recovering the NetBackup catalog ...................... 225
      About NetBackup catalog recovery on Windows computers 227
      About NetBackup catalog recovery from disk devices .... 227
      About NetBackup catalog recovery and symbolic links .... 228
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About NetBackup catalog recovery and OpsCenter</td>
<td>228</td>
</tr>
<tr>
<td>NetBackup disaster recovery email example</td>
<td>229</td>
</tr>
<tr>
<td>About recovering the entire NetBackup catalog</td>
<td>233</td>
</tr>
<tr>
<td>Establishing a connection with NAT media server before catalog</td>
<td>246</td>
</tr>
<tr>
<td>recovery</td>
<td></td>
</tr>
<tr>
<td>About recovering the NetBackup catalog image files</td>
<td>247</td>
</tr>
<tr>
<td>About recovering the NetBackup relational database</td>
<td>262</td>
</tr>
<tr>
<td>Recovering the NetBackup catalog when NetBackup Access</td>
<td>272</td>
</tr>
<tr>
<td>Control is configured</td>
<td></td>
</tr>
<tr>
<td>Recovering the NetBackup catalog from a nonprimary copy of a</td>
<td>274</td>
</tr>
<tr>
<td>catalog backup</td>
<td></td>
</tr>
<tr>
<td>Recovering the NetBackup catalog without the disaster recovery file</td>
<td>274</td>
</tr>
<tr>
<td>Recovering a NetBackup user-directed online catalog backup from the</td>
<td>276</td>
</tr>
<tr>
<td>command line</td>
<td></td>
</tr>
<tr>
<td>Restoring files from a NetBackup online catalog backup</td>
<td>280</td>
</tr>
<tr>
<td>Unfreezing the NetBackup online catalog recovery media</td>
<td>280</td>
</tr>
<tr>
<td>Steps to carry out when you see exit status 5988 during catalog</td>
<td>281</td>
</tr>
<tr>
<td>recovery</td>
<td></td>
</tr>
</tbody>
</table>

**Index**                                                                 | 285  |
Introduction

This chapter includes the following topics:

- NetBackup logging and status code information
- Troubleshooting a problem
- Problem report for Technical Support
- About gathering information for NetBackup-Java applications

NetBackup logging and status code information

The following material has been moved 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, available here:
http://www.veritas.com/docs/DOC5332

For descriptions and recommended actions for 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.
### Steps for troubleshooting NetBackup problems

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Remember the error message</td>
<td>Error messages are usually the vehicle for telling you something went wrong. If you don’t see an error message in an interface, but still suspect a problem, check the reports and logs. NetBackup provides extensive reporting and logging facilities. These can provide an error message that points you directly to a solution. The logs also show you what went right and the NetBackup operation that was ongoing when the problem occurred. For example, a restore operation needs media to be mounted, but the required media is currently in use for another backup. Logs and reports are essential troubleshooting tools. See the NetBackup Logging Reference Guide.</td>
</tr>
</tbody>
</table>
| Step 2 | Identify what you were doing when the problem occurred | Ask the following questions:  
- What operation was tried?  
- What method did you use?  
  - For example, more than one way exists to install software on a client.  
  - Also more than one possible interface exists to use for many operations. Some operations can be performed with a script.  
- What type of server platform and operating system was involved?  
- If your site uses both the master server and the media server, was it a master server or a media server?  
- If a client was involved, what type of client was it?  
- Have you performed the operation successfully in the past? If so, what is different now?  
- What is the service pack level?  
- Do you use operating system software with the latest fixes supplied, especially those required for use with NetBackup?  
- Is your device firmware at a level, or higher than the level, at which it has been tested according to the posted device compatibility lists? |
### Table 1-1 Steps for troubleshooting NetBackup problems (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Record all information</td>
<td>Capture potentially valuable information:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- NetBackup progress logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- NetBackup Reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- NetBackup Utility Reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- NetBackup debug logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Media and Device Management debug logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- On UNIX NetBackup servers, check for error or status messages in the system log or standard output.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Error or status messages in dialog boxes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- On Windows, NetBackup servers, check for error or status information in the Event Viewer Application and System log.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Record this information for each try. Compare the results of multiple tries. A record of tries is also useful for others at your site and for Technical Support in the event that you cannot solve the problem. You can get more information about logs and reports. See the NetBackup Logging Reference Guide.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Correct the problem</td>
<td>After you define the problem, use the following information to correct it:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Take the corrective action that the status code or message recommends. See the Status Codes Reference Guide.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 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 &quot;Troubleshooting NetBackup problems&quot; on page 19.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Complete a problem report for Technical Support</td>
<td>If your troubleshooting is unsuccessful, prepare to contact Technical Support by filling out a problem report.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Contact Technical Support</td>
<td>The Veritas Technical Support website has a wealth of information that can help you solve NetBackup problems.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access Technical Support at the following URL:</td>
</tr>
</tbody>
</table>
**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)
About gathering information for NetBackup-Java applications

If you encounter problems with the NetBackup-Java applications, use the following methods to gather data for support.
The following scripts are available for gathering information:

jnbSA
(NetBackup-Java administration application startup script)

Logs the data in a log file in
/usr/openv/netbackup/logs/user_ops/nbjlogs. At startup, the script tells you which file in this directory it logs to. Normally, this file does not become very large (usually less than 2 KB). Consult the file /usr/openv/java/Debug.properties for the options that can affect the contents of this log file.

NetBackup-Java administration application on Windows

If NetBackup is installed on the computer where the application was started, the script logs the data in a log file at install_path\NetBackup\logs\user_ops\nbjlogs.

If NetBackup was not installed on this computer, then no log file is created. To produce a log file, modify the last “java.exe” line in the following to redirect output to a file:
install_path\java\nbjava.bat.

If NetBackup was not installed on this computer, the script logs the data in a log file at install_path\Veritas\Java\logs.

Note: When NetBackup is installed where the application is started, and when install_path is not set in the setconf.bat file, the script logs the data here: install_path\Veritas\Java\logs.

/usr/openv/java/get_trace

UNIX/Linux only.
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.

UNIX/Linux:
/usr/openv/netbackup/bin/support/nbsu

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

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

An application does not respond.
Wait for several minutes before you assume that the operation is hung. Some operations can take quite a while to complete, especially operations in the Activity Monitor and Reports applications.
Run `/usr/openv/java/get_trace` under the account where you started the Java application. This script causes a stack trace to write to the log file.

For example, if you started `jnbSA` from the root account, start `/usr/openv/java/get_trace` as root. Otherwise, the command runs without error, but fails to add the stack trace to the debug log. This failure occurs because root is the only account that has permission to run the command that dumps the stack trace.

UNIX/Linux only: Still no response after several minutes.

Get data about your configuration.

Run the `nbsu` 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 Veritas Technical Support

Provide the log file and the output of the `nbsu` 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
- Troubleshooting vnetd proxy connections
- Troubleshooting security certificate revocation
- About troubleshooting networks and host names
- Verifying host name and service entries in NetBackup
- About the bplntcmd utility
- Using the Host Properties window to access configuration settings
- Resolving full disk problems
- Frozen media troubleshooting considerations
- Troubleshooting problems with the NetBackup web services
- Troubleshooting problems with the NetBackup web server certificate
- Resolving PBX problems
- Troubleshooting problems with validation of the remote host
- 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
- Troubleshooting error messages in the NetBackup Administration Console
- Extra disk space required for logs and temporary files for the NetBackup Administration Console
- Unable to logon to the NetBackup Administration Console after external CA configuration
- Troubleshooting file-based external certificate issues
- Troubleshooting Windows certificate store issues
- Troubleshooting backup failures
- Troubleshooting backup failure issues with NAT clients or NAT servers
- Troubleshooting issues with the NetBackup Messaging Broker (or nbmqbroker) service
- Issues with email notifications for Windows systems
- Issues with KMS configuration
- Issues with initiating the NetBackup CA migration because of large key size
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 Veritas Technical Support site has a wealth of information that can help you solve NetBackup problems. See the following site for comprehensive troubleshooting details:

https://www.veritas.com/support/en_US.html

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**

- The following procedures describe what to check first. They branch off to other procedures as appropriate.
- See “Troubleshooting NetBackup problems” on page 19.
- See “Verifying that all processes are running on UNIX servers” on page 22.
- See “Verifying that all processes are running on Windows servers” on page 25.

**Installation troubleshooting**

- Problems that apply specifically to installation.
- See “Troubleshooting installation problems” on page 28.

**Configuration troubleshooting**

- Problems that apply specifically to configuration.
- See “Troubleshooting configuration problems” on page 29.
General test and troubleshooting

These procedures define general methods for finding server and client problems and should be used last.

See “Testing the master server and clients” on page 34.
See “Testing the media server and clients” on page 38.
See “Resolving network communication problems with UNIX clients” on page 41.
See “Resolving network communication problems with Windows clients” on page 46.
See “Verifying host name and service entries in NetBackup” on page 73.
See “About the bpclntcmd utility” on page 84.
See “Verifying host name and service entries in NetBackup” on page 73.

Other troubleshooting procedures

See “Resolving full disk problems” on page 87.
See “Frozen media troubleshooting considerations” on page 89.
See “About the conditions that cause media to freeze” on page 90.
See “Troubleshooting network interface card performance” on page 122.

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 77.
- See “Example of host name and service entries on UNIX master server and media server” on page 79.
- See “Example of host name and service entries on UNIX PC clients” on page 81.
- See “Example of host name and service entries on UNIX server that connects to multiple networks” on page 82.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Verify operating systems and peripherals.</td>
<td>Ensure that your servers and clients are running supported operating system versions and that any peripherals you use are supported. See the <a href="http://www.veritas.com/docs/DOC5332">NetBackup Master Compatibility List</a>. In addition, the NetBackup release notes include a section &quot;Required operating system patches and updates for NetBackup&quot; that should be checked. The release notes for your release are available here: <a href="http://www.veritas.com/docs/DOC5332">http://www.veritas.com/docs/DOC5332</a>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Use reports to check for errors.</td>
<td>Use the <strong>All Log Entries</strong> report and check for NetBackup errors for the appropriate time period. This report can show the context in which the error occurred. Often it provides specific information, which is useful when the status code can result from a variety of problems. See the Reports information in the <a href="http://www.veritas.com/docs/DOC5332">NetBackup Administrator’s Guide, Volume I</a>. If the problem involved a backup or archive, check the <strong>Status of Backups</strong> report. This report gives you the status code. If you find a status code or message in either of these reports, perform the recommended corrective actions. See the <a href="http://www.veritas.com/docs/DOC5332">Status Codes Reference Guide</a>.</td>
</tr>
</tbody>
</table>
| Step 3 | Check the operating system logs. | Check the system log (UNIX) or the **Event Viewer** Application and System log (Windows) if the problem pertains to media or device management and one of the following is true:  
  - NetBackup does not provide a status code.  
  - You cannot correct the problem by following the instructions in NetBackup status codes and messages.  
  - You cannot correct the problem by following the instructions in media and device management status codes and messages.  
These logs can show the context in which the error occurred. The error messages are usually descriptive enough to point you to a problem area. |
### Table 2-1 Steps for troubleshooting NetBackup problems (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 4 | Review the debug logs. | Read the applicable enabled debug logs and correct any problems you detect. If these logs are not enabled, enable them before you retry the failed operation.  
See the *NetBackup Logging Reference Guide*. |
| Step 5 | Retry the operation. | If you performed corrective actions, retry the operation. If you did not perform corrective actions or if the problem persists, continue with the next step. |
| Step 6 | Get more information for installation problems. | If you see the problem during a new installation or upgrade installation, or after you make changes to an existing configuration, see the following procedures:  
See “Troubleshooting installation problems” on page 28.  
See “Troubleshooting configuration problems” on page 29. |
| Step 7 | Ensure that the servers and clients are operational. | If you experienced a server or a client disk crash, procedures are available on how to recover the files that are critical to NetBackup operation.  
See “About disk recovery procedures for UNIX and Linux” on page 193.  
See “About disk recovery procedures for Windows” on page 203. |
| Step 8 | Ensure that the partitions have enough disk space. | Verify that you have enough space available in the disk partitions that NetBackup uses. If one or more of these partitions is full, NetBackup processes that access the full partition fail. The resulting error message depends on the process. Possible error messages: “unable to access” or “unable to create or open a file.”  
On UNIX systems, use the `df` command to view disk partition information.  
On Windows systems, use Disk Manager or Explorer.  
Check the following disk partitions:  
- The partition where NetBackup software is installed.  
- On the NetBackup master or media server, the partition where the NetBackup databases reside.  
- The partition where the NetBackup processes write temporary files.  
- The partition where NetBackup logs are stored.  
- The partition where the operating system is installed. |
| Step 9 | Increase the logging level. | Enable verbose logging either for everything or only for the areas that you think are related to the problem.  
See the *NetBackup Logging Reference Guide* for information on changing the logging level. |
### Table 2-1  Steps for troubleshooting NetBackup problems  

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 10</td>
<td>Determine which daemons or processes are running.</td>
<td>Follow the procedures for UNIX or Windows NetBackup servers. See “Verifying that all processes are running on UNIX servers” on page 22. See “Verifying that all processes are running on Windows servers” on page 25.</td>
</tr>
</tbody>
</table>

#### 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/openv/netbackup/bin/bpps`
2. Ensure that the following processes are running on the NetBackup servers:

**Master server**

<table>
<thead>
<tr>
<th>Process</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>bpcd -standalone</td>
<td>nb pem</td>
</tr>
<tr>
<td>bpcompatd</td>
<td>nbproxy</td>
</tr>
<tr>
<td>bpdbm</td>
<td>nbbrb</td>
</tr>
<tr>
<td>bjobod</td>
<td>nbrrmms</td>
</tr>
<tr>
<td>bprd</td>
<td>nbsl</td>
</tr>
<tr>
<td>java</td>
<td>nbstserv</td>
</tr>
<tr>
<td>nbars</td>
<td>nbsvcmgr</td>
</tr>
<tr>
<td>nbatd</td>
<td>nbwmc</td>
</tr>
<tr>
<td>nbdisco (discovery manager)</td>
<td>NB_dbsrv</td>
</tr>
<tr>
<td>nbemm</td>
<td>pbx_exchange</td>
</tr>
<tr>
<td>nbevtmgr</td>
<td>vmd</td>
</tr>
<tr>
<td>nbim (index manager)</td>
<td>vnetd -standalone</td>
</tr>
<tr>
<td>nbjm</td>
<td></td>
</tr>
</tbody>
</table>

**Media server**

<table>
<thead>
<tr>
<th>Process</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>avrd (automatic volume recognition, only if drives are configured on the server)</td>
<td></td>
</tr>
<tr>
<td>bpcd -standalone</td>
<td></td>
</tr>
<tr>
<td>ltid (needed only if tape devices are configured on the server)</td>
<td></td>
</tr>
<tr>
<td>mtstrmd (if the system has data deduplication configured)</td>
<td></td>
</tr>
<tr>
<td>nbrrmms</td>
<td></td>
</tr>
<tr>
<td>nbsl</td>
<td></td>
</tr>
<tr>
<td>nbsvcmgr</td>
<td></td>
</tr>
<tr>
<td>pbx_exchange</td>
<td></td>
</tr>
<tr>
<td>spad (if the system has data deduplication configured)</td>
<td></td>
</tr>
<tr>
<td>spoold (if the system has data deduplication configured)</td>
<td></td>
</tr>
<tr>
<td>vmd (volume)</td>
<td></td>
</tr>
<tr>
<td>vnetd -standalone</td>
<td></td>
</tr>
</tbody>
</table>

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 [https://www.veritas.com/support/en_US/article.100002166](https://www.veritas.com/support/en_US/article.100002166).
3 If either the NetBackup Request Daemon (bprd) or the NetBackup Database Manager Daemon (bpdbm) is not running, start them by entering the following command:

/usr/openv/netbackup/bin/initbprd

4 If the NetBackup Web Management Console (nbwmc) is not running, start it with the following command:

/usr/openv/netbackup/bin/nbwmc

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

/usr/openv/volmgr/bin/stoptlid

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

/usr/openv/volmgr/bin/vmps

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

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

/usr/openv/volmgr/bin/ltid

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

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Start all services on the master servers.</td>
<td>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 Activity Monitor or the Services application in the Windows Control Panel. To start all of the services, run <code>{install_path}/NetBackup/bin/bpup.exe</code>.</td>
</tr>
</tbody>
</table>

**Services on master servers:**
- NetBackup Authentication
- NetBackup Client Service
- NetBackup Compatibility Service
- NetBackup Database Manager
- NetBackup Discovery Framework
- NetBackup Enterprise Media Manager
- NetBackup Event Manager
- NetBackup Indexing Manager
- NetBackup Job Manager
- NetBackup Policy Execution Manager
- NetBackup Relational Database Manager
- NetBackup Remote Manager and Monitor Service
- NetBackup Request Daemon
- NetBackup Resource Broker
- NetBackup Service Layer
- NetBackup Service Monitor
- NetBackup Storage Lifecycle Manager
- NetBackup Vault Manager
- NetBackup Volume Manager
- NetBackup Web Management Console
- Veritas Private Branch Exchange

**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 [https://www.veritas.com/support/en_US/article.100002166](https://www.veritas.com/support/en_US/article.100002166)
Table 2-2  Steps to ensure that all necessary processes are running on Windows servers (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 2 | Start all services on the media servers. | Services on media servers:  
- NetBackup Client Service  
- NetBackup Deduplication Engine (if the system has data deduplication configured)  
- NetBackup Deduplication Manager (if the system has data deduplication configured)  
- NetBackup Deduplication Multi-Threaded Agent (if the system has data deduplication configured)  
- NetBackup Device Manager service (if the system has configured devices)  
- NetBackup Remote Manager and Monitor Service (if the system has data deduplication configured)  
- NetBackup Volume Manager service |
| Step 3 | Start all services on the clients. | Services on clients:  
- NetBackup Client Service  
- NetBackup Legacy Client Service  
- Veritas Private Branch Exchange |
| Step 4 | Start `avrd` and processes for robots. | Use the NetBackup Activity Monitor to see if the following processes are running:  
- `avrd` (automatic media recognition), only if drives are configured on the server  
- Processes for all configured robots.  
  See the NetBackup Administrator’s Guide, Volume I.  
If these processes are not running, stop and restart the NetBackup Device Manager service. Use the NetBackup Activity Monitor or the Services application in the Windows Control Panel. |
Table 2-2  Steps to ensure that all necessary processes are running on Windows servers (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 5 | Restart the operation or do additional troubleshooting. | If you had to start any of the processes or services in the previous steps, retry the operation.  
If the processes and services are running or the problem persists, you can try to test the servers and clients.  
See “Testing the master server and clients” on page 34.  
See “Testing the media server and clients” on page 38.  
If you cannot start any of these processes or services, check the appropriate debug logs for NetBackup problems.  
See the NetBackup Logging Reference Guide.  
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, it is recommended that you add commands for starting them to your startup scripts, so they restart in case you have to restart. |

Troubleshooting installation problems

Use the following steps to troubleshoot installation problems.

Table 2-3  Steps for troubleshooting installation problems.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Determine if you can install the software on the master server and the media servers by using the release media. | Some reasons for failure are as follows:  
- Not logged on as an administrator on a Windows system (you must have permission to install services on the system)  
- Permission denied (ensure that you have permission to use the device and to write the directories and files being installed)  
- Bad media (contact Technical Support)  
- Defective drive (replace the drive or refer to vendor’s hardware documentation)  
- Improperly configured drive (refer to the system and the vendor documentation) |
## Table 2-3

Steps for troubleshooting installation problems. *(continued)*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 2 | Determine if you can install NetBackup client software on the clients.  | **Note:** Before you install or use NetBackup on a Linux client, verify that the `bpcd -standalone` and `vnetd -standalone` services are started on that computer. These services ensure proper communication between the NetBackup master and the Linux client.  
**Note:** 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.  
**Note:** See the [NetBackup Appliance Administrator’s Guide](#). |
|        | Do the following:                                                      |                                                                                                                                          |
|        | ■ For an install to a trusting UNIX client, verify the following:       |                                                                                                                                          |
|        | ■ The correct client name is in your policy configuration.              |                                                                                                                                          |
|        | ■ The correct server name is in the client `/.rhosts` file.             |                                                                                                                                          |
|        | If the installation hangs, check for problems with the shell or the environment variables for the root user on the client. The files that you check depend on the platform, operating system, and shell you use. For example, your `.login` on a Sun system runs an `stty` (such as `stty ^erase`) before it defines your terminal type. If this action causes the install process to hang, you can modify the `.login` file to define the terminal before you run the `stty`. Or, move the client `.login` to another file until the install is complete.  
■ For an installation to a secure UNIX client, check your `ftp` configuration. For example, you must use a user name and password that the client considers valid. |
| Step 3 | Resolve network problems.                                              | Determine if the problem is related to general network communications. See “Resolving network communication problems with UNIX clients” on page 41.  
See “Resolving network communication problems with Windows clients” on page 46. |

## Troubleshooting configuration problems

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Check for device</td>
<td>Check for the following device configuration problems:</td>
</tr>
<tr>
<td></td>
<td>configuration problems.</td>
<td>- Configuration for robotic drive does not specify the robot.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Drive is configured as wrong type or density.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Incorrect Robotic Drive Number.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- SCSI ID for the robotic control is specified instead of the logical Robot Number that is assigned to the robot.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The same robot number is used for different robots.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- SCSI ID for the drive is specified instead of a unique Drive Index number.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- A platform does not support a device or was not configured to recognize it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Robotic device is not configured to use LUN 1, which some robot hardware requires.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- On UNIX, drive no-rewind device path is specified as a rewind path.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- On UNIX, tape devices are not configured with &quot;Berkeley style close.&quot; NetBackup requires this feature which is configurable on some platforms. Further explanation is available.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- On UNIX, tape devices (other than QIC) are not configured as &quot;variable mode.&quot; 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>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- On UNIX, pass-through paths to the tape drives have not been established.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>More description is available on device configuration problems:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See the <a href="#">NetBackup Device Configuration Guide</a>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Check the daemons or</td>
<td>Check for the following problems with the daemons or services:</td>
</tr>
<tr>
<td></td>
<td>services.</td>
<td>- The daemons or services do not start during restart (configure system so they start).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Wrong daemons or services are started (problems with media server startup scripts).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Configuration was changed while daemons or services were running.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See the <a href="#">NetBackup Administrator’s Guide, Volume I</a>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 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 <code>robotic daemons</code>.</td>
</tr>
</tbody>
</table>
Table 2-4 Steps for troubleshooting configuration problems (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 3 | Retry the operation and check for status codes and messages. | If you found and corrected any configuration problems, retry the operation and check for NetBackup status codes or messages in the following:  
  - Check the All Log Entries report for NetBackup errors for the appropriate time period. This report can show the context in which the error occurred. Often it provides specific information, which is useful when the error can result from a variety of problems.
    - If the problem involved a backup or archive, check the job's Detailed Status in the Activity Monitor. Also check the Status of Backups report.
    - If you find a status code or message in either of these reports, perform the recommended corrective actions.
    - See the Status Codes Reference Guide.
  - Check the system logs on UNIX or the Event Viewer Application and System log on Windows if the following is true: The problem pertains to media or device management, and NetBackup does not provide a status code. Or you cannot correct the problem by following the instructions in the status codes.
  - Check the appropriate enabled debug logs. Correct any problems you detect.
    - If these logs are not enabled, enable them before your next try.
    - See the NetBackup Logging Reference Guide. |
| Step 4 | Retry the operation and do additional troubleshooting. | If you performed corrective actions, retry the operation. If you did not perform corrective actions or the problem persists, go to one of the following procedures.  
  - See “Resolving full disk problems” on page 87.  
  - See “Frozen media troubleshooting considerations” on page 89.  
  - See “About the conditions that cause media to freeze” on page 90.  
  - See “Troubleshooting network interface card performance” on page 122. |

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>
<thead>
<tr>
<th>Message</th>
<th>Explanation</th>
<th>Recommended action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive does not support serialization</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Robot does not support serialization</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>No license for this robot type</td>
<td>NetBackup server does not support the robotic type that is defined for this robot.</td>
<td>Define a different robot. Use only the robotic libraries that NetBackup server supports.</td>
</tr>
<tr>
<td>No license for this drive type</td>
<td>The drive type that is defined for this drive that the NetBackup server does not support.</td>
<td>Define a different drive. Use only the drives that NetBackup supports.</td>
</tr>
<tr>
<td>Unable to determine robot type</td>
<td>NetBackup does not recognize the robotic library. The robotic library cannot be auto-configured.</td>
<td>Do the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Download a new device_mapping file from the Veritas Support website, and try again.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Configure the robotic library manually.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Use only the robotic libraries that NetBackup supports.</td>
</tr>
<tr>
<td>Drive is standalone or in unknown robot</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Robot drive number is unknown</td>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 2-5  Recommended actions for device configuration messages (continued)

<table>
<thead>
<tr>
<th>Message</th>
<th>Explanation</th>
<th>Recommended action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive is in an unlicensed robot</td>
<td>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.</td>
<td>Configure a drive that does not reside in the unlicensed robot.</td>
</tr>
</tbody>
</table>
| Drive’s SCSI adapter does not support pass-thru (or pass-thru path does not exist) | A drive was found that does not have a SCSI pass-through path configured. The possible causes are:  
  ■ The drive is connected to an adapter that does not support SCSI pass-through.  
  ■ The pass-through path for this drive has not been defined. | Change the drive’s adapter or define a pass-through path for the drive. For information about the SCSI adapter pass-through, see the NetBackup Device Configuration Guide.                                                                                             |
| No configuration device file exists          | A device has been detected without the corresponding device file necessary to configure that device.                                                                                                           | For directions about how to create device files, see the NetBackup Device Configuration Guide.                                                                                                                                                                                               |
| Unable to determine drive type               | The NetBackup server does not recognize the drive. The drive cannot be auto-configured.                                                                                                                      | Do the following:  
  ■ Download a new device_mapping file from the Veritas Support website, and try again.  
  ■ Configure the drive manually.  
  ■ Use only the drives that NetBackup supports.                                                                                                                                                                                                                                         |
| Unable to determine compression device       | A drive was detected without the expected compression device file that is used to configure that device. Automatic device configuration tries to use a device file that supports hardware data compression. When multiple compression device files exist for a drive, automatic device configuration cannot determine which compression device file is best. It uses a non-compression device file instead. | If you do not need hardware data compression, no action is necessary. The drive can be operated without hardware data compression. Hardware data compression and tape drive configuration help are available. For directions about how to create device files, see the NetBackup Device Configuration Guide. |

---

Troubleshooting procedures
Device configuration problem resolution
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>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enable debug logs.</td>
<td>Enable the appropriate debug logs on the master server. For information on logging, see the NetBackup Logging Reference Guide.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure a test policy.</td>
<td>Configure a test policy to use a basic disk storage unit. 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 bplabel command, NetBackup automatically assigns a previously unused media ID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 2-6: Steps for testing the master server and clients (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 3 | Verify the daemons and services. | To verify that the NetBackup daemons or services are running on the master server, do the following:  
- To check the daemons on a UNIX system, enter the following command:  
  `/usr/openv/netbackup/bin/bpps -x`  
- To check the services on a Windows system, use the NetBackup Activity Monitor or the Services application of the Windows Control Panel. |
| Step 4 | Backup and restore a policy. | Start a manual backup of a policy by using the manual backup option in the NetBackup administration interface. Then, restore the backup.  
These actions verify the following:  
- NetBackup server software is functional, which includes all daemons or services, programs, and databases.  
- NetBackup can mount the media and use the drive you configured. |
| Step 5 | Check for failure. | If a failure occurs, check the job’s **Detailed Status** in the **Activity Monitor**.  
You can also try the NetBackup **All Log Entries** report. For the failures that relate to drives or media, verify that the drive is in an UP state and that the hardware functions.  
To isolate the problem further, use the debug logs.  
For an overview of the sequence of processing, see the information on backup processes and restore processes in the **NetBackup Logging Reference Guide**. |
| Step 6 | Consult information besides the debug logs. | If the debug logs do not reveal the problem, check the following:  
- Systems Logs on UNIX systems  
- Event Viewer and System logs on Windows systems  
- Media Manager debug logs on the media server that performed the backup, restore, or duplication  
- The **bpdm** and **bptm** debug logs on the media server that performed the backup, restore, or duplication  
See the vendor manuals for information on hardware failures. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 7 | Verify robotic drives. | If you use a robot and the configuration is an initial configuration, verify that the robotic drive is configured correctly. In particular, verify the following:  
- The same robot number is used both in the Media and Device Management and storage unit configurations.  
- Each robot has a unique robot number.  
On a UNIX NetBackup server, you can verify only the Media and Device Management part of the configuration. To verify, use the `tpreq` command to request a media mount. Verify that the mount completes and check the drive on which the media was mounted. Repeat the process until the media is mounted and unmounted on each drive from the host where the problem occurred. If this works, the problem is probably with the policy or the storage unit configuration. When you are done, `tpunmount` the media. |
| Step 8 | Include a robot in the test policy. | If you previously configured a nonrobotic drive and your system includes a robot, change your test policy now to specify a robot. Add a volume to the robot. The volume must be in the NetBackup volume pool on the EMM database host for the robot.  
Return to step 3 and repeat this procedure for the robot. This procedure verifies that NetBackup can find the volume, mount it, and use the robotic drive. |
| Step 9 | Use the robotic test utilities. | If you have difficulties with the robot, try the test utilities. See “About the robotic test utilities” on page 183.  
Do not use the Robotic Test Utilities when backups or restores are active. These utilities prevent the corresponding robotic processes from performing robotic actions, such as loading and unloading media. The result is that it can cause media mount timeouts and prevent other robotic operations like robotic inventory and inject or eject from working. |
| Step 10 | Enhance the test policy. | Add a user schedule to your test policy (the backup window must be open while you test). Use a storage unit and media that was verified in previous steps. |
### Table 2-6  Steps for testing the master server and clients (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 11 | Backup and restore a file.      | Start a user backup and restore of a file by using the client-user interface on the master server. Monitor the status and the progress log for the operation. If successful, this operation verifies that the client software is functional on the master server.  
If a failure occurs, check the NetBackup **All Log Entries** report. To isolate the problem further, check the appropriate debug logs from the following list.  
On a UNIX system, the debug logs are in the `/usr/openv/netbackup/logs/` directory. On a Windows computer, the debug logs are in the `install_path\NetBackup\logs\` directory.  
Debug log directories exist for the following processes:  
- `bparchive` (UNIX only)  
- `bpbackup` (UNIX only)  
- `bpbkar`  
- `bpcd`  
- `bplist`  
- `bprd`  
- `bprestore`  
- `nbwin` (Windows only)  
- `bpinetd` (Windows only)  
Explanations about which logs apply to specific client types are available.  
For information on logging, see the *NetBackup Logging Reference Guide*.  |
| Step 12 | Reconfigure the test policy.    | Reconfigure your test policy to name a client that is located elsewhere in the network. Use a storage unit and media that has been verified in previous steps. If necessary, install the NetBackup client software. |
| Step 13 | Create debug log directories.   | Create debug log directories for the following processes:  
- `bprd` on the server  
- `bpcd` on the client  
- `bpbkar` on the client  
- `nbwin` on the client (Windows only)  
- `bpbackup` on the client (except Windows clients)  
- `bpinetd` (Windows only)  
- `tar`  
- **On the media server:** `bpbrm`, `bpdm`, and `bptm`  
Explanations about which logs apply to specific client types are available.  
For information on logging, see the *NetBackup Logging Reference Guide*. |
Table 2-6  Steps for testing the master server and clients (continued)

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

Testing the media server and clients

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

See “Testing the master server and clients” on page 34.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enable legacy debug logs.</td>
<td>Enable appropriate legacy debug logs on the servers, by entering the following: UNIX/Linux: /usr/openv/netbackup/logs/mklogdir Windows: install_path\NetBackup\logs\mklogdir.bat See the NetBackup Logging Reference Guide. 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.</td>
</tr>
</tbody>
</table>
Table 2-7  Steps for testing the media server and clients *(continued)*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 2 | Configure a test policy. | Configure a test policy with a user schedule (set the backup window to be open while you test) by doing the following:  
- Name the media server as the client and a storage unit that is on the media server (preferably a nonrobotic drive).  
- Add a volume on the EMM database host for the devices in the storage unit. Ensure that the volume is in the NetBackup volume pool.  
- Insert the volume in the drive. If you do not pre-label the volume by using the `bplabel` command, NetBackup automatically assigns a previously unused media ID. |
| Step 3 | Verify the daemons and services. | Verify that all NetBackup daemons or services are running on the master server. Also, verify that all Media and Device Management daemons or services are running on the media server.  
To perform this check, do one of the following:  
- On a UNIX system, run:  
  ```bash
  /usr/openv/netbackup/bin/bpps -x
  ```  
- On a Windows system, use the Services application in the Windows Control Panel. |
| Step 4 | Backup and restore a file. | Perform a user backup and then a restore of a file from a client that has been verified to work with the master server.  
This test verifies the following:  
- NetBackup media server software.  
- NetBackup on the media server can mount the media and use the drive that you configured.  
- Communications between the master server processes `nbemm`, `nbemn`, `nbemt`, `nbemm` server process, and media server processes `bpem`, `bpbem`, `bpdm`, and `bptm`.  
- Communications between media server process `bpbem`, `bpdm`, `bptm`, and client processes `bpem` and `bpbkar`.  
For the failures that relate to drives or media, ensure that the drive is in an UP state and that the hardware functions. |
| Step 5 | Verify communication between the master server and the media servers. | If you suspect a communications problem between the master server and the media servers, check the debug logs for the pertinent processes.  
If the debug logs don’t help you, check the following:  
- On a UNIX server, the System log  
- On a Windows server, the Event Viewer Application and System log  
- `vmd` debug logs |
**Table 2-7** Steps for testing the media server and clients (*continued*)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 6 | Ensure that the hardware runs correctly. | For the failures that relate to drives or media, ensure that the drive is running and that the hardware functions correctly. See the vendor manuals for information on hardware failures. If you use a robot in an initial configuration condition, verify that the robotic drive is configured correctly. In particular, verify the following:  
  - The same robot number is used both in the Media and Device Management and storage unit configurations.  
  - Each robot has a unique robot number.  
On a UNIX server, you can verify only the Media and Device Management part of the configuration. To verify, use the `tpreq` command to request a media mount. Verify that the mount completes and check the drive on which the media was mounted. Repeat the process until the media is mounted and unmounted on each drive from the host where the problem occurred. Perform these steps from the media server. If this works, the problem is probably with the policy or the storage unit configuration on the media server. When you are done, use `tpunmount` to unmount the media. |
Table 2-7 Steps for testing the media server and clients (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 7 | Include a robotic device in the test policy. | If you previously configured a non-robotic drive and a robot was attached to your media server, change the test policy to name the robot. Also, add a volume for the robot to the EMM server. Verify that the volume is in the NetBackup volume pool and in the robot. Start with step 3 to repeat this procedure for a robot. This procedure verifies that NetBackup can find the volume, mount it, and use the robotic drive. If a failure occurs, check the NetBackup All Log Entries report. Look for any errors that relate to devices or media. See the NetBackup Administrator’s Guide, Volume I. If the All Log Entries report doesn’t help, check the following:  
  - On a UNIX server, the system logs on the media server  
  - vmd debug logs on the EMM server for the robot  
  - On a Windows system, the Event Viewer Application and System log In an initial configuration, verify that the robotic drive is configured correctly. Do not use a robot number that is already configured on another server. Try the test utilities. See “About the robotic test utilities” on page 183. Do not use the Robotic Test Utilities when backups or restores are active. These utilities prevent the corresponding robotic processes from performing robotic actions, such as loading and unloading media. The result is that it can cause media mount timeouts and prevent other robotic operations like robotic inventory and inject or eject from working. |
| Step 8 | Test other clients or storage units. | When the test policy operates satisfactorily, repeat specific steps as necessary to verify other clients and storage units. |
| Step 9 | Test the remaining policies and schedules. | When all clients and storage units are in operation, test the remaining policies and schedules that use storage units on the media server. If a scheduled backup fails, check the All Log Entries report for errors. Then follow the suggested actions for the appropriate status code. |

Resolving network communication problems with UNIX clients

The following procedure is for resolving NetBackup communications problems, such as those associated with NetBackup status codes 25, 54, 57, and 58. This
procedure consists of two variations: one for UNIX clients and another for 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>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create debug log directories.                                           During communication retries, the debug logs provide detailed debug information, which can help you analyze the problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create the following directories:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• bpcd (on the master server and clients)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• vnetd (on the master server and clients)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• bprd (on the master server)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use the bprd log directory to debug client to master server communication, not client to media server communication problems.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Test a new configuration or modified configuration.                     If this configuration is a new or a modified configuration, do the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Check any recent modifications to ensure that they did not introduce the problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ensure that the client software was installed and that it supports the client operating system.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Check the client names, server names, and service entries in your NetBackup configuration as explained in the following topic:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See “Verifying host name and service entries in NetBackup” on page 73.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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 bprd debug log on the master server to determine what occurred when the server received the request.</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Step 3 | Verify name resolution. | To verify name resolution, run the following command on the master server and the media servers:  
  
  ```
  # bpclntcmd -hn client name
  ```  
  
  If the results are unexpected, review the configuration of these name resolution services: `nsswitch.conf` file, `hosts` file, `ipnodes` file, and `resolv.conf` file.  
  
  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:  
  
  ```
  # bpclntcmd -hn server name
  # bpclntcmd -ip IP address of server
  ``` |
| Step 4 | Verify network connectivity. | Verify network connectivity between client and server by pinging the client from the server.  
  
  ```
  # ping clientname
  ```  
  
  Where `clientname` is the name of the client as configured in the NetBackup policy configuration.  
  
  For example, to ping the policy client that is named `ant`:  
  
  ```
  # ping ant
  ant.nul.nul.com: 64 byte packets
  64 bytes from 199.199.199.24: icmp_seq=0. time=1. ms
  ----ant.nul.nul.com PING Statistics----
  2 packets transmitted, 2 packets received, 0% packet loss
  round-trip (ms) min/avg/max = 1/1/1
  ```  
  
  A successful ping verifies connectivity between the server and client. If the ping fails and ICMP is not blocked between the hosts, resolve the network problem outside of NetBackup before you proceed.  
  
  Some forms of the ping command let you ping the `bpcd` port on the client as in the following command:  
  
  ```
  # ping ant 1556
  ```  
  
  Ping 1556 (PBX) and 13724 (vnetd) in sequence, the same sequence that NetBackup tries by default. You then know which ports are closed so that you can open them for more efficient connection tries. |
### Table 2-8  Steps for resolving network communication problems with UNIX clients *(continued)*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 5 | Ensure that the client listens on the correct port for the `bpcd` connections. | On the client, run one of the following commands (depending on platform and operating system):

```
netstat -a | grep bpcd
netstat -a | grep 13782
rpcinfo -p | grep 13782
```
Repeat for 1556 (*PBX*) and 13724 (*vnetd*). If no problems occur with the ports, the expected output is as follows:

```
# netstat -a | egrep '1556\|PBX\|13724\|vnetd\|13782\|bpcd' | grep LISTEN
*.1556  *.*  0  0  49152  0 LISTEN
*.13724  *.*  0  0  49152  0 LISTEN
*.13782  *.*  0  0  49152  0 LISTEN
```

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

If the NetBackup processes are running correctly, the expected output is as follows:

```
# ps -ef | egrep 'pbx_exchange\|vnetd\|bpcd' | grep -v grep
root  306 1 0 Jul 18 ? 13:52 /opt/VRTSpbx/bin/pbx_exchange
root 10274 1 0 Sep 13 ? 0:11 /usr/openv/netbackup/bin/vnetd -standalone
root 10277 1 0 Sep 13 ? 0:45 /usr/openv/netbackup/bin/bpcd -standalone
```
Repeat the procedure on the master server(s) and media server(s), to test communication to the client.
Table 2-8 Steps for resolving network communication problems with UNIX clients (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 6 | Connect to the client through `telnet`.     | On the client, `telnet` to 1556 (PBX) and 13724 (vnetd). Check both ports to make sure that a connection is made on at least one of them. If the `telnet` connection succeeds, keep the connection until after you perform step 8, then terminate it with Ctrl-c.  
  
  `telnet clientname 1556`
  `telnet clientname 13724`
  
  Where `clientname` is the name of the client as configured in the NetBackup policy configuration. 
  
  For example, 
  
  `# telnet ant vnetd`
  `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`. 
  
  Repeat the procedure on the master server(s) and media server(s), to test communication to the client. |
| Step 7 | Identify the outbound socket on the server host. | 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). 
  
  `# netstat -na | grep ‘<client_IP_address>’ | egrep ‘1556|13724’`
  `10.82.105.11.45856 10.82.104.99.1556 49152 0 49152 0 ESTABLISHED`
  
  If `telnet` is still connected and a socket is not displayed: Remove the port number filtering and observe the port number to which the site has mapped the service name. Check that process listens on the port number in step 5. 
  
  `$ netstat -na | grep ‘<client_IP_address>’`
  `10.82.105.11.45856 10.82.104.99.1234 49152 0 49152 0 ESTABLISHED`
  
  If the socket is in a SYN_SENT state instead of an ESTABLISHED state, the server host is trying to make the connection. However, a firewall blocks the outbound TCP SYN from reaching the client host or blocks the return bound TCP SYN+ACK from reaching the server host. |
### Table 2-8  Steps for resolving network communication problems with UNIX clients (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 8 | Confirm that the telnet connection reaches this client host. | On the master server(s) and media server(s), to confirm that the telnet connection reaches this client host, run the following command:  
```
$ netstat -na | grep '<source_port>'
```

```
10.82.104.99.1556 10.82.105.11.45856 49152 0 49152 0 ESTABLISHED
```

One of the following conditions occurs:
- If 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.
- If the socket is in a SYN_RCVD state instead of an ESTABLISHED state, then the connection reached this client host. However, a firewall blocks the return of the TCP SYN+ACK to the server host.

| Step 9 | Verify communication between the client and the master server. | To verify client to master server communications, use the \texttt{bpclntcmd} utility. When \texttt{-pn} and \texttt{-sv} run on a NetBackup client, they initiate inquiries to the NetBackup master server (as configured in the client \texttt{bp.conf} file). The master server then returns information to the requesting client. More information is available about \texttt{bpclntcmd}.  
See “About the \texttt{bpclntcmd} utility” on page 84.  
The PBX, vnetd, and bprd debug logs should provide details on the nature of any remaining failure. |

---

### 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 `bprd` 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 73.

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`

   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:
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 87.

Correct the port number if necessary. Then, on Windows clients and servers, stop and restart the NetBackup Client service. Do not change NetBackup port assignments unless it is necessary to resolve conflicts with other applications. If you do change them, do so on all NetBackup clients and servers. These numbers must be the same throughout your NetBackup configuration.
5 Verify that the NetBackup Request Service (bprd) port number on Microsoft Windows is the same as on the server (by default, 13720). Do one of the following:

- **Windows clients**
  - Check the NetBackup client service port number.
  - Start the **Backup, Archive, and Restore** interface on the client. On the **File** menu, click **NetBackup Client Properties**.
  - In the **NetBackup Client Properties** dialog box on the **Network** tab, check the NetBackup client service port number.
  - Verify that the setting on the **Network** tab matches the one in the services file. The services file is located in:
    - `%SystemRoot%\system32\drivers\etc\services` (Windows)
    - The values on the **Network** tab are written to the services file when the NetBackup client service starts.

- **UNIX NetBackup servers**
  - The bprd port number is in the `/etc/services` file.
  - See “Using the Host Properties window to access configuration settings” on page 87.

- **Windows NetBackup servers**
  - Set these numbers in the **Client Properties** dialog box in the **Host Properties** window.
  - See “Using the Host Properties window to access configuration settings” on page 87.

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

- **Windows**
  - `%SystemRoot%\system32\drivers\etc\hosts`

- **UNIX**
  - `/etc/hosts`

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 \texttt{bpclntcmd} utility to verify client to master server communications. When the \texttt{-pn} and \texttt{-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 \texttt{bpclntcmd} utility” on page 84.

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

A complete description of \texttt{bptestbpcd} is in the \textit{NetBackup Commands Reference Guide}.

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

\section*{Troubleshooting vnetd proxy connections}

The Veritas Network Daemon \texttt{vnetd} process and its proxy processes enable communication between NetBackup hosts and remote hosts.

The following topics contain security certificate revocation troubleshooting information:

See “vnetd proxy connection requirements” on page 50.

See “Where to begin to troubleshoot vnetd proxy connections” on page 52.

See “Verify that the vnetd process and proxies are active” on page 52.

See “Verify that the host connections are proxied” on page 53.

See “Test the vnetd proxy connections” on page 53.

See “Examine the log files of the connecting and accepting processes” on page 56.

See “Viewing the vnetd proxy log files” on page 56.

If you cannot determine the cause of connection problems, contact your Veritas support representative.

\section*{vnetd proxy connection requirements}

For communication within the same NetBackup domain:

- Host ID-based certificates and a certificate revocation list must be present on all NetBackup 8.1 and later hosts.
  
  The NetBackup global security settings configure how NetBackup provisions certificates.
Verify the global settings under **Security Management** in the **NetBackup Administration Console**.

To observe the certificates that NetBackup uses between hosts, use the `-verbose` option with the `bptestbpcd -host` command and option and with the `bpclntcmd -pn` command and option.

- Host IDs must be mapped for host names on all NetBackup 8.1 and later hosts. The NetBackup global security settings configure how NetBackup maps host IDs to name.
  - Verify the global settings under **Security Management** in the **NetBackup Administration Console**. Alternatively, you can use the following command and option:
    - Windows:
      ```
      install_path\Veritas\NetBackup\bin\admincmd\nbseccmd
      -getsecurityconfig -autoaddhostmapping
      ```
    - UNIX:
      ```
      /usr/openv/netbackup/bin/admincmd/nbseccmd -getsecurityconfig
      -autoaddhostmapping
      ```

- For NetBackup hosts earlier than 8.1, you must allow insecure communication. The NetBackup global security settings configure if NetBackup can communicate with hosts earlier than 8.1.
  - Verify the global settings under **Security Management** in the **NetBackup Administration Console**. Alternatively, you can use the following command and option:
    - Windows:
      ```
      install_path\Veritas\NetBackup\bin\admincmd\nbseccmd
      -getsecurityconfig -insecurecommunication
      ```
    - UNIX:
      ```
      /usr/openv/netbackup/bin/admincmd/nbseccmd -getsecurityconfig
      -insecurecommunication
      ```

- The NetBackup web services on the master server must be active. To confirm that they are active, use the following NetBackup command and option:
  - Windows: `install_path\Veritas\NetBackup\bin\nbcertcmd -ping`
  - UNIX: `/usr/openv/netbackup/bin/nbcertcmd -ping`

- If the master server is configured to use external CA-signed certificates, the hosts should enroll their external CA-signed certificates with the appropriate master server domain.
  
  For more information on external CA support and certificate enrollment, refer to the *NetBackup Security and Encryption Guide*. 

---

Troubleshooting procedures

**Troubleshooting vnetd proxy connections**
For Auto Image Replication, host ID-based certificates from the source master server are required on all of the trusted master servers in the destination domains.

If the master server is configured to use external CA-signed certificates, ensure that trust is established between the source and target master servers using external CA-signed certificates.

For more information, see the *NetBackup Deduplication Guide*.

Where to begin to troubleshoot vnetd proxy connections

NetBackup status code 61 and status codes in the 76xx range relate to vnetd proxy communication.

If a NetBackup job fails because of vnetd proxy connection problems, examine the job details for the status codes of interest. Then, refer to the NetBackup documentation for the explanations of status codes. Take note of any connection IDs in the following format; they are helpful for additional troubleshooting:

{23FAD260-7D2F-11E7-91C6-2EB679166937}:OUTBOUND

If the failure is not during a NetBackup job, examine the exit status of the operation for the status codes of interest. Also examine the debug logs for the processes that are involved in the operation. Look first at the command that initiated the operation or the service that performed the request.

You can find the status codes described in the following:

- The *NetBackup Status Codes Reference Guide*.
- The NetBackup Administration Console help.
- The **Troubleshooter** in the *NetBackup Administration Console*.
- The NetBackup OpsCenter help.

If a job did not run, verify that the vnetd process and its proxies are active.

Verify that the vnetd process and proxies are active

On Windows, you can use the **Task Manager Processes** tab (you must show the **Command Line** column) to determine if the proxies are active. On UNIX and Linux, you can use the NetBackup bpps command, as follows:

```
$ bpps
...output shortened...
root 13577  1  0 Jun27 ?   00:00:04 /usr/openv/netbackup/bin/vnetd -standalone
root 13606  1  0 Jun27 ?   00:01:55 /usr/openv/netbackup/bin/vnetd -proxy inbound_proxy
   -number 0
```
Depending on which vnetd process or proxy is or is not running, try the following:

- If the vnetd process (-standalone) is not running, start it.
- If the vnetd process is running, examine the vnetd debug log to confirm that it tries to start the proxies.
- If the vnetd process tries to start the inbound and the outbound proxies: Examine the proxy log file to determine why the proxy does not listen for connections. Use the nbpxyhelper short component name or its originator ID 486 with the vxlogview command.
- If the vnetd process tries to start the HTTP tunnel proxy, examine the HTTP tunnel proxy log. Use the nbpxytlnl short component name or its originator ID 490 with the vxlogview command.

If the vnetd process and its proxies are active, determine if the connections are proxied.

**Verify that the host connections are proxied**

You can use the NetBackup bptestbpcd command on a NetBackup 8.1 or later server to verify that the connections to a remote host are proxied, as follows:

**Windows:** `install_path\Veritas\NetBackup\bin\admincmd\bptestbpcd -host remote_host`

**UNIX:** `/usr/openv/netbackup/bin/admincmd/bptestbpcd -host remote_host`

The **PROXY** in the following command output example shows that the connections are proxied:

```
1 1 0
127.0.0.1:42553 -> 127.0.0.1:52236 PROXY 10.81.245:895     -> 10.81.40.148:1556
127.0.0.1:35386 -> 127.0.0.1:49429 PROXY 10.81.245:51325 -> 10.81.40.148:1556
```

If the connections are proxied, test the proxy connections.

**Test the vnetd proxy connections**

The NetBackup command that you use to test the vnetd proxy connections differs between a server and a client.
Testing a vnet proxy connection from a server

To test connections from a NetBackup 8.1 or later server to another NetBackup 8.1 or later host, you can use the NetBackup `bptestbpcd` command with the `-verbose` option. Examine the command output for status codes or any indications of failure. Then, refer to the NetBackup documentation for the explanations of the status codes.

The following example shows a successful connection test from a NetBackup media server named `connect-host.example.com` to a media server named `accept-host.example.com`:

```
# bptestbpcd -host accept-host.example.com -verbose
1 1 1
127.0.0.1:43697 -> 127.0.0.1:58089 PROXY 10.80.97.186:47054 -> 10.80.97.140:1556
127.0.0.1:52061 -> 127.0.0.1:58379 PROXY 10.80.97.186:37522 -> 10.80.97.140:1556
LOCAL_CERT_ISSUER_NAME = /CN=broker/OU=root@master.example.com/O=vx
LOCAL_CERT_SUBJECT_COMMON_NAME = a753da9b-b1ff-4a5f-b57d-69a4e2b47e29
PEER_CERT_ISSUER_NAME = /CN=broker/OU=root@master.example.com/O=vx
PEER_CERT_SUBJECT_COMMON_NAME = b900a238-d7be-4c6e-8af6-19b5c1d1dec4
PEER_NAME = connect-host.example.com
HOST_NAME = accept-host.example.com
CLIENT_NAME = accept-host.example.com
VERSION = 0x08100000
PLATFORM = linuxR_x86_2.6.18
PATCH_VERSION = 8.1.0.0
SERVER_PATCH_VERSION = 8.1.0.0
MASTER_SERVER = master.example.com
EMM_SERVER = master.example.com
NB_MACHINE_TYPE = MEDIA_SERVER
SERVICE_TYPE = VNET_DOMAIN_CLIENT_TYPE
PROCESS_HINT = 7157d866-8eb2-45bb-bde8-486790c0b40c
```

Conversely, the following example shows a connection test to the same media server that fails after its security certificate was revoked:

```
# bptestbpcd -host accept-host.example.com -verbose
<16>bptestbpcd main: Function ConnectToBPCD(accept-host.example.com) failed: 7653
<16>bptestbpcd main: The Peer Certificate is revoked
<16>bptestbpcd main: The certificate of the host that you want to connect to is revoked.
Revocation Reason Code : 0 Revocation Time : 1502637798: 7653
The Peer Certificate is revoked
```

NetBackup hosts must have a valid host ID-based security certificate and a valid certificate revocation list so they can communicate with other NetBackup hosts.
The lack of either prevents communication. In this case, you can look up status code 7653 to find the explanation for and recommended action to recover from the error.

**Testing a vnet proxy connection from a client**

On a NetBackup 8.1 or later client, you can use the NetBackup `bpclntcmd` command to test the connection to the master server. Examine the command output for status codes or any indications of failure. Then, refer to the NetBackup documentation for the explanations of status codes. The following is the command syntax:

Windows:

```
install_path\Veritas\NetBackup\bin\bpclntcmd -pn -verbose
```

UNIX:

```
/usr/openv/netbackup/bin/bpclntcmd -pn -verbose
```

The following example shows a successful response to the `bpclntcmd` command:

```
# bpclntcmd -pn -verbose
expecting response from server master.example.com
127.0.0.1:52704 -> 127.0.0.1:33510 PROXY 10.80.97.186:40348 -> 10.80.97.157:1556
LOCAL_CERT_ISSUER_NAME = /CN=broker/OU=root@master.example.com/O=vx
LOCAL_CERT_SUBJECT_COMMON_NAME = 7157d866-8eb2-45bb-bde8-486790c0b40c
PEER_CERT_ISSUER_NAME = /CN=broker/OU=root@master.example.com/O=vx
PEER_CERT_SUBJECT_COMMON_NAME = b900a238-d7be-4c6e-8af6-19b5c1d1dec4
PEER_IP = 10.80.97.186
PEER_PORT = 40348
PEER_NAME = connect-host.example.com
POLICY_CLIENT = *NULL*
Old Domain Service Type VNET_DOMAIN_SERVER_TYPE and Hint
New Domain Service Type VNET_DOMAIN_SERVER_TYPE and Hint 7157d866-8eb2-45bb-bde8-486790c0b40c
```

Conversely, the following example shows a response to the `bpclntcmd` command on a NetBackup client that has a revoked certificate:

```
# bpclntcmd -pn -verbose
Unable to perform peer host name validation. Curl error has occurred for peer name: master.example.com, self name: connect-host: 0
   [PROXY] Encountered error (VALIDATE_PEER_HOST_PROTOCOL_RUNNING) while processing (ValidatePeerHostProtocol): 1
Can't connect to host master.example.com: cannot connect on socket (25)
```

If the vnetd proxy connections are active, examine the log files of the connecting and accepting processes.

Troubleshooting vnetd proxy connections

55

Troubleshooting procedures
Examine the log files of the connecting and accepting processes

A NetBackup process that initiates a connection is the connecting process, and the target of that connection is the accepting process. The connecting and accepting processes communicate with the respective outbound and inbound vnetd proxy processes. Each proxy process verifies whether the connection is permitted.

The debug logs of the connecting process and the accepting process show their interaction with the proxy. Examine the logs for any status codes and status messages. Also examine the logs for the unique inbound and outbound connection IDs. You can use those IDs if you need to examine the vnetd proxy process logs. You can debug most connections from either host.

For example, the following connecting process log file excerpt shows that a host validation failure prevented a connection:

Peer host validation failed for SECURE connection; Peer host: accepting-host.example.com, Error: 8618, Message: Connection is dropped, because the host ID-to-hostname mapping is not yet approved., nbu status = 7648, severity = 1

A NetBackup host’s names must be mapped to its host ID. If a host name is not mapped properly in NetBackup, communication fails. In this case, you can look up status code 7648 to find the explanation for and recommended action to recover from the error.

If you do not find an indication of a problem by examining the connecting process and accepting process log files, examine the vnetd proxy log files. You can use the connection IDs to find relevant information.

Viewing the vnetd proxy log files

The vnetd proxy processes log to different files than vnetd itself. The following table identifies the unified logging short component names and the originator IDs for the vnetd proxies.

<table>
<thead>
<tr>
<th>Proxy</th>
<th>Component name</th>
<th>Originator ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>The inbound and the outbound proxies</td>
<td>nbpxyhelper</td>
<td>486</td>
</tr>
<tr>
<td>The HTTP tunnel</td>
<td>nbpxytntl</td>
<td>490</td>
</tr>
</tbody>
</table>

The following is the NetBackup vxlogview command syntax to view the inbound and the outbound proxy log file using the short component name:
Windows: `install_path\Veritas\NetBackup\bin\vxlogview -p NB -i nbpxyhelper`

UNIX: `/usr/openv/netbackup/bin/vxlogview -p NB -i nbpxyhelper`

The `vxlogview` command includes options to refine the view of the log file. For example, to troubleshoot `vnetd` proxy connections, you can use the connection ID as follows:

`vxlogview -p NB -i nbpxyhelper -X '{23FAD260-7D2F-11E7-91C6-2EB679166937}:OUTBOUND'`

**Note:** On Windows, omit the single quote marks from the connection ID string.

The [NetBackup Commands Reference Guide](#) describes the `vxlogview` command and its options.

The [NetBackup Logging Reference Guide](#) describes unified logging and how to view the log files.

**Troubleshooting security certificate revocation**

For jobs, NetBackup writes the cause of failures to the Job Details. Jobs are backups, restores, duplications, and replications. To troubleshoot errors related to host certificates, examine the job details for the messages and the status codes. Look for the messages that relate to certificates, revocation, and CRL. The status codes that accompany the messages are closely adjacent. Look up the descriptions of the status codes for explanations and recommended actions to resolve the issues.

You also may need to examine the `vnetd` proxy process log files. As with the job details, examine the logs for the messages and the status codes that relate to certificates, revocation, and CRL. Status codes that accompany a message are closely adjacent.

See "Viewing the vnetd proxy log files" on page 56.

You can find the status codes described in the following:

- The [NetBackup Status Codes Reference Guide](#).
- The NetBackup Administration Console help.
- The Troubleshooter in the [NetBackup Administration Console](#).
- The NetBackup OpsCenter help.

A host's CRL may affect troubleshooting.

See "How a host’s CRL affects certificate revocation troubleshooting" on page 59.
The following topics describe how to troubleshoot several security certificate revocation scenarios:

See “NetBackup job fails because of revoked certificate or unavailability of CRLs” on page 60.

See “NetBackup job fails because of apparent network error” on page 61.

See “NetBackup job fails because of unavailable resource” on page 62.

See “Master server security certificate is revoked” on page 63.

If you cannot determine the cause of problems, contact your Veritas technical support representative.

Troubleshooting cloud provider’s revoked SSL certificate issues

If SSL is enabled and the CRL option is enabled, each non-self-signed SSL certificate is verified against the CRL. If the certificate is revoked, NetBackup does not connect to the cloud provider.

For troubleshooting cloud storage CRL validation issues, refer to the following logs for cURL error 60:

- \texttt{tpcommand} logs for configuration issues.
- \texttt{bptm} logs for backup and restore issues.
- \texttt{nbrmms} logs if the cloud storage server is down.

Symptoms:

- Cloud Storage creation fails.
- Backup job fails because the cloud storage server is down.

Causes:

- The certificate is revoked, NetBackup does not connect to the cloud provider.
- The CRL file failed to download.

Resolution:

- If the problem is a CRL verification failure, contact your security administrator
- If the problem is a download failure, verify the firewall settings. Refer to the \texttt{NetBackup Cloud Administrator's Guide} and ensure that you have met all the requirements for CRL.
Troubleshooting procedures

Troubleshooting cloud provider’s CRL download issues
Download fails because any HTTP connection that is made to port 80 is blocked in the media server.

Symptoms:
■ Cloud Storage creation fails.
■ Backup job fails because the cloud storage server is down.

Causes:
■ NetBackup cannot connect to the destination port 80.
■ The firewall setting does not allow connecting to unknown URLs.

Resolution:
■ Update the firewall setting to connect to port 80. If you cannot, turn off the CRL check.
■ To turn off the CRL, change the cloud storage host properties. Refer to the NetBackup Cloud Administrator’s Guide for more information.

How a host’s CRL affects certificate revocation troubleshooting
Each NetBackup host obtains a fresh certificate revocation list periodically. When a host’s certification revocation list is up-to-date, job failure messages and status codes are accurate and dependable. Likewise, NetBackup audit messages are accurate and dependable.

However, if the CRL is not up-to-date, job failures may appear as network errors. You may need to examine more than the NetBackup job details and command output to isolate the error.

Each NetBackup host learns about new certificate revocations only when its CRL is refreshed.

If a NetBackup CA-signed certificate is used
The CRL on the master server is generated every 60 minutes or within 5 minutes of a revocation. Conversely, the interval at which other NetBackup hosts request a new CRL from the master server may be longer.

The Security level for certificate deployment setting determines the CRL refresh interval for all NetBackup hosts. Although all NetBackup hosts update their CRLs on the same time interval, when each host requests a new CRL varies.

Verify the security settings under Security Management in the NetBackup Administration Console.
If an external CA-signed certificate is used

If a NetBackup host is configured to use CRLs from the path that is specified for the `ECA_CRL_PATH` configuration option, CRLs are refreshed as per `ECA_CRL_PATH_SYNC_HOURS`.

If the NetBackup host is configured to download CRLs from CDPs, CRLs are refreshed as per `ECA_CRL_REFRESH_HOURS`.

For more information about external certificate configuration options for CRLs and the global security settings, see the NetBackup Security and Encryption Guide.

NetBackup job fails because of revoked certificate or unavailability of CRLs

**Symptom**
A NetBackup job fails.

**Cause**
The cause may be one of the following reasons:

- The security certificate of the client is revoked.
- The security certificate of the media server that backs up the client is revoked.
- The security certificate of the master server is revoked.
- The CRL on the client, media server, or the master server is corruptedor missing.

**Resolution**

1. Examine the job details for the following message strings and adjacent status codes:
   - For certificate revocation, look for the message strings that contain `certificate` and `revoked`.
   - For the CRL, look for the message strings that contain `certificate revocation list` or `CRL and missing, corrupted, or unavailable`.

2. If necessary, determine if the client or the media server certificate was revoked.
   See “Determining a NetBackup host's certificate state” on page 64.

3. If an external CA-signed certificate is used, refer to the external certificate section:
   See “Troubleshooting issues with external CA-signed certificate revocation” on page 67.
4. Refer to the NetBackup documentation for the explanations for the status codes and recommended actions for recovery. If possible, resolve the issue.

5. If you cannot resolve the issue in a timely fashion, remove the revoked host from the backup policy or deactivate the policy. If the revoked host is the media server, deactivate it. (You can ignore “NetBackup version” errors when you deactivate the host.)


7. If necessary, add the client back to the backup policy, activate the backup policy, or activate the media server.

NetBackup job fails because of apparent network error

Symptom
A job may fail with network error 23, 25, 59, or perhaps other network error.

Cause
The host certificate of a NetBackup client or the media server that backs it up may be revoked. Also, the CRL on the client or the media server may be out-of-date, missing, or corrupt. Therefore, the client or the media server cannot determine that a host certificate is revoked. The job runs but communication fails and appears as a network error.

Resolution
1. Determine if the client or the media server certificate was revoked.
   See “Determining a NetBackup host's certificate state” on page 64.

2. Optionally, verify the cause by doing one of the following:
   a. Log onto the revoked host and examine the vnetd proxy log file. Look for the message strings that contain the following:
      - PEER_HOST_PROTOCOL_ERROR
      - certificate revocation list
      - CRL and missing or corrupted
   See “Viewing the vnetd proxy log files” on page 56.
   b. Use the NetBackup bptestbpcd command to see if a host certificate is revoked.
   See “Determining a NetBackup host's certificate state” on page 64.
3. Resolve the issue:
   - If the CRL on a host is missing or corrupt, refresh the CRL on that host. How to refresh a host’s CRL is documented in the NetBackup Security and Encryption Guide.
   - If an external CA-signed certificate is used, refer to the external certificate section. See “Troubleshooting issues with external CA-signed certificate revocation” on page 67.
   - If NetBackup CA-signed host certificate is revoked, resolve the security issue and then reissue the certificate. How to reissue a certificate is documented in the NetBackup Security and Encryption Guide.

NetBackup job fails because of unavailable resource

**Symptom**
A problem with a certificate or CRL may appear as an unavailable resource. For example, the job details may show that a storage server is down or unavailable. A job may run for an extended period of time before it times out.

**Cause**
The security certificate of the media server that backs up or restores the client is revoked. Or for disk-based storage, the certificate of the storage server may be revoked.

**Resolution**
1. Determine the state of the security certificate on the client and the media server or the storage server. See “Determining a NetBackup host's certificate state” on page 64.
2. Depending on which host has the revoked certificate, do one of the following:
   - If the revoked host is a client, remove it from the backup policy or deactivate the policy.
   - If the revoked host is the media server or a storage server, deactivate it. (You can ignore “NetBackup version” errors when you deactivate the host.) If possible, change the storage unit to use a different media server or storage server.
3. Investigate the revoked host to determine the security issue and then resolve the issue.
If an external CA-signed certificate is used, refer to the external certificate section.

See “Troubleshooting issues with external CA-signed certificate revocation” on page 67.

4. If a NetBackup CA-signed host certificate is revoked, resolve the security issue and then reissue the certificate. Certificate reissue is documented in the NetBackup Security and Encryption Guide.

5. After you return the revoked host to service, revert any policy changes you made to prevent jobs for the client or reactivate the media server.

Master server security certificate is revoked

A revoked security certificate on a NetBackup master server is the worst case scenario for NetBackup security. The following symptoms may indicate that the master server certificate is revoked:

■ Jobs fail with network errors.
■ Media servers deactivate spontaneously.
■ The vnetd proxy process log files on hosts show that the master server’s certificate is revoked.
  See “Viewing the vnetd proxy log files” on page 56.
■ The bptestbpcd -host master_server command output may show that the master server’s certificate is revoked.
  See “Determining a NetBackup host’s certificate state” on page 64.

If the master server is compromised and remains compromised, do the following:

If a NetBackup CA-signed certificate is used

1. Do not trust the certificate revocation list on any host.
2. Resolve the issue, reissue the master server’s security certificate, and then return the master server to service.
3. If you cannot resolve the issue and return the master server to service, replace it. You must then reissue all host certificates.

If an external CA-signed certificate is used, you can undo the revocation of the master server’s certificate or enroll a new certificate for the master server.

See “Troubleshooting issues with external CA-signed certificate revocation” on page 67.
Determining a NetBackup host's certificate state

If NetBackup CA-signed certificate is used

You can determine the state of a NetBackup certificate: Active or Revoked. Doing so may help troubleshoot connection and communication problems. Three methods exist to determine a certificate state, as follows:

- **Verify a host certificate from the host itself**
  
  The method uses the NetBackup `nbcertcmd` command.
  
  See “To verify the host’s certificate state from the host” on page 65.

- **Verify a host certificate from a NetBackup server**
  
  The method uses the NetBackup `bptestbpcd` command.
  
  See “To verify from a NetBackup server if a different host’s certificate is revoked” on page 65.

- **Verify a host certificate from the NetBackup Administration Console**
  
  See “To verify a host’s certificate using the NetBackup Administration Console” on page 66.
To verify the host's certificate state from the host

1. Optionally, on the NetBackup host run the following command as an administrator to get the most recent certificate revocation list:

   UNIX: /usr/openv/netbackup/bin/nbcertcmd -getCRL [-server master_server_name]

   Windows: install_path\NetBackup\bin\nbcertcmd -getCRL [-server master_server_name]

   To get a CRL from a NetBackup domain other than the default, specify the -server master_server_name option and argument.

2. On the NetBackup host, run the following command as an administrator:

   UNIX: /usr/openv/netbackup/bin/nbcertcmd-hostSelfCheck [-cluster] [-server master_server_name]

   Windows: install_path\NetBackup\bin\nbcertcmd -hostSelfCheck [-cluster] [-server master_server_name]

   Use one or both of the following options if necessary:

   -cluster Use this option on the active node of a NetBackup master server cluster to verify the certificate of the virtual host.

   -server Use this option with the master_server_name argument to verify a certificate from a master server other than the default.

3. Examine the command output. The output indicates that either the certificate is or is not revoked.

To verify from a NetBackup server if a different host's certificate is revoked

1. As an administrator on the NetBackup master server or a NetBackup media server, run the following command:

   UNIX: /usr/openv/netbackup/bin/admincmd/bptestbpcd -host hostname -verbose

   Windows: install_path\NetBackup\bin\bptestbpcd -host hostname -verbose

   For -host hostname, specify the host for which you want to verify the certificate.

2. Examine the command output. If the certificate on the specified host is revoked, the command output includes the string The Peer Certificate is revoked. If the command output does not include that string, the certificate is valid.
To verify a host’s certificate using the NetBackup Administration Console

2. For the host of interest, examine the Certificate State column for state of the certificate.

If external CA-signed certificate is used

You can determine the state of an external CA-signed host certificate: Active or Revoked. Doing so may help troubleshoot connection and communication problems.

Two methods exist to determine a certificate state, as follows:

Verify a host certificate from the host itself  
See “To verify a host certificate from the host itself” on page 66.

Verify a host certificate from a NetBackup server  
See “To verify from a NetBackup server if a different host’s certificate is revoked” on page 67.

To verify a host certificate from the host itself

1. Refresh the CRLs in the NetBackup CRL cache.
   
   See “Troubleshooting issues with external CA-signed certificate revocation” on page 67.

2. On the NetBackup host, run the following command as an administrator:
   
   UNIX: `/usr/openv/netbackup/bin/nbcertcmd -hostSelfCheck [-cluster]

   Windows: `install_path\NetBackup\bin\nbcertcmd -hostSelfCheck [-cluster]`

   Use the -cluster option on the active node of a clustered master server to verify the certificate of the virtual name.

3. Examine the command output. The output indicates whether the certificate is revoked or not.
To verify from a NetBackup server if a different host’s certificate is revoked

1. As an administrator on the NetBackup master server or a NetBackup media server, run the following command:

   **UNIX:**
   `/usr/openv/netbackup/bin/admincmd/bptestbpcd -host hostname -verbose`

   **Windows:**
   `install_path\NetBackup\bin\bptestbpcd -host hostname -verbose`

   For `-host hostname`, specify the host for which you want to verify the certificate.

2. Examine the command output. If the certificate on the specified host is revoked, the command output includes the string ‘The Peer Certificate is revoked’. If the command output does not include that string, the certificate is valid.

Troubleshooting issues with external CA-signed certificate revocation

The NetBackup CRL cache is updated with the required CRLs using either `ECA_CRL_PATH` or CDPs.

For more details, refer to the About certificate revocation lists for external CA chapter from the *NetBackup Security and Encryption Guide*.

**Symptom**

The certificate revocation list is unavailable (NetBackup status code - 5982)

**Cause**

- The NetBackup is not configured with correct CRL path or the certificate does not contain valid CDP.
- The host does not have a CRL cached in the NetBackup CRL cache.

**Resolution**

1. If the `ECA_CRL_PATH` setting is specified in the NetBackup configuration file, ensure the following:

   - `ECA_CRL_PATH` has the correct CRL directory path
   - CRL directory contains CRLs for all required certificate issuers (based on the `ECA_CRL_CHECK` setting)

   If the CDP is used (`ECA_CRL_PATH` is not specified)
   - Ensure that the certificate has at least one CDP (with HTTP/HTTPS protocol) that points to a CRL that includes revocation information for all reasons.
- CDP URL is accessible.

2 Ensure that the CRL is valid in the directory specified for ECA_CRL_PATH or at CDP location.
  - CRL is in PEM or DER format.
  - CRL is not expired.
  - CRL is not a delta CRL.
  - CRL's last update date is not in future.

3 If the bpclntcmd -crl_download service is running, terminate it using the bpclntcmd -terminate command and retry the operation.

4 Examine the required CRLs are available in the NetBackup CRL cache at the following location:
   UNIX:/usr/openv/var/vxss/crl
   Windows: install_path\NetBackup\var\vxss\crl

5 If the issue persists, examine bpclntcmd logs at the following location:
   UNIX:/usr/openv/netbackup/logs/bpclntcmd
   Windows: install_path\NetBackup\logs\bpclntcmd

Symptom
The NetBackup is functioning correctly even if the certificate is revoked or the NetBackup operations are failing with the error ‘certificate is revoked’ even if the certificate is not revoked.

Cause
The NetBackup host’s CRL cache is not updated.
Resolution

1. Verify if the CRLs at the following location are updated:
   UNIX: /usr/openv/var/vxss/crl
   Windows: install_path\NetBackup\var\vxss\crl

   If not, clean up the cached CRLs for issuers in the certificate chain as per the ECA_CRL_CHECK setting.

   For cleanup operation, use the `nbcertcmd -cleanupCRLCache -issuerHash SHA-1_hash_of_CRL_issuer_name` command.

2. If the ECA_CRL_PATH setting is specified in the NetBackup configuration file, ensure that it contains the latest CRLs for all the required issuers.

3. If the `bpclntcmd -crl_download` service is running, terminate it using the `bpclntcmd -terminate` command and retry the operation.

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/openv/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 function).
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/openv/netbackup/bin/bpclntcmd -pn (UNIX)
# install_path\NetBackup\bin\bpclntcmd -pn (Windows)
```

Expecting response from server wind.abc.me.com
danr.abc.me.com danr 194.133.172.3 4823

Where the first output line identifies the server to which the request is directed. 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/openv/netbackup/db/altnames/host.xlate (UNIX)
install_path\NetBackup\db\altnames\host.xlate (Windows)
```

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

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

```
key  hostname_from_client  client_as_known_by_server
```

The following describes the preceding variables:

- **key** is a numeric value used by NetBackup to specify the cases where the translation is to be done. Currently this value must always be 0, which indicates a configured name translation.

- **hostname_from_client** is the value to translate. This value must correspond to the name that the client’s gethostname() function obtains and sends to the server in the request.

- **client_as_known_by_server** is the name to substitute for `hostname_from_client` when the client responds to requests. This name must be the name that is configured in the NetBackup configuration on the master server. It must also be known to the master server’s network services.

This following is an example:
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 69.

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 gethostbyname() failed.
  ```

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

  See “Using the Host Properties window to access configuration settings” on page 87.

On UNIX NetBackup servers and clients

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

- Ensure that a SERVER entry exists for the master server and each media server in the configuration. The master server must be the first name in the list. If you add or modify SERVER entries on the master server, stop and restart bprd and bpdbm before the changes take effect.

- The bp.conf of the master server does not require the addition of other clients, other than the master server as CLIENT_NAME = master server name. The name is added by default.

  The bp.conf file is in the /usr/openv/netbackup directory on UNIX clients.

  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/openv/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/openv/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 77.

   See “Example of host name and service entries on UNIX master server and media server” on page 79.

   See “Example of host name and service entries on UNIX PC clients” on page 81.

   See “Example of host name and service entries on UNIX server that connects to multiple networks” on page 82.

   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.

   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.

- Check the bp.conf file on UNIX servers and 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 84.

---

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.
Consider the following about Figure 2-1:

Troubleshooting procedures
Verifying host name and service entries in NetBackup
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.
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 (Windows) 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

Troubleshooting procedures

Verifying host name and service entries in NetBackup
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.
Consider the following about Figure 2-4:

UNIX server connects to multiple networks

**Figure 2-4**

- **UNIX client**: mars
- **UNIX media server**: saturn
- **UNIX master server**: jupiter, meteor, saturn, pluto
- **Policy Client List**: jupiter, mars, saturn, pluto

** troubleshoot procedures**

- **Verifying host name and service entries in NetBackup**

```plaintext
/usr/openv/netbackup/bp.conf
SERVER=jupiter
SERVER=meteor
SERVER=saturn
CLIENT_NAME=mars

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

/usr/openv/netbackup/bp.conf
SERVER=jupiter
SERVER=meteor
SERVER=saturn
CLIENT_NAME=mars

/usr/openv/netbackup/bp.conf
SERVER=jupiter
SERVER=meteor
SERVER=saturn
CLIENT_NAME=pluto

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

/etc/services
#Volume Manager services
vmd 13701/tcp vmd
```
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.

With the -pn option, bpcIntcmd connects to the master server and returns how the master server sees the connecting host: source IP address and port number, host name to which the IP resolves, and policy client for that host name. Add the -verbose option to see additional connection details including the host certificates that NetBackup uses to authenticate the hosts.

The following directory contains the command that starts the utility:

**Windows**

\install_path\NetBackup\bin

**UNIX**

/usr/openv/netbackup/bin

On Windows, run this bpcIntcmd command in an MS-DOS command window so you can see the results.
The `bpclntcmd` options that are useful for testing the functionality of the host name and IP address resolution are `-ip`, `-hn`, `-sv`, and `-pn`. The following topics explain each of these options:

**-ip**

`bpclntcmd -ip IP_Address`

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

**-hn**

`bpclntcmd -hn Hostname`

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

**-sv**

`bpclntcmd -sv`

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

**-pn**

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

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

The following is true of this command example:

- **expecting response from server**
  - `rabbit.friendlyanimals.com` is the master server entry from the server list on the client.
  - `dove.friendlyanimals.com` is the connection name (peer name) returned by the master server. The master server obtained this name through `getaddrinfo()`.
  - `dove` is the client name configured in the NetBackup policy client list.
  - `123.145.167.3` is the source IP address from which the client connected to the master server.
  - `57141` is the source port number of the connection from the client.
Use with the `-pn` option to display more details about the connection and the host certificates used. The following is an example of the output:

```
$ bpclntcmd -pn -verbose
expecting response from server rabbit.friendlyanimals.com
127.0.0.1:34923 -> 127.0.0.1:50464 PROXY 123.145.167.3:27082
  -> 192.168.0.15:1556
LOCAL_CERT_ISSUER_NAME = /CN=broker/OU=root@rabbit.friendlyanimals.com /O=vx
LOCAL_CERT_SUBJECT_COMMON_NAME = fad46a25-1fe2-4143-a62b-2dc0642d8c45
PEER_CERT_ISSUER_NAME = /CN=broker/OU=root@rabbit.friendlyanimals.com /O=vx
PEER_CERT_SUBJECT_COMMON_NAME = 3ca8ab18-8eb3-4c8e-825d-faeef9320d1
PEER_IP = 123.145.167.3
PEER_PORT = 27082
PEER_NAME = dove.friendlyanimals.com
POLICY_CLIENT = dove
```

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

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

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

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

**Note:** The `bpclntcmd` command logs messages to the `usr/openv/netbackup/logs/bpclntcmd` directory (UNIX) or the `install_path\NetBackup\logs\bpclntcmd` (Windows). For earlier versions of NetBackup, `bpclntcmd` logs are sent to the `bplist` directory, not the `bpclntcmd` 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_dbsrv 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/openv/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/openv/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/openv/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  
- The bptm log from the media servers that froze the media:
  /usr/openv/netbackup/logs/bptm
- The Admin messages or syslog from the operating system.
Windows

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

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

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

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

See “Frozen media troubleshooting considerations” on page 89.
See “About the conditions that cause media to freeze” on page 90.

### 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 Veritas Support website:

  [www.veritas.com/docs/TECH59978](http://www.veritas.com/docs/TECH59978)
Media not supported

Ensure that the media is supported for use with the tape drive by the tape drive vendor.

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

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

  The following conditions can cause this error:

  - NetBackup requests a media ID to be mounted in a drive. If the media ID that is physically recorded on the tape is different than the NetBackup media ID, the media freezes. This error occurs if the robot needs to be inventoried, or if barcodes have been physically changed on the media.

  - Another NetBackup installation previously wrote to the media with different barcode rules.

  - The drives in the robot are not configured in order within NetBackup, or they are configured with the wrong tape paths. The correct robot drive number is important to the proper mounting and use of media. The robot drive number is normally based on the relationship of the drive serial number with the drive serial number information from the robotic library. Validate this number before you consider that the device configuration is complete.

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

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

  These library tapes may have been written outside of NetBackup. By default, NetBackup only writes to a blank media or other NetBackup media. Other media types (DBR, TAR, CPIO, ANSI, MTF1, and recycled Backup Exec BE-MTF1 media) are frozen as a safety measure. Change this behavior by using the following procedure:
On UNIX
To allow NetBackup to overwrite foreign media, add the following to the `bp.conf` file that is located at
`/usr/openv/netbackup/bp.conf` for the related media server:

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

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

On Windows
On the 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:

```plaintext
FREEZING media id 000067: it contains Veritas 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
```

## Troubleshooting problems with the NetBackup web services

Use the following steps to troubleshoot issues with the NetBackup web services.

### To resolve problems with the NetBackup web services

1. Verify that NetBackup Web Management Console service is running.
   - On UNIX, enter the following command:
     ```
     /usr/openv/netbackup/bin/bpps -x
     ```
   - On Windows, use NetBackup Activity Monitor or the Services application of the Windows Control Panel.

2. Stop and restart the NetBackup Web Management Console service.
   - On UNIX:
     ```
     install_path/netbackup/bin/nbwmc -terminate
     ```
   - On Windows, use the Services application in the Windows Control Panel.

3. Review the NetBackup web server logs and web application logs.

   See “Viewing NetBackup web services logs” on page 94.
See the following tech note for the web server tasks you must perform before installing the master server:


Viewing NetBackup web services logs

NetBackup creates logs for the NetBackup web server and for the web server applications.

- The logs for the NetBackup web server framework do not use unified logging. For more information on the format of these logs and how they are created, see the documentation for Apache Tomcat at http://tomcat.apache.org. These logs are written to the following location:

  `usr/openv/wmc/webserver/logs`

  `install_path\NetBackup\wmc\webserver\logs`

- The NetBackup web application logs use unified logging. These logs are written to the following location.

  `usr/openv/logs/nbwebservice`

  `install_path\NetBackup\logs\nbwebservice`

  Contact Technical Support for additional help with these logs.

Troubleshooting web service issues after external CA configuration

**Problem**

The web service does not start or respond after external certificate (ECA) configuration.

**Cause**

Check the web server logs at the following location:

`install_path/wmc/webserver/logs/catalina.log`

Check if the logs contain any of the following strings:

```
SEVERE [main] org.apache.tomcat.util.net.SSLUtilBase.getStore Failed to load keystore type [JKS] with path [C:\Program Files\Veritas\NetBackup\var\global\wal\credentials\tpcredentials\nbwebservice.jks] due to [Illegal character in opaque part at index 2: C:\Program Files\Veritas\NetBackup\var\global\wal\credentials\tpcredentials\nbwebservice.jks]
```
Caused by: java.lang.IllegalArgumentException: Keystore was tampered with, or password was incorrect

The root cause can be: The keystore of the external CA used by the NetBackup web service is tampered or deleted.

Solution

- Verify that NetBackup Web Management Console service is running.
  Run the following command:
  On UNIX: /usr/openv/netbackup/bin/bpps -x
  On Windows: Use the NetBackup Activity Monitor or the services application of the Windows Control Panel.

- If the status is FAIL, reconfigure the external certificate by executing the following command:
  On Windows: Install path\netbackup\wmc\bin\configureWebServerCerts
  -addExternalCert -nbHost -certPath file_path -privateKeyPath file_path
  -trustStorePath file_path
  On Unix:/usr/openv/netbackup/bin/configureWebServerCerts
  -addExternalCert -nbHost -certPath file_path -privateKeyPath file_path
  -trustStorePath file_path

- Try to start the NetBackup web service.
  For windows: Install path\netbackup\wmc\bin\nbwmc.exe -start -srvname "NetBackup Web Management Console"
  For Unix:/usr/openv/netbackup/bin/nbwmc start

Problem

External certificate is not configured.

Cause

The issue can occur because of the following:

- Invalid certificate, private key, or trust store.
  Error message: The certificate could not be added. Please check the
  configureWebServerCerts logs.

- Certificate does not contain server name in the subject alternative name (SAN) of the certificate.

Solution for cause: Invalid Certificate, private key or trust store

- Open web server configuration logs
Location: <install dir>/NetBackup/wmc/webserver/logs/configureWebServerCerts.log

- Review the log messages:
  - If the logs have the following message:
    unable to load private key 22308:error:0906D06C:PEM routines:PEM_read_bio:no start line:..\crypto\pem\pem_lib.c:697:Expecting: ANY PRIVATE KEY Could not export certificates in PKCS#12 format, 1.
    The private key does not match the private key of the certificate that is provided.
    Provide the appropriate private key.
  - If the logs have following message:
    Error occurred while adding certificate to keystore. Exception: java.security.cert.CertificateParsingException: signed overrun, bytes = 918 Exiting.. Could not import CA certificates in JAVA keystore, -1.
    The file path that is provided for the -trustStorePath option is not a valid file path or a valid trust store CA certificate is not present at the given file path.
    Provide the trust store bundle path for the -trustStorePath option.

Solution for cause: Certificate does not contain server name in the subject alternative name (SAN)

The following error message is displayed:

The server name server_name was not found in the web service certificate.

The certificate could not be added. Please check configureWebServerCerts logs.

For successful configuration, ensure the following:

- Common name of the subject name and the SAN names should not be empty at the same time.
- If the SAN is not empty, host name must be present in the SAN entry.
- If SAN is empty, common name of the subject name must be host name.
  Only PEM formatted certificates are allowed.
**Note:** The host name is the name provided for the master server at the time of installation. Host name can be found in the setenv file with the `NB_HOSTNAME` property.

**Location of the file:**

On UNIX: `/usr/openv/wmc/bin/setenv`

On Windows: `install_path\Veritas\NetBackup\wmc\bin\setenv`

**Communication can be successful in the following scenarios:**

- The certificate contains all host names that the master server is known by (host names that are listed in the `SERVER` entries of other hosts in the domain) in the SAN field of the certificate.
- Server authentication attributes are set in the certificate.
- Check the logs for the missing entry.
  Add the missing host name in the SAN of the certificate.

---

**Troubleshooting problems with the NetBackup web server certificate**

NetBackup generates and deploys an X509 certificate for the NetBackup Web Management Console (`nbwmc`) or NetBackup web server during installation. This certificate authenticates the NetBackup master server and validates that a client is connected to the master server. This certificate is periodically refreshed.

**Generation of the NetBackup web server certificate**

The NetBackup web server certificate is generated during NetBackup installation. To troubleshoot the generation of this certificate, refer to the following logs. The `nbcert` and `nbatd` logs use unified logging. The `configureCerts.log` uses a simple logging style and not VxUL.

```
/usr/openv/logs/nbcert
/usr/openv/wmc/webserver/logs/configureCerts.log
/usr/openv/logs/nbatd
```

```
install_path\NetBackup\logs\nbcert
C:\ProgramData\Veritas\NetBackup\InstallLogs\WMC_configureCerts_yyyymmdd_timestamp.txt
install_path\NetBackup\logs\nbatd
```
Renewal of the NetBackup web certificate

The web server certificate has an expiration time of one year. NetBackup tries to automatically renew the certificate every 6 months. The renewed certificate is automatically deployed. If the certificate cannot be renewed, the information is audited and the error is logged in the NetBackup error log. In such cases NetBackup tries periodically try to renew the certificate (every 24 hours). If the failure to renew the certificate persists, contact Technical Support.

You can see the audit records using the `nbauditreport` command.

To troubleshoot the certificate renewal, refer to the following logs. The `nbwebservice` (OID 466 and 484) and `nbatd` (OID 18) logs use unified logging. The `configureCerts.log` uses a simple logging style and not VxUL.

```
/usr/openv/logs/nbwebservice
/usr/openv/wmc/webserver/logs/configureCerts.log
/usr/openv/logs/nbatd

install_path\NetBackup\logs\nbwebservice
C:\ProgramData\Veritas\NetBackup\InstallLogs\WMC_configureCerts_yyyymmdd_timestamp.txt
install_path\NetBackup\logs\nbatd
```

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 99.

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

   See “Checking that PBX is running” on page 99.

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 100.
4 Access and check the PBX logs by using the following procedure:
   See “Accessing the PBX logs” on page 101.

5 Check the PBX security and correct any problem by using the following procedure:
   See “Troubleshooting PBX security” on page 102.

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 104.

Checking PBX installation

NetBackup requires the Veritas 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/VRTSpbx

2 To check the version of PBX, enter the following:
   ■ On Windows: install_path\VxPBX\bin\pbxcfg -v
   ■ On UNIX: /opt/VRTSpbx/bin/pbxcfg -v

Checking that PBX is running

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

1. On UNIX, check for the PBX process:

   ```
   ps | grep pbx_exchange
   ```

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

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

   On Windows, make sure that the Private Branch Exchange service 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/VRTSpbx/bin/pbxcfg -p
     ```

     Example output:

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

2 Reset Auth User or Secure Mode as needed:
   - To add the correct user to the authenticated user list (UNIX example):
     
     /opt/VRTSpbx/bin/pbxcfg -a -u root
   
   - To set Secure Mode to false:
     
     /opt/VRTSpbx/bin/pbxcfg -d -m
   
   For more information on the pbxcfg command, refer to the pbxcfg man page.

Accessing the PBX logs

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

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

The unified logging originator number for PBX is 103. 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, nb pem, 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/VRTSpbx/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 `vmoprcmd` do not work. PBX messages similar to the following appear in `/opt/VRTSpbx/log` (UNIX) or `<install_path>\VxPBX\log` (Windows).

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

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

3 Stop NetBackup:

- On Windows:
  
  `install_path\NetBackup\bin\bpdown`

- On UNIX:
  
  `/usr/openv/netbackup/bin/bp.kill_all`

4 Stop PBX:

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

- On UNIX:
  
  `/opt/VRTSpbx/bin/vxpbx_exchanged stop`

5 Start PBX:

- On UNIX:
  
  `/opt/VRTSpbx/bin/vxpbx_exchanged start`

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

6 Start NetBackup:

- On Windows:
  
  `install_path\NetBackup\bin\bpup`
Determining if the PBX daemon or service is available

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

When a NetBackup service is not running and another process tries to connect to it, messages similar to the following appear in `/opt/VRTSpbx/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\bpdowm
     install_path\NetBackup\bin\bpup
     ```

   - On UNIX:
     
     ```
     /usr/openv/netbackup/bin/bp.kill_all
     /usr/openv/netbackup/bin/bp.start_all
     ```
Troubleshooting problems with validation of the remote host

NetBackup uses Secure Socket Layer (SSL) to communicate securely with other NetBackup hosts. Unless the other host is 8.0 or earlier, NetBackup 8.1 always requires the communication to be secure. For this, all hosts that are setting up or accepting a connection validate the remote host against its details available with the master server. The connection is dropped, if the host validation fails and this in turn can cause certain operations (like backup or restore) to fail.

To resolve the issues that arise because of host validation failures, do the following:

- Check the logs pertaining to host validation failures.
  See “Viewing logs pertaining to host validation” on page 106.
- Verify that the NetBackup web services are running on the master server.
  See “Troubleshooting problems with the NetBackup web services” on page 93.
- Verify that the NetBackup web server certificate is correctly deployed.
  See “Troubleshooting problems with the NetBackup web server certificate” on page 97.
- Verify that the host can connect to the NetBackup web service on the master server.
  See the 'About the communication between a NetBackup client located in a demilitarized zone and a master server through an HTTP tunnel' topic from the NetBackup Security and Encryption Guide.
- If the remote host is 8.0 or earlier, verify that insecure communication with such hosts is enabled.
  See “Enabling insecure communication with NetBackup 8.0 and earlier hosts” on page 106.
- Verify if there are any host ID-to-host name mappings for the remote host that are pending for approval on the master server.
  See “Approving pending host ID-to-host name mappings” on page 107.
- If NetBackup software of the remote host was recently downgraded from 8.1 to an earlier version, ensure that host information is reset on the master server.
  See the 'Resetting a NetBackup host attributes' topic from the NetBackup Security and Encryption Guide.
- Verify that the host cache has updated information about the remote host.
  See “Clearing host cache” on page 108.
If the NetBackup web server is configured to use external CA-signed certificates, ensure that the host certificate is successfully enrolled with the appropriate master server domain.

For more information on the external CA support and certificate enrollment, refer to the *NetBackup Security and Encryption Guide*.

**Viewing logs pertaining to host validation**

Host validation logs from proxy are located at the following location:

**Windows:** `Install_Path\NetBackup\logs\nbpxyhelper`

**UNIX:** `/usr/openv/logs/nbpxyhelper`

Proxy uses unified logging.

Additionally, for incoming connections, host validation logs are also stored in the respective process log files, where NetBackup host authorization occurs.

For example, if host validation has failed during `bpcd` authorization, the relevant logs can be found at:

**Windows:** `Install_Path\NetBackup\logs\bpcd`

**UNIX:** `/usr/openv/NetBackup/logs/bpcd`

Example log messages that are recorded when a host connection is dropped:

- Connection is to be dropped for peer host: examplemaster with error code:8618 error message: Connection is dropped, because the host ID-to-hostname mapping is not yet approved.

- Connection is to be dropped for peer host: 10.10.10.10 with error code:8620 error message: Connection is dropped, because insecure communication with hosts is not allowed.

**Note:** The host validation failures are shown as connection failure errors on NetBackup 8.0 and earlier hosts.

**Enabling insecure communication with NetBackup 8.0 and earlier hosts**

Check if insecure communication with NetBackup 8.0 and earlier hosts is enabled on the master server.

Run the following command:
- **Windows**: `Install_Path\NetBackup\bin\admincmd\nbseccmd -getsecurityconfig -insecurecommunication`
- **UNIX**: `/usr/openv/netbackup/bin/admincmd/nbseccmd -getsecurityconfig -insecurecommunication`

If the `insecurecommunication` option is set to 'off', enable insecure communication with NetBackup 8.0 and earlier hosts.

Run the following command:

- **Windows**: `Install_Path\NetBackup\bin\admincmd\nbseccmd -setsecurityconfig -insecurecommunication on`
- **UNIX**: `/usr/openv/netbackup/bin/admincmd/nbseccmd -setsecurityconfig -insecurecommunication on`

**Note**: Insecure communication must be enabled for OpsCenter to be able to communicate with the master server.

### Approving pending host ID-to-host name mappings

Run the following command to check the list of pending approval requests for host ID-to-host name mappings:

- **Windows**: `Install_Path\NetBackup\bin\admincmd\nbhostmgmt -list -pending`

**Example output:**

<table>
<thead>
<tr>
<th>Host ID: zzzzzz-1271-4ea4-zzzz-5281a4f760e6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host: example1.com</td>
</tr>
<tr>
<td>Master Server: example1.com</td>
</tr>
<tr>
<td>OS Type: Windows</td>
</tr>
<tr>
<td>Operating System: Microsoft Windows Server 2008 R2 64-bit Service Pack 1, Build 7601(6.1.7601)</td>
</tr>
<tr>
<td>NetBackup EEBs:</td>
</tr>
<tr>
<td>Hardware Description: GenuineIntel Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz, 4 CPUs</td>
</tr>
<tr>
<td>CPU Architecture: Intel x64</td>
</tr>
<tr>
<td>Version: NetBackup_8.1</td>
</tr>
<tr>
<td>Secure: Yes</td>
</tr>
<tr>
<td>Comment:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mapped Host Name</th>
<th>Approved</th>
<th>Conflict</th>
<th>Auto-discovered</th>
<th>Shared</th>
<th>Created On</th>
<th>Last Updated On</th>
</tr>
</thead>
</table>
UNIX: /usr/openv/netbackup/bin/admincmd/nbhostmgmt -list -pending
Example output:
Host ID: xxxxx-52e8-xxxx-ba92-7be20c6dceb9
Host: example2.com
Master Server: example2.com
OS Type: UNIX
Operating System: RedHat Linux(2.6.32-642.el6.x86_64)
NetBackup EEBs:
Hardware Description: AuthenticAMD AMD Opteron(tm) Processor 6366 HE,
16 CPUs
CPU Architecture: x86_64
Version: NetBackup_8.1
Secure: Yes
Comment:

<table>
<thead>
<tr>
<th>Mapped Host Name</th>
<th>Approved</th>
<th>Conflict</th>
<th>Auto-discovered</th>
<th>Shared</th>
<th>Created On</th>
<th>Last Updated On</th>
</tr>
</thead>
<tbody>
<tr>
<td>example2.com</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Jul 28, 2017</td>
<td>Jul 28, 2017</td>
</tr>
</tbody>
</table>

Run the following command to approve a host ID-to-host name mapping:

- **Windows**: Install_Path\NetBackup\bin\admincmd\nbhostmgmt -add -hostid zzzzzzzz-1271-4ea4-zzzz-5281a4f760e6 -mappingname mymaster
  Example output: example1.com is successfully updated.
- **UNIX**: /usr/openv/netbackup/bin/admincmd/nbhostmgmt -add -hostid xxxxx-52e8-xxxx-ba92-7be20c6dceb9 -mappingname mymaster
  Example output: example2.com is successfully updated.

**Clearing host cache**

Clearing the host cache ensures that any changes related to a host’s validation (for example, approval of host ID-to-host name mapping or changes to the global security settings) are reflected immediately on the host.

To clear the host cache, run the following command:

- **Windows**: Install_Path\NetBackup\bin\bpclntcmd -clear_host_cache
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 consume a read resource from the disk volume on which the source images reside. If no media server is available, 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. 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 action to take on the automatic replication job depends on several conditions as shown in the following table.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify the following:</td>
<td></td>
</tr>
<tr>
<td>- The SLP is active.</td>
<td></td>
</tr>
<tr>
<td>- The <code>nbstserv</code> daemon is running.</td>
<td></td>
</tr>
<tr>
<td>- The image has not exceeded the extended retry count.</td>
<td></td>
</tr>
</tbody>
</table>

**AIR replication jobs have not started**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No media server or I/O stream is available.</td>
<td></td>
</tr>
</tbody>
</table>

**AIR replication jobs are queued but have not started**
<table>
<thead>
<tr>
<th><strong>Action</strong></th>
<th><strong>Condition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>AIR replication jobs fail, for example with status 191</td>
<td>Check the job details for more information about the failure. For more details, review the <code>bpdm</code> log on the media server that processed the replication job.</td>
</tr>
</tbody>
</table>

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:

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

   Example output:
   
   LSU Info:
   Server Name: PureDisk:ss1.acme.com
   LSU Name: PureDiskVolume
   Allocation : STS_LSU_AT_STATIC
   Storage: STS_LSU_ST_NONE
   Description: PureDisk storage unit (/ss1.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:

   ```bash
   # 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
```

```
V_5_ DiskVolume < "PureDiskVolume" "PureDiskVolume" 46068048064 46058373120 0 0 0 16 1 >
V_5_ ReplicationTarget < "bayside:PureDiskVolume" >
```

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

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

```
# nbdevquery -listdv -stype PureDisk -U
```

```
Disk Pool Name : PDpool
Disk Type : PureDisk
Disk Volume Name : PureDiskVolume
...
Flag : AdminUp
Flag : InternalUp
Flag : ReplicationSource
Num Read Mounts : 0
...
```

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 0 PDpool *NULL*
```

The output shows that storage unit PDstu uses disk pool PDpool.
Check the settings on the disk pool by running the following command:

```bash
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 : ss1.acme.com (UP)

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

To check the list of media servers that are credentialed to access the storage servers and their disk pools, run the following command:

```bash
# tpconfig -dsh -all_hosts
```

```
==============================================================
Media Server: ss1.acme.com
Storage Server: ss1.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, ss1.acme.com. You have completed the storage configuration validation.
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
```
To show the status for completed replication copies, run the following command:

```bash
tbstlutil replist -U
```

**Image:**
- **Master Server:** ss1.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:** ss1.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:** ss1.acme.com
- **Backup ID:** woodridge_1287610477
- **Copy Number:** 102
**Rules for master servers used with Auto Image Replication and SLPs**

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

- 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.

  **Note:** Ensure that the Import SLP name is less than 113 characters.

- 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.

**Targeted AIR trusted master server operation failed in case of external certificate configuration**

**Add or update trust**

**Problem**

Adding or updating the trust between the source and target master server is failed.
Cause

The issue can occur because of the following reasons:

- **Cause 1** - Enrollment of source master server to target master server failed.
- **Cause 2** - Failed to add the target master server in the trusted master server database and in the configuration file as `TRUSTED_MASTER`.

Solution for cause 1 - External certificate enrollment of the source master server with the target master server failed.

See “Troubleshooting Windows certificate store issues” on page 139.

Solution for cause 2 - Failed to add the target master server in the trusted master server database and in the configuration file as `TRUSTED_MASTER`

1. Review the error message: (EXIT STATUS 5630: Failed to get version of remote master server.)
   
   If the `vnetd` proxy service is down or connection to `vnetd` proxy failed on the source master server, check the logs in the following order:
   
   - Check the connection to the `vnetd` proxy of the remote master server.
     
     To check the connection to the remote master server's `vnetd` proxy, run the `bptestbpcd -host remote_master_server_name` command.
   
   - Check the proxy logs:
     
     **Windows:** \Program Files\Veritas\NetBackup\logs\nbpxyhelper\log_file  
     **UNIX:** /usr/openv/logs/nbpxyhelper/log_file

2. Review the error message: (EXIT STATUS 5616: The local master server is not reachable. The trust is unidirectional right now, the remote master server trusts the local master server, but the local master server doesn't trust the remote master. Please remove the trust)

   If the `bprd` service is down on the source master server, check the logs in the following order:
   
   - Check the `bprd` logs.
     
     **Windows:** \Program Files\Veritas\NetBackup\logs\bprd\log_file  
     **UNIX:** /usr/openv/netbackup/logs/bprd/log_file
   
   - Check the proxy logs.
     
     **Windows:** \Program Files\Veritas\NetBackup\logs\nbpxyhelper\log_file
Remove trust

Problem
Remove trust operation failed

Cause
Failed to remove target master server from trusted master server database and from configuration file as TRUSTED_MASTER.

Solution
- Review the error message: (EXIT STATUS 5616: The local master server is not reachable. The trust is unidirectional right now, the remote master server trusts the local master server, but the local master server doesn't trust the remote master. Please remove the trust).
- The bprd service is down on the source master server.
- Check the logs in the following order:
  - Check bprd logs.
    - Windows: C:\Program Files\Veritas\NetBackup\logs\bprd\log_file
    - UNIX: /usr/openv/netbackup/logs/bprd/log_file
  - Check the proxy logs.
    - Windows: C:\Program Files\Veritas\NetBackup\logs\nbpxyhelper\log_file
    - UNIX: /usr/openv/logs/nbpxyhelper/log_file
  - Check the EMM database logs.
    - Windows: C:\Program Files\Veritas\NetBackup\logs\nbemm\log_file
    - UNIX: /usr/openv/logs/nbemm/log_file

About troubleshooting automatic import jobs that SLP components manage

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 the import operation in an SLP 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.example.com
- Backup ID: gdwinlin04_1280299412
- Client: gdwinlin04
- 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.example.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)
The action to take on the automatic import job and the automatic import event depends on several conditions as shown in the following table.

<table>
<thead>
<tr>
<th>Action</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic import jobs queue</td>
<td>No media server or I/O stream is available for this disk volume.</td>
</tr>
<tr>
<td>Automatic import jobs never start (copy stays at storage lifecycle state 1)</td>
<td>- The storage lifecycle policy is inactive.</td>
</tr>
<tr>
<td></td>
<td>- The storage lifecycle policy import destination is inactive.</td>
</tr>
<tr>
<td></td>
<td>- The storage lifecycle policy is between sessions.</td>
</tr>
<tr>
<td></td>
<td>- The image has exceeded the extended retry count and the extended retry time has not passed.</td>
</tr>
</tbody>
</table>
### Condition
- The event specifies a backup ID that already exists in this master server catalog.
- The event specifies a disk volume that is not configured in NetBackup for this storage server.
- The storage lifecycle policy that is specified in the event does not contain an import destination.
- The storage lifecycle policy that is specified in the event has an import destination with a residence that does not include the disk volume that is specified by the event.
- The storage lifecycle policy that is specified does not exist. By default, the `Storage Lifecycle Policies` 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. More information is available for the storage lifecycle policy configuration options. See the *NetBackup Administrator’s Guide, Volume I*.

### Action
- Automatic import event is discarded and the image is ignored.
- Automatic import job is started but the image is expired and deleted to clean up disk space in some cases. The event logs an error in the Problems Report or `bperror` output. An import job runs, but the import for this image fails showing a status code in the range 1532–1535.

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

To troubleshoot the job flow for automatic import jobs, use the same commands 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.example.com
Backup ID : woodridge_1287610477
Client : woodridge
Policy : two-hop-with-dup
Client Type : 0
Schedule Type : 0
Storage Lifecycle Policy : woodridge2bayside2pearl_withdup
Storage Lifecycle State : 3 (COMPLETE)
Data Classification ID : (none specified)
Version Number : 0
OriginMasterServer : woodridge.example.com
OriginMasterServerID : f5cec09a-da74-11df-8000-f5b3612d8988
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.example.com
Backup ID : gdwinlin04_1280299412
Client : gdwinlin04
Policy : (none specified)
Client Type : 0
Schedule Type : 0
Storage Lifecycle Policy : (none specified)
Storage Lifecycle State : 1 (NOT_STARTED)
Time In Process : 0 (Wed Dec 31 18:00:00 1969)
Data Classification ID : (none specified)
Version Number : 0
OriginMasterServer : master_tlk
OriginMasterServerID : 00000000-0000-0000-0000-000000000000
Import From Replica Time : 0 (Wed Dec 31 18:00:00 1969)
Required Expiration Date : 0 (Wed Dec 31 18:00:00 1969)
Created Date Time : 1287680533 (Thu Oct 21 12:02:13 2010)

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

Troubleshooting network interface card performance

If backup or restore jobs are running slowly, verify that the network interface cards (NIC) are set to full duplex. Half duplex often causes poor performance.
Note: If the NIC in a NetBackup master or media server is changed, or if the server IP address changes, CORBA communications may be interrupted. To address this situation, stop and restart NetBackup.

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

To troubleshoot network interface card performance

1. Log onto the host that contains the network interface card whose duplex mode you want to check.

2. Enter the following command to view the current duplex setting.

   `ifconfig -a`

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

   The following is an example output from a NAS filer:

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

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

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

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

   `ifconfig e0 mediatype 100tx-fd`

4. For most hosts, you can set full-duplex mode permanently, such as in the host’s `/etc/rc` files. Refer to the host’s documentation for more information.
About SERVER entries in the bp.conf file

On 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

Operations for a member of the Administrator’s group can fail with the following error, where command is a NetBackup administrator command:

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

To resolve a NetBackup Administration operations failure on Windows

1. Open the Local Security Policy.
2. Expand Local Policies > Security Options.
3. Disable the setting User Account Control: Run All administrators in Admin Approval Mode.

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.

Troubleshooting error messages in the NetBackup Administration Console

The following types of error messages can display in NetBackup.
<table>
<thead>
<tr>
<th>Error type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetBackup status codes and messages</td>
<td>The operations that are performed in the NetBackup Administration Console can result in the errors that are recognized in other parts of NetBackup. These errors usually appear exactly as documented in the NetBackup status codes and messages.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> A status code does not always accompany the error message.</td>
</tr>
<tr>
<td>NetBackup Administration Console: application server status codes and messages</td>
<td>These messages have status codes in the 500 range.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> A status code does not always accompany the error message.</td>
</tr>
<tr>
<td>Java exceptions</td>
<td>Either the Java APIs or NetBackup Administration APIs generate these exceptions. Java exceptions usually appear in one of the following places:</td>
</tr>
<tr>
<td></td>
<td>■ The status line of the NetBackup Administration Console</td>
</tr>
<tr>
<td></td>
<td>■ The log file that the jnbSA or jbpSA commands generate</td>
</tr>
</tbody>
</table>

**Extra disk space required for logs and temporary files for the NetBackup Administration Console**

The NetBackup Administration Console requires extra disk space to store logs and temporary files in the following locations.

■ On the host that is specified in the logon dialog box
■ In /usr/openv/netbackup/logs/user_ops
■ On the host where the console was started
■ In /usr/openv/netbackup/logs/user_ops/nbjlogs

If space is not available, you can experience the following issues:

■ Long waits for application response
■ Incomplete data
■ No response during logon
■ Reduced functionality in the NetBackup interface, for example, only the Backup, Archive, and Restore and Files System Analyzer nodes appear in the tree
■ Unexpected error messages:
■ "Cannot connect" socket errors during logon to the NBJava application server
Unable to logon to the NetBackup Administration Console after external CA configuration

Review the troubleshooting following scenarios.

For information on the external CA support in NetBackup, refer to the NetBackup Security and Encryption Guide.

Scenario

If the `vnetd` service is down on the host to which the NetBackup Administration Console is connecting

**Recommended action**

Check if the services are up on the host and try logging in again.

Scenario

If external certificate’s private key is not available or is in an incorrect format, error VRTS-28678 is displayed.

**Recommended action**

- Check if the path provided for the `ECA_PRIVATE_KEY_PATH` configuration option is valid (it should not be empty).
- Check if the path provided for `ECA_PRIVATE_KEY_PATH` is accessible and also if the private key file has required access permissions.
- Provide a valid private key and try logging in again.

In case of Windows certificate store, do the following:

- Run the `certlm.msc` command.
  
  In case `certlm.msc` is not working, you can access the Windows certificate store by running the `mmc.exe` command. Go to File > Add Remove Snap in.
- Open the certificate by double clicking it.
The certificate with private key should have a message stating that you have a private key corresponding to this certificate.

**Scenario**

If the external certificate is not present while you establish the trust with the NetBackup Administration Console.

**Recommended action**

- Check if the path provided for the `ECA_TRUST_STORE_PATH` configuration option is not empty.
- Check if the path provided for `ECA_TRUST_STORE_PATH` is accessible and also if the CA certificate file has required access permissions.
- Provide a valid external certificate and try logging in.

In case of Windows certificate store, do the following:

- Check if the root CA certificate is added in the Windows Cert Store’s Trusted Root Certificate Authorities.
- Run `certlm.msc` command. In the certificate management window, open the store named Trusted Root Certificate Authorities. The Trusted Root Certificate Authorities store contains all the self-signed certificates that are trusted by that machine.
  
  In case `certlm.msc` is not working, you can access the Windows certificate store by running `mmc.exe`. Go to File > Add Remove Snap in.

  - Select certificates from left hand side.
  - Click Add.
  - Select computer account. Click Next.
  - Click Finish and then OK.
  - Click Trusted Root Certification Authorities > Certificates.
  - Check if the root CA certificate in the certificate chain is present in the Trusted Root Certificate Authorities store.

  - If the root CA certificate is not present, do the following:
    - Click All Actions > Import.
    - Select .PEM or .CRT or .CER file of the certificate and click Import.
Note: All the certificates should be imported in the local machine store and not in the current user store. You can verify the current store in the certificate management window.

- Add a valid external CA certificate and try logging in.

Scenario

If an external CA-signed certificate is not present or not accessible, the following error is displayed:

The host does not have external CA-signed certificate. The certificate is mandatory to establish a secure connection.

Recommended action

- Check if the path provided for ECA_CERT_PATH in NetBackup configuration file is not empty.

- Check if the path provided for ECA_CERT_PATH points to the entire certificate chain.

- Check if the path provided for ECA_CERT_PATH is accessible and also if it has required access permissions.

- Provide a valid external CA-signed certificate and try logging in.

In case of Windows certificate store, do the following:

- Check if ECA_CERT_PATH contains the appropriate value: Windows Certificate Store Name\Issuer Name\Subject Name. Verify if the certificate exists in the Windows certificate store.

- Run the certlm.msc command.
  
  In case certlm.msc is not working, you can access the Windows certificate store by running the mmc.exe.
  
  File > Add Remove Snap in.

- Navigate to your certificate as per your input Windows Certificate Store Name\Issuer Name\Subject Name.

- Open your certificate by double-clicking it.

- Ensure that it is valid, has a private key, a correct issuer name, and a correct subject name.

  If you are using $hostname in Subject name, check that certificate subject has fully qualified domain name of the host.

  If this is not the case, either change the ECA_CERT_PATH or put the right certificate in Windows certificate store and then try logging in.
Scenario
Certificate revocation list (CRL) is not signed by a trusted authority.

Recommended action
This may occur at the time of login if the master server was configured to use NetBackup certificates and later it was enabled to use external certificates and vice versa. So the NetBackup Administration Console starts using the new CRL if you click Activity Monitor, locks the screen, tries to login again or in the periodic checks after every 1 hour, the certificate revocation status verification fails.

To fix this issue, you need to close the console and login again so that the peer host's certificate and the CRL are in sync.

If logging in again does not fix the issue then the reason can be the new CRL was not downloaded.

Run following command after correcting the CRL format:
UNIX: /usr/openv/netbackup/bin/nbcertcmd -updateCRLCache
Windows: install_path\Veritas\Netbackup\bin\nbcertcmd -updateCRLCache

Scenario
The revocation status of the host certificate cannot be verified using the CRL, because the CRL format is not valid.

Recommended action
This error can occur if a delta CRL is used.

NetBackup does not support delta CRLs, so you need to use non-delta CRLs.

Run following command after correcting the CRL format:
UNIX: /usr/openv/netbackup/bin/nbcertcmd -updateCRLCache
Windows: install_path\Veritas\Netbackup\bin\nbcertcmd -updateCRLCache

Scenario
The certificate of the host name is revoked.

Recommended action
If the certificate was revoked in error, reissue a certificate for the host.

If the certificate was revoked intentionally, a security breach may have occurred. Contact your security administrator.
Scenario
The Certificate Revocation List could not be downloaded. Therefore the certificate revocation status could not be verified.

Recommended action
The possible causes include the following:

- ECA_CRL_PATH is missing or has incorrect path.
- The CRL file is missing. The CRL file is corrupted.
- The CRL file could not be locked.
- The CRL file could not be unlocked.

For more information, see the bpjava logs.

Scenario
The Certificate Revocation List is not updated. Therefore the certificate revocation status could not be verified.

Recommended action
The possible causes include the following:

- The next update date / time of the CRL is older than the current system date / time.
- The CRL was valid at the time of login. The console was open and now the CRL has become invalid.

Ensure that the system time is correct.

In case the new CRL was not downloaded, run the following command

UNIX: /usr/openv/netbackup/bin/nbcertcmd -updateCRLCache

Windows: install_path\Veritas\Netbackup\bin\nbcertcmd -updateCRLCache

Scenario
Unable to connect to the NetBackup Web Management Console service.

Recommended action
The possible causes include the following:

- The NetBackup Web management Console service is down.
- ECA_CERT_PATH does not point to the entire certificate chain.
Troubleshooting file-based external certificate issues

This issue may occur because of one of the following reasons:

- The web service certificate that is used for communication is not configured properly.
- Some of the NetBackup core services have not started.
- The required prerequisites for external certificate are not met.
- External certificate configuration path (ECA_CERT_PATH) is not configured properly.
- Certificate revocation check failed.

To resolve the issue, review the following causes and run the following command to determine the current state of the problem.

```
Install_Path/bin/nbcertcmd -enrollCertificate -preCheck -server server_name
```

*Install_Path* refers to the following:

On Windows: VERITAS\NetBackup\bin

On Unix: /usr/openv/netbackup/bin

**Cause 1: The web server certificate that is used for communication is not configured properly.**

- The NetBackup web server is not configured to use external certificates.
  - The following error is displayed:
    - EXIT STATUS 26: client/server handshaking failed.
- Run the following command on the master server to check if external CA is configured (ON) or not (OFF).
  Install_Path/nbcertcmd -getSecConfig -caUsage
  On Windows: C:\Program Files\VERITAS\NetBackup\bin\nbcertcmd -getSecConfig -caUsage
  On Unix: /usr/openv/netbackup/bin/netbackup/bin/nbcertcmd -getSecConfig -caUsage
  For example: C:\Program Files\Veritas\NetBackup\bin>nbcertcmd -getSecConfig -caUsage
  Output:
  NBCA:OFF ECA:ON

  If an external CA is not configured, run the configureWebServerCerts command on the web server.
  In certain cases, you may also get the following error when an external CA is not configured on the web server.
  EXIT STATUS 5982: The certificate revocation list is unavailable.
  In this case, first check the value of the ECA parameter. If it is OFF, run the configureWebServerCerts command.

- The web service certificate that is used for communication is not trusted by a certificate authority.

- Check the certificate path (the configureWebServerCert -certPath option) must have a leaf certificate with the entire chain of CA certificates except the trust anchor (root CA).

- Run the following command to list the certificates that are configured for the web server.
  nbcertcmd -listallcertificates -jks
  On Windows: C:\Program Files\VERITAS\NetBackup\bin\nbcertcmd -listallcertificates -jks
  On Unix: /usr/openv/netbackup/bin/netbackup/bin/nbcertcmd -listallcertificates -jks

- Run the following command to list the host certificate details of the NetBackup master server.
  Install_Path/goodies/vxsslcmd x509 -in certificate_path -noout -text -purpose
  On Windows: C:\Program Files\VERITAS\NetBackup\bin\goodies\vxsslcmd x509 -in certificate_path -noout -text -purpose
On Unix: /usr/openv/netbackup/bin/netbackup/bin/goodies/vxsslcmd

x509 -in certificate_path -noout -text -purpose

Validate whether the host certificate of the master server is issued by the
same root CA as of the web server certificate.
If host certificate is not issued by the same root CA as of web server
certificate then issue new certificate with that CA for NetBackup Master
server and enroll certificate again.

- The specified server name was not found in the web service certificate.
The server name does not match any of the host names listed in the server's
certificate.
Names listed in the server's certificate are:
  DNS: nb-master _ext
  DNS: nb-master .some.domain.com
  DNS: nb-master _web_svr

EXIT STATUS 8509:
Either update the configuration on the NetBackup host so that it uses one of
the names that are present in the web server certificate to refer to the master server
or Include all names of the master server that are known to the NetBackup
domain in the certificate.

For more information, refer to the following article:

Cause 2
Some of the NetBackup core services have not started.

Carry out the following procedure to resolve the issue:
- Check the status of the following services by running the bpps command from
  the NetBackup/bin directory:
  - nbsl
  - vnetd -standalone
  - NB_dbsrv (on UNIX) or the dbsrv16 (on Windows)

For more details on the NetBackup commands, refer to the NetBackup
Commands Reference Guide.

- Start the nbsl and the vnetd services, if they are not running.
- Start the NB_dbsrv (on Unix) service or the dbsrv16 (on Windows) service, if it
  is not running.

Restart nbsl, vnetd, and NB_dbsrv (or dbsrv16) services as follows:

On Windows:
Alternatively, you may use the Service Control Manager to restart the NetBackup Service Layer (NBSL), NetBackup Legacy Network Service (vnetd), and SQLANYs_VERITAS_NB services.

For example:

C:\Program Files\Veritas\NetBackup\bin\bpdown -e "NetBackup Service Layer" -f -v
C:\Program Files\Veritas\NetBackup\bin\bpup -e "NetBackup Service Layer" -f -v
C:\Program Files\Veritas\NetBackup\bin\bpdown -e "NetBackup Legacy Network Service" -f -v
C:\Program Files\Veritas\NetBackup\bin\bpup -e "NetBackup Legacy Network Service" -f -v
C:\Program Files\Veritas\NetBackup\bin\bpdown -e "SQLANYs_VERITAS_NB" -f -v
C:\Program Files\Veritas\NetBackup\bin\bpup -e "SQLANYs_VERITAS_NB" -f -v

On Unix:

Install_Path/netbackup/bin/nbsl -terminate
Install_Path/netbackup/bin/nbsl

To stop vnetd and NB_dbsrv, refer to the following example:

To start vnetd and NB_dbsrv, run the following commands:

install_path/netbackup/bin/vnetd -standalone
install_path/db/bin/NB_dbsrv

For example:

/usr/openv/netbackup/bin/nbsl -terminate
/usr/openv/netbackup/bin/nbsl
# ps -fed | grep vnetd | grep standalone
root 16018 1 4 08:47:35 ? 0:01 ./vnetd -standalone
# kill 16018
# ps -fed |grep NB_dbsrv
root 11959 1 4 08:47:35 ? 0:01 ./NB_dbsrv
root 16174 16011 0 08:47:39 pts/2 0:00 grep ./NB_dbsrv
# kill 11959
/usr/openv/netbackup/bin/vnetd -standalone
/usr/openv/db/bin/NB_dbsrv

If the problem persists, contact the Technical Support team.

**Cause 3**

The required prerequisites for external certificate are not met.

Review the following prerequisites:

- Subject DN should be unique and stable for each host. It should have less than 255 characters and should not be empty.
- Only ASCII 7 characters are supported in the certificate subject DN and X509v3 Subject Alternative Name.
- Server and client authentication attributes (SSL server and SSL client) should be set (or should be true) in the certificate.
- Certificate is in **PEM** format.
- CRL distribution points (CDPs) are supported only for HTTP/HTTPS.

Run the following command to verify if the prerequisites are met.

```
Install_Path/goodies/vxsslcmd x509 -in certificate_path -noout -text -purpose
```

**Note:** The certificate paths that are provided for the configureWebServerCert -certPath option and the ECA_CERT_PATH option must have a leaf certificate with the entire chain of the CA certificates except the trust anchor (root CA).

Desirable conditions:

- Host name (**CLIENT_NAME**) that is used for certificate enrollment should be part of X509v3 Subject Alternative Name under DNS type.
- Common name (CN) of the subject name should not be empty.
Note: The following warning is generated when the `vxsslcmd` command is run and can be safely ignored:

```
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
```

### Cause 4

External certificate configuration path is not configured properly.

Ensure the following external certificate configuration options are configured properly:

- `ECA_CERT_PATH`
- `ECA_TRUST_STORE_PATH`
- `ECA_PRIVATE_KEY_PATH`
- `ECA_CRL_PATH`
- `ECA_CRL_CHECK`

Ensure the following:

- The peer host certificate has the CRL distribution point (CDP).
  If you have not specified `ECA_CRL_PATH`, NetBackup uses the CRLs on the URLs that are specified in the peer host certificate's CDP.
- `ECA_CRL_PATH` is not a volume ID path on Windows.

Run the following command and validate the external certificate configuration parameters.

**On UNIX:**

```
Install_Path/bin/nbgetconfig | grep ECA
```

**Windows:**

```
Install_Path/bin/nbgetconfig | findstr ECA
```

For more information about the configuration options, refer to the *NetBackup Security and Encryption Guide*.

### Cause 5

The requirements that are mentioned in **Cause 3** are not met.

- Host name (`CLIENT_NAME`) used for the certificate enrollment is not part of X509v3 Subject Alternative Name under the DNS type.
  If enrollment fails with this error, do one of the following:
  - Generate new certificate having host name in subject alternative name of the certificate.
Add or update (first delete and then add) the subject name of the certificate (RFC 2253 compliant) in the external certificate database on the master server.

Run the following command to add an entry for the host and the associated subject name in the NetBackup certificate database (only administrator can perform this operation):

```
Install_Path/bin/nbcertcmd -createECACertEntry -host host_name |-hostId host_id -subject subject name of external cert [-server master_server_name]
```

Alternatively, run the following command to delete an entry for the host and the associated subject name from the NetBackup certificate database and then add an entry using the -createECACertEntry command (only administrator can perform this operation):

```
Install_Path/bin/nbcertcmd -deleteECACertEntry -subject subject name of external cert [-server master_server_name]
```

Common name (CN) of the subject name is not present in the certificate.
If certificate enrollment fails with this error, do one of the following:

- Generate a new certificate with the common name in the certificate.
- Generate a new certificate with the host name in the subject alternative name of the certificate.
- Add host in the NetBackup host database and add an entry for the host and the associated subject name in the NetBackup certificate database.

Run the following command to add a host in the NetBackup host database (only administrator can perform this operation):

```
Install_Path/bin/admincmd/nbhostmgmt -addhost -host host_name |-hostId host_id [-server master_server_name]
```

Run the following command to add an entry for the host and the associated subject name in the NetBackup certificate database.

```
Install_Path/bin/nbcertcmd -createECACertEntry -host host_name |-hostId host_id -subject subject name of external cert [-server master_server_name]
```

Subject name of the external certificate should be RFC 2253 compliant.

**Cause 6**
Certificate revocation check failed.

External certificate enrollment can fail with the certificate revocation error for the following reasons:

- The external certificate is revoked.
The web server certificate is revoked.

CRL is unavailable on either the host or the master server.

See “Troubleshooting issues with external CA-signed certificate revocation” on page 67.

For more details on enrollment of external certificates in NetBackup, refer to the NetBackup Security and Encryption Guide.

Troubleshooting Windows certificate store issues

The web service certificate is issued by an unknown certificate authority when using Windows certificate store

Problem

The web service certificate cannot be trusted while enrolling the host certificate.

Cause

This issue is caused by one of the following:

- The web service certificate that is used for communication is not configured properly.
- The root certificate in the certificate chain of web service certificate is not present in the Trusted Root Certification Authorities of the Windows certificate store.

Solution

To resolve the issue, review the following causes and run the following command to determine the current state of the problem.

```
Install_Path/bin/ nbcertcmd -enrollCertificate -preCheck -server server_name
```

*Install_Path* refers to the following:

- On Windows: VERITAS\NetBackup\bin
- On Unix: /usr/openv/netbackup/bin

Solution for the cause: The web service certificate that is used for communication is not configured properly

Check if web server is configured with valid certificate along with its CA certificates.

- Run the following command to list the certificates that are configured for the web server.

```
Install_Path/nbcertcmd -listallcertificates -jks
```

On Windows:

C:\Program Files\ VERITAS\NetBackup\bin\nbcertcmd -listallcertificates -jks

On Unix:

/usr/openv/netbackup/bin/netbackup/bin/nbcertcmd -listallcertificates -jks

- Ensure that all the certificates in the chain (except the root CA certificate) are present in the jks.

Check the following parameters in the nbcertcmd -listallcertificates -jks output.

- Alias name: eca

- Entry type: PrivateKeyEntry

If they are not present, add the CA chain in the end of the entity certificate file that is the web service certificate file. The web service certificate should be at the top, its issuer CA certificate is below that, issuer of that CA certificate is below that, and so on.

If the certificate chain has only two certificates (root certificate and web service certificate), the certificate file has only one certificate that is the web service certificate.

Run the configureWebServerCerts command.

Solution for the cause: The root certificate in the certificate chain of the web service certificate is not present in the Windows certificate store

- Run the certlm.msc command.

  In the certificate management window, open the store named Trusted Root Certificate Authorities.

  The Trusted Root Certificate Authorities store contains all the self-signed certificates that are trusted by that machine.

  In case certlm.msc does not work, you can access the Windows certificate store by running the mmc.exe command.

  File > Add Remove Snap in.

  Select the certificates from the left side.

  Click Add.

  Select the Computer account.

  Click Next > Finish > OK.

  Click Trusted Root Certification Authorities > Certificates.

  Check if the root CA certificate in the certificate chain used to configure the web service is present in the Trusted Root Certificate Authorities store.
If the root CA certificate is not present, click **All Actions > Import**, select .PEM / .CRT / .CER file of the certificate and click **Import**. All the certificates should be imported in the local machine store and not in the current user store.

You can verify the current store in the certificate management window.

### Problem
Certificate's public key algorithm is not supported.

The public key algorithm is not supported by NetBackup. Currently only the RSA algorithm is supported.

### Cause
The certificate with given path exists in windows cert store but its signature algorithm is not supported.

### Solution
You need to use the certificate with public key algorithm that is supported by NetBackup.

For more details on enrollment of external certificates in NetBackup, refer to the *NetBackup Security and Encryption Guide*.

### Problem
Private key for the given certificate is not available.

The certificate in specified by the path does not have a corresponding private key imported in Windows certificate store.

### Cause
This is typically caused by importing a .crt, .cer, or .pem certificate manually in the Windows certificate store instead of .pfx.

### Solution
Ensure that the certificate has its private key imported.

- Run the `certlm.msc` command.
  - In case `certlm.msc` does not work, you can access the Windows certificate store by running the `mmc.exe` command.
  - **File > Add Remove Snap in**
- Navigate to your certificate.
- Open your certificate by double-clicking it.
The certificate with the private key should have a message stating that you have a private key corresponding to this certificate.

- If certificate is to be manually enrolled, import a .pfx file and not just the .cer or .crt file.

For more details on enrollment of external certificates in NetBackup, refer to the *NetBackup Security and Encryption Guide*.

**Problem**

Certificate with the given subject name is not found

Could not find the certificate when a special keyword $hostname is used in ECA_CERT_PATH

**Cause**

The certificate does not exist in the local machine store for the given ECA_CERT_PATH.

One of the attributes from store name, issuer name, or subject name does not match the one in the local machine store.

**Solution**

- Check if the certificate exists in the local machines store. Do the following:
  - Run the certlm.msc command.
    - In case certlm.msc does not work, you can access the Windows certificate store by running the mmc.exe command.
    - File > Add Remove Snap in.
  - Check if the certificate exist

- Verify that the following criteria are satisfied:
  - Certificate location is a path or comma separated paths where each path is specified using store name, issuer name and subject name separated by (/) slash.
  - Store name must exactly match the store your certificate is in.
  - Issuer name and subject name should always be part of ECA_CERT_PATH. If nothing is specified for issuer name, it means any issuer can be considered.
  - $hostname is special keyword and can be used in subject name. When finding the certificate $hostname is replaced with actual FQDN of the host.
  - When using $hostname, the certificate must have FQDN as a part of CN.
  - Double quotes to be used in case the backward slash (/) is present in the actual Store name, Issuer name or Subject name.
Though the subject name is always part of `ECA_CERT_PATH`, `CN=example`.

CN is not allowed.

The subject in `ECA_CERT_PATH` should be any sub-string of actual CN, OU, O, L, S, C and so on.

For more details on enrollment of external certificates in NetBackup, refer to the `NetBackup Security and Encryption Guide`.

**Troubleshooting backup failures**

**Problem**

Backup fails with the following peer host validation error: Certificate operation failed because NetBackup CA certificates cannot be used for host communication in the domain.

**Cause**

Possible reasons for the failure are:

- The master server (web server) is configured to use only external CA-signed certificates, but the media server or the clients are not configured to use external certificates. Their external certificates are not enrolled with the master server domain.

- The master server (web server) is configured to use only external CA-signed certificates, but the media server or the clients are still not upgraded to 8.2 or later.

**Solution**

- Check the master server certificate authority (CA) configuration using the `nbcertcmd -getsecconfig -caUsage` command, the NetBackup Administration Console, or the NetBackup Web UI.

  If the web server is configured to use only external certificates, do the following:

- Identify the two hosts for which the communication fails.

- Check if any of the two hosts is 8.2 or later, but is not configured to use external certificates.

  If it is true, enroll an external certificate for the host with the master server domain.

- Check if any of the two hosts is 8.1.x.

  If it is true, upgrade the host to 8.2 or later and enroll an external certificate for the host with the master server domain or configure the web server to use both external and NetBackup certificates.
Troubleshooting backup failure issues with NAT clients or NAT servers

Backup fails with the following error: bpbrm (pid=31553) cannot send mail because BPCD on host exited with status 21: socket open failed

This issue may occur because of one of the following reasons:

- Media server cannot connect to the NetBackup Messaging Broker (or nbmqbroker) service.
- The nbmqbroker service may not be up and running on the master server.
- The NAT client is not configured to accept the reverse connection.
- The client is not a NAT client.
- The client is 8.1.2 or earlier.
- Port configuration for the nbmqbroker service is updated.
- The master server services are restarted.

**Cause 1**
Media server cannot connect to the nbmqbroker service.

**Cause 2**
The nbmqbroker service may not be up and running on the master server.

Cause 1 and Cause 2 have the same solution as follows:

- Check the bpbrm logs on the media server at Install_Path/logs/bpbrm.
- Check the nbmqbroker log file at:
  UNIX: /usr/openv/mqbroker/logs
  Windows: Install_Path/mqbroker/logs
- Ensure that the nbmqbroker service is running on the master server. Use the following commands:
  - Run the bppms command.
Run the `bptestbpcd -host hostname` command from the master or media server and check the admin logs at `Install_Path/logs/admin`.

**Cause 3: The NAT client or NAT server is not configured to accept the reverse connection**

Do the following:

- Check the subscriber logs at:
  - UNIX: `usr/openv/logs/nbsubscriber`
  - Windows: `Install_Path/logs/nbsubscriber`
- Check the `vnetd` logs at `Install_Path/logs/vnetd`.
- Run the `bptestbpcd -host hostname` command on the master or media server and check the admin logs at `Install_Path/logs/admin`.
- Run the `nbmqutil -publish -master hostname -message message_text -remoteHost hostname` command.
- Ensure that the `ACCEPT_REVERSE_CONNECTION` configuration option is set to `TRUE` using the `nbgetconfig` command.
- Check the subscriber service is running on the NAT client by running the `bpps` command.

**Cause 4: The client is not a NAT client**

Do the following:

Ensure that the `ENABLE_DIRECT_CONNECTION` configuration option is set to `TRUE` on the master or media server using the `nbgetconfig` command.

**Cause 5: The client is 8.1.2 or earlier**

Do the following:

Ensure that the `ENABLE_DIRECT_CONNECTION` configuration option is set to `TRUE` on the master or media server using the `nbgetconfig` command.

**Cause 6: Port configuration for the nbmqbroker service is updated**

Do the following:

- Wait until the cache is cleared.
- Clear host cache on the media server using the `bpclntcmd -clear_host_cache` command.
Cause 7: The master server services are restarted

Do the following:

- Check the subscriber service logs at:
  - UNIX: /usr/openv/logs/nbsubscriber
  - Windows: Install_Path/logs/nbsubscriber
- Wait until the subscriber service starts on the client.
- Restart the subscriber service.

Backup fails with the following error: bpbrm (pid=9880) bpcd on host exited with status 48: client hostname could not be found

This issue may occur because of one of the following reasons:

- The NAT client's host name is not mapped to it's host ID.
- Host ID that is associated with the client is null or is not valid.

Do the following:

- Check the bpbrm logs at Install_Path/logs/bpbrm
- Check the existing host ID-to-host name mapping of the client by running the
  `Install_Path/bin/admincmd/nbhostmgmt -li -json` command on the master or media server.
- If the client name is not mapped to the host ID, add a new name for the client and map it to existing host ID using the
  `Install_Path/bin/admincmd/nbhostmgmt -add -hostid hostid -mappingname hostname` command.
- Clear host cache on the client using `Install_Path/bin/bpclntcmd -clear_host_cache`.

Backup takes too long to complete

This issue may occur because of one of the following reasons:

- Client's configuration file (bp.conf file on UNIX or Windows registry) contains wrong media server entry.
- The `ENABLE_DATA_CHANNEL_ENCRYPTION` option is not set to FALSE on the NAT host.

Cause 1: Client's configuration file contains wrong media server entry

Do the following:
Troubleshooting procedures

Troubleshooting backup failure issues with NAT clients or NAT servers

- Run the the `Install_Path/bin/admincmd/bptestbpcd -host hostname` from the master or media server and check the admin logs at `Install_Path/logs/admin`.

- Add the media server name in the `/etc/hosts` file on the client.

- Add the media server name in the configuration file on the client using the `nbsetconfig` command.

**Cause 2: The `ENABLE_DATA_CHANNEL_ENCRYPTION` option is enabled**

Do the following:

- Set the `ENABLE_DATA_CHANNEL_ENCRYPTION` to `FALSE` using the `nbsetconfig` command.

**Backup fails as the job is hung and no new job is triggered for the policy**

This issue may occur because of the following reason:

- The NAT host awaits an incoming message, but the `nbmqbroker` service has closed the client connection, and client cannot detect the closed connection.

Do the following:

- Check the client logs to see if it contains the following message:

  ```
  Trying to get Message from MQ Broker:[master server name]
  ```

- Check the current heartbeat value that is set for the `SUBSCRIBER_HEARTBEAT_TIMEOUT` configuration option on the server. Use the `nbgetconfig` command.

- Set the `SUBSCRIBER_HEARTBEAT_TIMEOUT` option value to minimum so that the client can detect a closed connection.

- Restart the subscriber service on the client.

**Backup or restore jobs fail after `CLIENT_CONNECT_TIMEOUT`**

This issue may occur because of the following reason:

- Subscriber was not able to establish the reverse connection with media server.

- Message is delivered by publisher but subscriber did not receive the message.

Do the following:

- Check the subscriber service logs to ensure that the subscriber service is able to connect to the PBX Transient ID.
Check the subscriber service logs to ensure that the publisher message is
delivered to the subscriber.
Log message:

Got Message from MQ Broker: [<message>] with return: <status code> total timeout, reset: <timeout reset>

Status of NAT media server is down after the services are restarted
Do the following:

1. Run the following command on the master server:
   
   `Install_Path/bin/admincmd/bptestbpcd -host host_name`

2. Check the logs at `Install_Path/logs/admin`.

3. Check if the media server is offline using the NetBackup Administration
   Console. Go to Media and Device Management > Devices > Media Servers.

4. If the master server service is restarted, restart the media server and wait for
   the media server to be online.

5. Check if the subscriber logs of the media server are ready to receive connection
   messages if the log level is set to a value greater than 1. For example:

   - Log message for the disconnected state: Retrying connection stopped
     for n seconds with attempt: m
   - Log message for the connected state: Successfully connected to MQ
     Broker: master server host with Host UUID NAT host ID

Troubleshooting issues with the NetBackup Messaging Broker (or nbmqbroker) service

The NetBackup Messaging Broker service is not running
Do the following:

- Ensure that the service is configured and started on the master server. To
  configure the service, run the `configureMQ` command.
  Refer to the NetBackup Commands Reference Guide.

The NetBackup Messaging Broker service is not able to start
Reasons:

- Ports that are configured for the service is in use by some other process.
The configuration file is corrupted.

Do the following:
1. Check the `configureMQ` command logs for failure.
2. Check the `nbmqbroker` service logs for failure.
3. Run the `configureMQ` command.

Refer to the NetBackup Commands Reference Guide.

The NetBackup Messaging Broker service is not connected to the NAT client

Reasons:
- The port configured for the service is not available for use.
- Connection fails with some SSL exception.
- The `nbmqbroker` service is not restarted after the `configureWebServerCerts` command is run on the master server.

Do the following:
1. Ensure that the port configured for the `nbmqbroker` service is available for use and accessible by NetBackup hosts.
2. Check the connectivity between the master server and the NAT client using the `nbcertcmd -ping` command.
   - If the command is not successfully executed, refer to the troubleshooting section for the NetBackup web service.
   - If the command is successfully executed, run `configureMQ` command to configure the `nbmqbroker` service.
3. Restart the `nbmqbroker` service.

Subscriber or publisher is not able to connect to the NetBackup Messaging Broker service

Reasons:
- The JSON web token (JWT) for the NAT client cannot be refreshed.
- The security certificate of the NAT client is revoked.
- The NetBackup Web Management Console (or `nbwmc`) service is not running.

Do the following:
1. Refer to the subscriber troubleshooting steps.
2. If the client's security certificate is revoked, reissue the certificate.
3. Start the nbwmc service.

The NetBackup Messaging Broker service is not able to start after disaster recovery

Reasons:
- The disaster recovery package is lost.
- The configureMQ command is not run after the disaster recovery (DR) installation.

Do the following:
- Run the configureMQ or configureMQ -defaultPorts command.
  Refer to the NetBackup Commands Reference Guide.

The NetBackup Messaging Broker service fails to start on Windows if the 8dot3 short file name setting is disabled on the volume where NetBackup is installed

To check if the installation root folder has the 8dot3 file name setting enabled, run the following command from your folder:

```
>dir /x
```

Example: The ‘Program Files’ directory has the 8dot3 file name setting enabled, therefore the short name ‘PROGRA~1’ is generated.

But it differs for the ‘not8 Dot3’ directory.

```
C:\>dir /x
```

The volume in drive C has no label.
The Volume Serial Number is FE21-2F8E

Directory of C:\

```
-5.6.3

12/06/2019  02:24 PM    <DIR>    not8 Dot3
12/02/2019  06:35 AM    <DIR>    PROGRA~1    Program Files
12/02/2019  10:44 AM    <DIR>    PROGRA~2    Program Files (x86)
```
Do the following to resolve the issue:

1. Enable 8dot3 name file setting for the NetBackup installation root folder using the `fsutil` command.
   
   Refer to the following article: Fsutil 8dot3name

2. If the problem persists, contact Technical Support.

The NetBackup Messaging Broker service behaves incorrectly after restoring the disaster recovery package in case of external CA setup

Consider the following scenario:

NetBackup is configured to use only external CA-singed certificates at the time of catalog backup. Therefore, the disaster recovery package that was created during catalog backup contains the required external certificates. If the host identity is recovered using such disaster recovery package after NetBackup installation, the `nbmqbroker` service may behave incorrectly because of the NetBackup CA-signed certificates that were issued during installation.
To resolve the issue

1. Verify if your the NetBackup environment uses only external CA-signed certificates. Run the following command:

   `nbcertcmd -getSecConfig -caUsage`

2. Check the certificates that the `nbmqbroker` service uses. Run the following command:

   **On Unix:**
   ```
   cat /usr/openv/var/global/mqbroker/mqbroker.config | grep ssl_options
   ```

   **On windows:**
   ```
   type "NetBackup_Install_path\var\global\mqbroker\mqbroker.config" | findstr "ssl_options"
   ```

   If only external CA-signed certificates are used in your environment, the command shows the path with `externalcacreds` entry.

   If the command shows the path with `nbcacreds` entry, NetBackup CA-signed certificates are used.

   For example:

   ```
   {ssl_options, [{cacertfile, "/usr/openv/var/global/mqbroker/certstore/nbcacreds/ca.pem"}],
   {ssl_options, [{cacertfile, "/usr/openv/var/global/mqbroker/certstore/nbcacreds/ca.pem"}],
   ```

   You need to remove the NetBackup certificates so that the `nbmqbroker` service works appropriately.

3. Run the following command to remove the NetBackup certificates:

   `configureWebServerCerts -removeNBCert`
4 Restart the NetBackup Web Management Console (`nbwmc`) service and the `nbqmbroker` service to reflect the changes.

5 Check the certificates that the `nbqmbroker` service uses. Run the following command:

   On Unix: `cat /usr/openv/var/global/mqbroker/mqbroker.config | grep ssl_options`

   On windows: `type "NetBackup_Install_path\var\global\mqbroker\mqbroker.config" | findstr "ssl_options"

Expected output for external certificate only mode:

   `{ssl_options, [{cacertfile, "/usr/openv/var/global/mqbroker/certstore/externalcacreds/ca.pem"}],
    {ssl_options, [{cacertfile, "/usr/openv/var/global/mqbroker/certstore/externalcacreds/ca.pem"}],

See “Restoring disaster recovery package on UNIX” on page 222.
See “Restoring disaster recovery package on Windows” on page 219.

**Issues with email notifications for Windows systems**

If email notifications to the backup administrator or the host administrator are not received, verify the following items:

- The email addresses are configured correctly.
- The BLAT binary is valid and compatible with the email system. Download the latest version.
- The correct BLAT syntax is used in the script.
- In the `nbmail.cmd` script, make sure that the BLAT command is not commented out.
- If the `blat.exe` command is not in the `\system32` directory, make sure that the path to `blat.exe` is specified in `nbmail.cmd` script.
- If the system experiences delays, you can use the `-ti n` timeout parameter.
- The email account is valid on the mail server.
- If the mail server requires authentication for SMTP, make sure that the account that is used for the NetBackup client process is authorized. The default account is the Local System.
Issues with KMS configuration

Backups fail on KMS-enabled storage after KMS configuration

NetBackup supports NetBackup Key Management Service (NetBackup KMS) and external key management service (external KMS).

This section provides procedures to resolve the backup failure issue in the following scenarios:

- When NetBackup KMS is configured
- When external KMS is configured

See the NetBackup Security and Encryption Guide for more information about KMS configurations.

To resolve backup failure issue in a setup where NetBackup KMS is configured

1. If a NetBackup policy is configured to use tape, AdvanceDisk or cloud storage, check job details. If you see any errors, refer to the NetBackup Status Codes Reference Guide.

   For example in case of tape storage type, you may see the following error in the job details tab:

   Mar 27, 2020 5:20:40 PM - Error bptm (pid=11143) KMS failed with error status: Error details : Error Code : 1298, Error Message : Cannot communicate with one or more key management servers., Server - example.master.com:0, Error code - 25,

   Mar 27, 2020 5:20:40 PM - Info bptm (pid=11143) EXITING with status 83 <----------

   Mar 27, 2020 5:20:43 PM - Info bpbkar (pid=11132) done. status: 83: media open error

2. Run the following command on the master server to verify whether NetBackup KMS is configured or not:

   ```
   Install_Path/bin/nbkmscmd -listKMSConfig -name nbkms
   ```

   If NetBackup KMS configuration is not listed, check if the `nbkms` service is running or not.

   - If the `nbkms` service is running, run the following command to add the `nbkms` service configuration:
     ```
     Install_Path/bin/nbkmscmd -discoverNBkms
     ```
   - If `nbkms` service is not running check `nbkms` logs at the following location:
     On UNIX - `/usr/openv/logs/nbkms`
     On Windows - `Install_Path\NetBackup\logs\nbkms`

   Check if a key is created on the KMS server with the required key group.
3 Validate the NetBackup KMS configuration using the following command:

```
Install_Path/bin/nbkmscmd -validateKMSConfig -name KMS_configuration_name
```

4 Check if at least one active key is listed using the following command:

```
Install_Path/bin/nbkmscmd -listKeys -name KMS_configuration_name -keyGroupName key_group_name
```

5 If key is not listed, create a key with the required key group and clear the cache on the media server. Run the following command:

```
Install_Path/bin/bpclntcmd -clear_host_cache
```

6 Check the following logs for further details:

- In case of tape, AdvanceDisk, and cloud storage:
  
  ```
  Install_Path/netbackup/logs/bptm
  ```

- In case of MSDP and cloud catalyst storage:
  
  ```
  MSDP_config_path/log/spoold/spoold.log
  ```

- For web service logs on the master server:
  
  ```
  Install_path/logs/nbwebservice/<51216-495-***-***-***-***.log>
  ```

- For nbkmsiputil logs for NetBackup KMS:  
  ```
  Install_Path/logs/nbkms
  ```

To resolve backup failure issue in a setup where external KMS is configured

1 If a NetBackup policy is configured to use tape, AdvanceDisk or cloud storage, check job details. If you see any errors, refer to the NetBackup Status Codes Reference Guide.

2 Run the following command on the master server to verify whether external KMS is configured or not:

```
Install_Path/bin/nbkmscmd -listKMSConfig -name KMS_configuration_name
```

If configuration is not listed, configure external KMS server.

3 Validate the external KMS configuration using the following command:

```
Install_Path/bin/nbkmscmd -validateKMSConfig -name KMS_configuration_name
```
4 Run the following command if certificate files exist on the master server.

```
Install_Path/netbackup/bin/goodies/nbkmiputil -validate -kmsServer
kms_server_name -port 5696 -certPath certificate_file_path
-privateKeyPath private_key_file_path -trustStorePath
ca_file_path
```

The output is in a JSON format.

5 Check if key is created on external KMS server with the required key group.

6 Check if at least one active key is listed using the following command:

```
Install_Path/bin/nbkmscmd -listKeys -name KMS_configuration_name
-keyGroupName key_group_name
```

If key is not listed, create a key with the required key group and clear the cache on the media server. Run the following command:

```
Install_Path/bin/bpclntcmd -clear_host_cache
```

7 Check the following logs for further details:

In case of tape, AdvanceDisk, and cloud storage:
```
Install_Path/netbackup/logs/bptm
```

In case of MSDP and cloud catalyst storage:
```
PDDE_Install_Path/log/spoold/spoold.log
```

For web service logs on the master server:
```
Install_Path/logs/nbwebservice/<51216-495-***-***-***.log>
```

For nbkmiputil logs for external KMS:
```
Install_Path/netbackup/logs/nbkmiputil
```

**Restore of the backup data of a KMS-enabled storage fails**

Use the following procedure to resolve the restore failure issue in case of a storage that is KMS enabled:

**To resolve restore failure issue**

1 In case of tape, AdvanceDisk, and cloud storage, check job details.

2 Validate the KMS configuration using the following commands:

```
Install_Path/bin/nbkmscmd -validateKMSConfig -name
KMS_configuration_name
```
3 Run the following command if certificate files exist on master server,

```
Install_Path/netbackup/bin/goodies/nbkmiputil -validate -kmsServer KMS_server_name -port 5696 -certPath certificate_file_path
-privateKeyPath private_key_file_path -trustStorePath ca_file_path
```

The output is displayed in the JSON format.

4 Ensure that the key with which backup is encrypted is still active on the KMS server.

See the following error in nbwebservice logs to get the key tag that is required for restore.

See the following log statements in the web service logs on the master server:

```
Install_path/logs/nbwebservice/<51216-495-***-***-***.log>
```

Here are the log snippets:

```
[com.netbackup.config.PeerInfoPopulatorFilter]
Request URL : https://<Master-Server>:1556/netbackup/security/key-management-services/keys
Connection Info :ConnectionInfo

[com.netbackup.security.kms.resource.KMSConfigResource]
HTTP GET filter query string is : KeyId eq 'bdc3492b015d4a9ab25426465b12adc6a834d6c6b449c49092'
and kadlen eq 32

[com.netbackup.security.kms.resource.KMSConfigResource]
com.netbackup.security.kms.resource.KMSConfigResource getKeys() - NBKMSRecordNotFoundException occurred due to missing KMS record.com.netbackup.nbkms.exception.NBKMSRecordNotFoundException: security.error.kms.KeyRecordNotFound
```

5 Check the following logs for further details:

For tape, AdvanceDisk, and cloud storage:

```
Install_Path/netbackup/logs/bptm
```

For MSDP and cloud catalyst storage:

```
PDDE_Install_Path/log/spoold/spoold.log
```

For web service logs on master server:

```
Install_Path/logs/nbwebservice/<51216-495-***-***-***.log>
```

For nbkmiputil logs:

- For NetBackup KMS,```Install_Path/logs/nbkms```
Issues with initiating the NetBackup CA migration because of large key size

Initiating the NetBackup CA migration may be timed out during installation or upgrade because of large key size.

Following is an example of the error that is logged in the installation logs:


06-19-2020, 20:40:39 : NetBackup security service is still generating key pairs with key size of 16384 bits.

06-19-2020, 20:40:39 : NetBackup will recheck the status of the NetBackup CA migration initiation phase after every 30 seconds.

06-19-2020, 20:40:40 : The NetBackup CA migration initiation process is taking more time than expected.

06-19-2020, 20:40:40 : Failed to set up the new NetBackup CA.


06-19-2020, 20:40:40 : "C:\Program Files\Veritas\NetBackup\bin\admincmd \nbseccmd.exe" -nbcamigrate -initiatemigration -quiet -keysize 16384 -reason "Upgrade" -installtime, ERROR: nbseccmd.exe failed with error status: 41

In case of such an error, it is possible that the CA migration was successfully initiated but the request is timed out because of the large key size. However, in the background the CA migration initiation may be complete and the certificates may be renewed with the new CA.

To verify if the initiation of NetBackup CA migration was successful:

1. Run the following command:

   \nbseccmd -nbcaMigrate -summary

2. Check if the NetBackup CA migration status is INITIATED.

   - If the migration status is NO_MIGRATION, it implies that the CA migration has failed during installation.
     Initiate a new migration using the following command:
nbseccmd -nbcaMigrate -initiateMigration | -i -keysiz <key-value> [-reason <comment>] [-json] [-quiet]

3 Once you have ensured that the migration status is INITIATED, run the following command to verify if the new CA is displayed in the list:

```
nbseccmd -nbcalist
```

- If the new CA is present in the list, it implies that the migration is successfully initiated.

- If the new CA is not present in the list, run the following command:

```
nbseccmd -nbcaMigrate -syncMigrationDB
```

4 If the certificates are still not updated, contact Veritas Technical Support.
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 nbcplogs utility
- About the robotic test utilities

About NetBackup troubleshooting utilities

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

<table>
<thead>
<tr>
<th>Table 3-1</th>
<th>Troubleshooting utilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utility</td>
<td>Description</td>
</tr>
<tr>
<td>Analysis utilities for NetBackup debug logs</td>
<td>They enhance NetBackup’s existing debug capabilities by providing a consolidated view of a job debug log. See “About the analysis utilities for NetBackup debug logs” on page 161.</td>
</tr>
<tr>
<td>Utility</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Logging Assistant | It simplifies the gathering of evidence for support cases. For more information, see the following:  
  - The NetBackup Logging Assistant FAQ: [http://www.veritas.com/docs/000088104](http://www.veritas.com/docs/000088104) |
| Network troubleshooting utilities | They verify various aspects of the network configuration inside and outside NetBackup to ensure that there is no misconfiguration. See “About network troubleshooting utilities” on page 166. |
| NetBackup support utility (nbsu) | It queries the host and gathers appropriate diagnostic information about NetBackup and the operating system. See “About the NetBackup support utility (nbsu)” on page 167. |
| NetBackup consistency check utility (NBCC) | It analyzes the integrity of portions of the NetBackup configuration and catalog and database information as they pertain to tape media. See “About the NetBackup consistency check utility (NBCC)” on page 171. |
| NetBackup consistency check repair (NBCCR) utility | It processes database-catalog repair actions and automates the application of approved suggested repair actions. See “About the NetBackup consistency check repair (NBCCR) utility” on page 179. |
| nbcplogs utility | It simplifies the gathering of logs to deliver to Veritas technical support. See “About the nbcplogs utility” on page 182. |
| Robotic test utilities | They communicate directly with robotic peripherals. See “About the robotic test utilities” on page 183. |

### 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>
<thead>
<tr>
<th>Utility</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backupdbtrace</td>
<td>Consolidates the debug log messages for specified NetBackup database backup jobs and writes them to standard output. It sorts the messages by time. backupdbtrace attempts to compensate for time zone changes and clock drift between remote servers and clients. At a minimum, you must enable debug logging for admin on the master server, and for bptm and bpbkar on the media server. For best results, set the verbose logging level to 5 and enable debug logging for the following: bpdbm on the master server and bpcd on all servers in addition to the processes already identified. A complete description of backupdbtrace is in the NetBackup Commands Reference Guide.</td>
</tr>
</tbody>
</table>
### Analysis utilities for NetBackup debug logs (continued)

<table>
<thead>
<tr>
<th>Utility</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backuptrace</td>
<td>Copies to standard output the debug log lines relevant to the specified backup jobs, including online (hot) catalog backups. 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. 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. A complete description of <code>backuptrace</code> is in the NetBackup Commands Reference Guide.</td>
</tr>
<tr>
<td>bpgetdebuglog</td>
<td>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. <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. A complete description of <code>bpgetdebuglog</code> is in the NetBackup Commands Reference Guide.</td>
</tr>
<tr>
<td>duplicatetrace</td>
<td>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. 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. A complete description of <code>duplicatetrace</code> is in the NetBackup Commands Reference Guide.</td>
</tr>
</tbody>
</table>
Table 3-2  Analysis utilities for NetBackup debug logs (continued)

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

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, nbpm, nbjm, nbrb, bpdbm, bpbrm, bptm, bpdf, and bpcd.

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

daystamp.millisecs.program.sequence machine log_line

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

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

---

**About the Logging Assistant**

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

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


- *About the Logging Assistant:*
  http://www.veritas.com/docs/000088104
# 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`; the settings they verify include connection methods and CORBA endpoint selection.

## Table 3-3  
Network troubleshooting utilities

<table>
<thead>
<tr>
<th>Utility</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bptestbpcd</code></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>A complete description of <code>bptestbpcd</code> is in the NetBackup Commands Reference Guide.</td>
</tr>
<tr>
<td><code>bptestnetconn</code></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>A complete description of <code>bptestnetconn</code> is in the NetBackup Commands Reference Guide.</td>
</tr>
<tr>
<td><code>nbdna</code> (NetBackup Domain Network Analyzer)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>A complete description of <code>nbdna</code> is in the NetBackup Commands Reference Guide.</td>
</tr>
</tbody>
</table>
About the NetBackup support utility (nbsu)

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

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

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

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

---

**Note:** The NetBackup support utility (nbsu) has been updated in NetBackup 8.1.1. The previous version of nbsu (renamed old_nbsu) is deprecated and will be removed in a future NetBackup release. Veritas recommends use of the newer version (nbsu).

Veritas 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 Veritas 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 Veritas Technical Support, see the NetBackup Commands Reference Guide.
  
  If you have a case ID from Technical Support of the form #######, rename the log files with the case ID number. Then manually upload the files to the Veritas Evidence Server. For additional assistance, see:
  
  http://www.veritas.com/docs/000097935

- 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 -g command line option to collect only OS and NET commands.

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. Note the following alternate ways to view nbsu error messages:

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

  Enter the following:
  - Windows
    
    ```
    install_path\NetBackup\bin\support\nbsu.exe 2>&1
    ```
  - UNIX
    
    ```
    /usr/openv/netbackup/bin/support/nbsu 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 STDOUT.

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

  - The general flow of the nbsu program
  - 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)

By default, the `nbsu` command creates the output as a compressed file in the same directory where the `nbsu` executable is located. The format of the command output is:

```
NBSU_hostname_role_mmddyyyy_timestamp.extension
```

For example:

- **UNIX/Linux**: `NBSU_mylinuxvm_master_11072017_152100.tgz`
- **Windows**: `NBSU_mywindowsvm_master_11072017_152100.cab`

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 is an example of part of the `nbsu` output file for the `bpgetconfig` command. The STDERR is shown as the output of the command and is captured in the output file. Exit status is outputted into the output file as follows:

```
<exit status code>
```

```
#####Command used:
/usr/openv/netbackup/bin/admincmd/bpgetconfig -g sivbl17.domain.com -L#####
Client/Master = Master
NetBackup Client Platform = Linux, RedHat2.6.18
NetBackup Client Protocol Level = 8.1.0
Product = NetBackup
Version Name = 8.1
Version Number = 810000
NetBackup Installation Path = /usr/openv/netbackup/bin
Client OS/Release = Linux 3.10.0-229.el7.x86_64

Exit status: 0
```

```
#####Command used: /usr/openv/netbackup/bin/admincmd/bpgetconfig###
SERVER = sivbl17.domain.com
```
WEB_SERVER_CONNECTION_TIMEOUT = 30
WEB_SERVER_TUNNEL_USE = AUTO
WEB_SERVER_TUNNEL_ENABLED = YES
WEB_SERVER_TUNNEL
TRUSTED_MASTER
KNOWN_MASTER
MASTER_OF_MASTERS
USEMAIL =
BPBACKUP_POLICY = any
BPBACKUP_SCHED = any

Exit status: 0

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

An example of a compressed archive file that \texttt{nbsu} created is as follows:

\texttt{/usr/openv/netbackup/bin/support/NBSU\_host1\_master\_01172018\_220505.tgz}

where host1 is the name of the host on which \texttt{nbsu} ran, and master indicates that the host is a NetBackup master server. The date is embedded in the file name in the \texttt{mmddyyyy} format.

\texttt{nbsu} supports tar for archive and gzip for compression.

A complete description of \texttt{nbsu} is in the \textbf{NetBackup Commands Reference Guide}.

\section*{Example of a progress display for the NetBackup support utility (nbsu)}

By default, the NetBackup support utility (\texttt{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:

\texttt{NBU\ Install\ path: \texttt{C:\Program\ Files\Veritas}\nmywindowsvm\ is\ a\ master\ server\nCollecting NBU\_adv\_disk\ info\nCollecting NBU\_all\_log\_entries\ info\nCollecting NBU\_altnames\ info\nCollecting NBU\_auth\_methods\_names\ info\nCollecting NBU\_available\_media\ info\nCollecting NBU\_backup\_status\ info\nCollecting NBU\_bpclient\ info}. 
Collecting OS_filesystem info
Collecting OS_process_list info
Collecting OS_set info
CAB file created successfully.

Final NBSU output located at NBSU_mywindowsvm_master_01172018_085005.cab

The execution time : 662.53431

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 Veritas technical support to review

NBCC resides in the following location:

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

Veritas 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 Veritas 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 173.

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

Output from the NetBackup consistency check utility (NBCC)

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

UNIX and Linux  
/usr/openv/netbackup/bin/support/output
 /nbcc/hostname_NBCC_timestamp

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

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

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

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

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

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

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

Example of an NBCC progress display

By default, 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 8.1 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
        pambl11vm3
    Detected the EMM NDMP Host entry
        fas3240a
...
2.3 Obtaining EMM server aliases...
    EMM aliases for detected EMM Server
        server1
            lidabl11.acme.com
    EMM aliases for detected master server
        server1
            lidabl11.acme.com
    EMM aliases for detected media server
        server4
...
2.4 Obtaining Storage Server information...
    Detected FalconStor OST direct copy to tape Storage Server
        falconstorvtl15
2.5 Building NetBackup storage unit list...
    Detected Storage Unit for NetBackup for NDMP media server
        reabl13
        and NDMP Host
        falconstorvtl15
    Detected disk media storage unit host
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...
   reabl13...
   virtualization5400a...

3.1 Gathering required NetBackup catalog information
Start time = 2013-02-27 09:41:07

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

3.3 Gathering list of all tapes associated with any Active Jobs
   Building NetBackup bpdbjobs list

3.4 Gathering all TryLog file names from the
   C:\Program Files\netbackup\db\jobs\trylogs
directory
   Found 10 TryLogs for 10 active jobs.
   TryLogs found for all Active Jobs

3.5 Building NetBackup Image database contents list
   Reading Image number 1000
   Reading Image number 2000
   Reading Image number 3000
   Reading Image number 4000
   Found 4014 images in the Image database

3.6 Building EMM database Media and Device configuration
   attribute lists
   Obtaining the EMM database Media attribute list for disk
   virtual server
      lidabl11 ...
      There were 0 bpmedialist records detected for media server
      lidabl11
      Getting device configuration data from server
      lidabl11 ...
      ...

3.7 Building EMM database Unrestricted Sharing Media attribute lists
   Found 0 Unrestricted Sharing media records in the EMM database

3.8 Building the EMM database Volume attribute list...
   Getting the EMM database Volume attributes from EMM server
      mlbnbu ...
   Found 43 Volume attribute records in the EMM database

3.9 Building NetBackup volume pool configuration list
   EMM Server lidabl11

3.10 Building NetBackup scratch pool configuration list
    EMM Server lidabl11

3.11 Gathering NetBackup EMM merge table list
    Found 0 EMM merge table records

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

Catalog data gathering took 189 seconds to complete

dir results for created NBCC files:
02/27/2013 09:42 AM 8 nbcc-active-tapes
02/27/2013 09:42 AM 752,698 nbcc-bpdbjobs-most_columns
07/07/2011 09:43 AM 2,211,811 nbcc-bpimagelist-l

4.0 Verifying required catalog components were gathered

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

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

5.12 Checking for the latest NBCCR repair output directory
No repair file output directory detected.

Summary of NBCC EMM Server processing
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+ Primary hostname: +
+ lidabl11 +
+ Alias hostnames: +
+ lidabl11 +
+ Sources: +
+ nbemmcmd vmoprcmd +
+ EMM Server = yes +
+ EMM NetBackup version = 8.1 +
+ NBCC NetBackup version = 8.1 +
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

Summary of NBCC Master server processing
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+ Primary hostname: +
+ lidabl11 +
+ Alias hostnames: +
+ lidabl11 +
+ Sources: +
+ nbemmcmd bpstulist nbdevquery bpgetconfig +
+ Master server = yes +
+ EMM NetBackup version = 8.1.0.0 +
+ NBCC NetBackup version = 8.1 +
+ Tape STU detected = no - Disk STU detected = yes +
+ Disk Pool Host = yes +
+ Associated Storage servers: +
+ lidabl11 lidaclvlm +
+ EMM tape media record extract attempted = yes +
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

Summary of NBCC Media server processing
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+ Primary hostname: +
+ lidabl14 +
+ Alias hostnames: +
+ lidabl14.acme.com +
+ Sources: +
+ nbemmcmd bpgetconfig +
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. Veritas 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, Veritas 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

<table>
<thead>
<tr>
<th>Stage</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stage 1</td>
<td>Data collection</td>
<td>NBCCR first collects the information that is required to perform a repair.</td>
</tr>
</tbody>
</table>
**Table 3-4  Stages of repair (continued)**

<table>
<thead>
<tr>
<th>Stage</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stage 2</td>
<td>Repair qualification</td>
<td>Immediately before the suggested repair is applied, <strong>NBCCR</strong> 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.</td>
</tr>
<tr>
<td>Stage 3</td>
<td>Repair</td>
<td>Finally, <strong>NBCCR</strong> 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, <strong>NBCCR</strong> tries to roll back the repair so that the corrective action does not introduce any new errors.</td>
</tr>
</tbody>
</table>

**NBCCR resides in the following location:**

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

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

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

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

On **UNIX**:  
/usr/openv/netbackup/bin/support/input/nbccr/SRA

On **Windows**:  
`install_path\NetBackup\bin\support\input\nbccr\SRA`
Output files

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

On UNIX: /usr/openv/netbackup/bin/support/output/nbccr/masternamenbccr_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
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 Veritas technical support can be difficult and time consuming.

By default, nbcplogs now runs the nbsu utility and collects 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.

If you have a case ID provided by Technical Support of the form #######, rename the log files with the case ID number. Then manually upload the files to the Veritas Evidence Server. For additional assistance, see:

http://www.veritas.com/docs/000097935

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:

  ```bash
  /usr/openv/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**
  ```bash
  /usr/openv/volmgr/bin/acstest -r ACSLS_hostpath
  ```
  for `acstest` to work on UNIX and Linux, `acssel` and `acsssi` must be running

- **TLD**
  ```bash
  /usr/openv/volmgr/bin/tldtest -r roboticpath
  ```

More information on ACS 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:
  ```bash
  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).

<table>
<thead>
<tr>
<th>ACS</th>
<th><code>install_path\Volmgr\bin\acstest -r ACSLS_HOST</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>TLD</td>
<td><code>install_path\Volmgr\bin\tldtest -r roboticpath</code></td>
</tr>
</tbody>
</table>

More information on ACS 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:

```bash
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
- About disaster recovery requirements
- Disaster recovery packages
- About disaster recovery settings
- 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
- Generating a certificate on a clustered master server after disaster recovery installation
- About restoring disaster recovery package
- About the DR_PKG_MARKER_FILE environment variable
- Restoring disaster recovery package on Windows
- Restoring disaster recovery package on UNIX
- 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, Veritas recommends that you contact technical support.

This topic provides information about NetBackup installation and (if necessary), catalog recovery after a system disk failure. Veritas 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.

---

**About disaster recovery requirements**

Veritas strongly recommends that during NetBackup installation in a disaster recovery mode after a disaster, you use the same master server name that is available in the disaster recovery email.

**Note:** Certificates for active and inactive nodes are not recovered during catalog recovery. Therefore, you must manually deploy certificates on all cluster nodes using a reissue token after you install NetBackup in a disaster recovery mode.

See “Generating a certificate on a clustered master server after disaster recovery installation” on page 217.

For a successful disaster recovery in all environments, you must know:

- The location of the disaster recovery package (.drpkg) file.
  
  See “Disaster recovery packages” on page 189.

- The passphrase for that specific disaster recovery package.

If the passphrase is lost, refer to the following article to get the host identity back.

http://www.veritas.com/docs/000125933

**NetBackup domain with external CA-signed certificates**

If external CA-signed certificates are used for host communication in your NetBackup domain, ensure the following before you start disaster recovery installation:

- You have configured the required Certificate Revocation Lists (CRLs).

- You have copied the valid external certificates in Windows certificate store, if they were not backed up during catalog backup.
Note: Be aware that NetBackup does not support push, remote, or silent installation for the disaster recovery of master servers. Exception: NetBackup supports these installation methods for hosts in a NetBackup master server cluster.

Disaster recovery packages

For increased security, a disaster recovery package is created during each catalog backup. The disaster recovery package file has .drpkg extension.

The disaster recovery package stores the identity of the master server host. NetBackup requires this package to get the identity of the master server back after a disaster. Once you have recovered the host identity, you can perform the catalog recovery.

The disaster recovery package contains the following information:

- NetBackup CA-signed certificates and private keys of the master server certificate and the NetBackup certificate authority (CA) certificate
- Information about the hosts in the domain
- Security settings

Note: You must set a passphrase for the disaster recovery package for the catalog backups to be successful.

See “About disaster recovery settings” on page 189.

About disaster recovery settings

For increased security, a disaster recovery package is created during each catalog backup.

See “Disaster recovery packages” on page 189.

During each catalog backup, a disaster recovery package is created and encrypted with the passphrase that you set. You need to provide this encryption passphrase while you install NetBackup on the master server in a disaster recovery mode after a disaster.

The following options are displayed on the Disaster Recovery tab:
Table 4-1  Disaster recovery settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passphrase</td>
<td>Enter the passphrase to encrypt disaster recovery packages.</td>
</tr>
<tr>
<td></td>
<td>- The passphrase must contain a minimum of 8 and a maximum of 1024 characters.</td>
</tr>
<tr>
<td></td>
<td>- The existing passphrase and the new passphrase must be different.</td>
</tr>
<tr>
<td></td>
<td>- Only the following characters are supported for the passphrase: White spaces, uppercase characters (A to Z), lowercase characters (a to z), numbers (0 to 9), and special characters. Special characters include: ~ ! @ # $ % ^ &amp; * ( ) _ + - = ` { } [ ]</td>
</tr>
<tr>
<td>Confirm Passphrase</td>
<td>Re-enter the passphrase for confirmation.</td>
</tr>
</tbody>
</table>

Caution: Ensure that the passphrase contains only the supported characters. If you enter a character that is not supported, you may face problems during disaster recovery package restore. The passphrase may not be validated and you may not be able to restore the disaster recovery package.

Note the following before you modify the passphrase for the disaster recovery packages:

- Subsequent disaster recovery packages are encrypted with the new passphrase that you set.
- If you change the passphrase anytime, it is not changed for the previous disaster recovery packages. Only new disaster recovery packages are associated with the new passphrase.
- Passphrase that you provide while you install NetBackup on the master server in a disaster recovery mode after a disaster must correspond to the disaster recovery package from which you want to recover the master server host identity.

Recommended backup practices

The following backup practices are recommended:
### Selecting files to back up
In addition to backing up files on a regular basis, it is important to select the correct files to back up. Include all files with records that are critical to users and the organization. Back up system and application files, so you can quickly and accurately restore a system to normal operation if a disaster occurs.

Include all Windows system files in your backups. In addition to the other system software, the Windows system directories include the registry, which is needed to restore the client to its original configuration. If you use a NetBackup exclude list for a client, do not specify any Windows system files in that list.

Do not omit executables and other application files. You may want to save tape by excluding these easy-to-reinstall files. However, backing up the entire application ensures that it is restored to its exact configuration. For example, if you have applied software updates and patches, restoring from a backup eliminates the need to reapply them.

### Bare Metal Restore
NetBackup Bare Metal Restore (BMR) protects client systems by backing them up with a policy configured for BMR protection. A complete description of BMR backup and recovery procedures is available.

See the *NetBackup Bare Metal Restore Administrator’s Guide*:
http://www.veritas.com/docs/DOC5332

### Critical policies
When you configure a policy for online catalog backup, designate certain NetBackup policies as critical. Critical policies back up systems and data deemed critical to end-user operation. During a catalog recovery, NetBackup verifies that all of the media that is needed to restore critical policies are available.

### Full backup after catalog recovery
If the configuration contains Windows clients that have incremental backup configurations set to **Perform Incrementals Based on Archive Bit**, run a full backup of these clients as soon as possible after a catalog recovery. The archive bit resets on the files that were incrementally backed up after the catalog backup that was used for the catalog recovery. If a full backup of these clients is not run after a catalog recovery, these files could be skipped and not backed up by subsequent incremental backups.

### Online catalog backups
Online, hot catalog backup is a policy-driven backup that supports tape-spanning and incremental backups. It allows for restoring catalog files from the Backup, Archive, and Restore interface. Online catalog backups may be run while other NetBackup activity occurs, which provides improved support for environments in which continual backup activity is typical.

### Online catalog backup disaster recovery files
Veritas recommends saving the disaster recovery files that are created by the online catalog backup to a network share or removable device. Do not save the disaster recovery files to the local computer. Catalog recovery from an online catalog backup without the disaster recovery image file is a more complex procedure and time-consuming procedure.
Automated recovery

The catalog disaster recovery file (created during an online catalog backup) is intended to automate the process of NetBackup recovery. If you recover a system other than the one that originally made the backups, it should be identical to the original system. For example, the system that performs the recovery should include NetBackup servers with identical names to those servers where the backups were made. If not, the automated recovery may not succeed.

Online catalog disaster recovery information email

Configure the online catalog backup policy to email a copy of the disaster recovery information to a NetBackup administrator in your organization. Configure this policy as part of every catalog backup. Do not save the disaster recovery information emails to the local computer. Catalog recovery without the disaster recovery image file or the disaster recovery information email available is exceedingly complex, time consuming, and requires assistance.

NetBackup emails the disaster recovery file when the following events occur:

- The catalog is backed up.
- A catalog backup is duplicated or replicated.
- The primary catalog backup or any copy of a catalog backup expires automatically or is expired manually.
- The primary copy of the catalog backup is changed as follows:
  - By using the `bpchangeprimary` command.
  - By using the option to change the primary copy when the catalog backup is duplicated manually.

You may tailor the disaster recovery email process by using the `mail_dr_info notify` script. More details are available.

See the *NetBackup Administrator’s Guide, Volume II*:

http://www.veritas.com/docs/DOC5332

If you are not able to receive the disaster recovery packages over emails even after you have configured your email, then ensure the following:

- Your email exchange server is configured to have the attachment size equal to or greater than the disaster recovery package size. You can check the size of the package (`.drpkg` file size) on the disaster recovery file location that you have specified in the catalog backup policy.
- The firewall and antivirus software in your environment allow the files with the `.drpkg` extension (which is the extension for a disaster recovery package file).
- If BLAT is used as email notification application, it is of v2.4 or later version.

Identifying the correct catalog backup

Ensure that you identify and use the appropriate catalog backup for your recovery. For example, if you recover from your most recent backups, use the catalog from your most recent backups. Similarly, if you recover from a specific point in time, use the catalog backup from that specific point in time.
Catalog recovery time

System environment, catalog size, location, and backup configuration (full and incremental policy schedules) all help determine the time that is required to recover the catalog. Carefully plan and test to determine the catalog backup methods that result in the desired catalog recovery time.

Master and media server backups

The NetBackup catalog backup protects your configuration data and catalog data. Set up backup schedules for the master servers and media servers in your NetBackup installation. These schedules protect the operating systems, device configurations, and other applications on the servers.

Master or media server recovery procedures when the system disk has been lost assume that the servers are backed up separately from the catalog backup. Backups of master and media servers should not include NetBackup binaries, configuration or catalog files, or relational database data.

About disk recovery procedures for UNIX and Linux

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

- Master server disk recovery procedures
  See “About recovering the master server disk for UNIX and Linux” on page 193.

- Media server disk recovery procedures
  See “About recovering the NetBackup media server disk for UNIX” on page 199.

- Client disk recovery procedures
  See “Recovering the system disk on a UNIX client workstation” on page 199.

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.veritas.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.

About 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 194.

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 starts from this disk during recovery. You then can 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 196.

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.veritas.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 require patches are installed, and that specific configuration settings are made. Take corrective action as needed.

2 Reinstall NetBackup software on the server you want to recover.

See the NetBackup Installation Guide for instructions:

http://www.veritas.com/docs/DOC5332

Note: For the NetBackup Web Services, you must use the same user account and credentials that were used when you backed up the NetBackup catalog. More information is available:

http://www.veritas.com/docs/000081350
3 Install any NetBackup patches that had been previously installed. See the documentation that was included with the patch software.

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

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

The following are examples:

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

5 If the recovery scenario involves restoring policy or catalog backups, the appropriate recovery device(s) must be configured, which may involve the following tasks:

- Install and configure the robotic software for the devices that read backups of the NetBackup catalog and regular backups of the disk being restored. If a non-robotic drive is available that can read these backups, then no robot is required. Although manual intervention is required if multiple pieces of media are required.
  
  See the *NetBackup Device Configuration Guide*:
  
  [http://www.veritas.com/docs/DOC5332](http://www.veritas.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.veritas.com/docs/DOC5332](http://www.veritas.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.veritas.com/docs/DOC5332](http://www.veritas.com/docs/DOC5332)

- Update the device mapping files.
  
  See the *NetBackup Administrator’s Guide, Volume I*:
  
  [http://www.veritas.com/docs/DOC5332](http://www.veritas.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*:
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.

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

See “About recovering the NetBackup catalog” on page 225.

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

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

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

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

The following procedure assumes that the root file system is lost along with everything else on the disk. This recovery reloads the operating system to an alternate boot disk and starts from this disk during recovery. You then can 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 the databases resided on the original disk. By default, they reside under the `/usr/openv` directory.
3 Verify that the operating system works, that any required patches are installed, and that specific configuration settings are made. Take corrective action as needed.

4 Install NetBackup on the alternate disk. Install only the robotic software for the devices that are required to read backups of the NetBackup catalogs and regular backups of the disk being restored. If a non-robotic drive can read these backups, no robot is required.

---

**Note:** For the NetBackup Web Services, you must use the same user account and credentials that were used when you backed up the NetBackup catalog. More information is available:

http://www.veritas.com/docs/000081350

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.veritas.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.veritas.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.veritas.com/docs/DOC5332

- Update the device mapping files.
  See the *NetBackup Administrator’s Guide, Volume I*:
  http://www.veritas.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.veritas.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 225.

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

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

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

**Warning:** Do not restore files to the `/usr/openv/var`, `/usr/openv/db/data`, or `/usr/openv/volmgr/database` directories (or relocated locations) or the directories that contain NetBackup database data. This data was recovered to the alternate disk in step 9 and is copied back to the recovery disk in step 12.
11 Stop all NetBackup processes that you started from NetBackup on the alternate disk. Use the Activity Monitor in the NetBackup Administration Console or the following:

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

12 Maintaining the same directory structure, copy the NetBackup catalogs from the alternate disk to the disk that you recover. These are the catalogs recovered in step 9.

13 Make the recovered disk the boot disk again and restart the system.

14 Start and test the copy of NetBackup on the disk that you have recovered.

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

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

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

About recovering the NetBackup media server disk for UNIX

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

See "Recovering the system disk on a UNIX client workstation" on page 199.

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.veritas.com/docs/DOC5332

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

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node failure</td>
<td>See “Replacing a failed node on a UNIX or Linux cluster” on page 200.</td>
</tr>
<tr>
<td>Shared disk failure</td>
<td>See “Recovering the entire UNIX or Linux cluster” on page 202.</td>
</tr>
<tr>
<td>Cluster failure</td>
<td>See “Recovering the entire UNIX or Linux cluster” on page 202.</td>
</tr>
</tbody>
</table>

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.veritas.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.veritas.com/docs/DOC5332

Note: For the NetBackup Web Services, you must use the same user account and credentials that are used on the other nodes of the cluster. More information is available:
http://www.veritas.com/docs/000081350

7. Install any Maintenance Packs and patches that are required to bring the newly installed node to the same patch level as the other cluster nodes.

8. Bring the NetBackup Resource group online on a node other than the freshly installed node.

9. Log onto the node on which the NetBackup resource group is online and run the following command:

/usr/openv/netbackup/bin/cluster/cluster_config -s nбу -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.veritas.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.veritas.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.veritas.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.veritas.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.veritas.com/docs/DOC5332

---

**Note:** For the NetBackup Web Services, you must use the same user account and credentials that were used when you backed up the NetBackup catalog. More information is available:
http://www.veritas.com/docs/000081350

4 Configure the clustered NetBackup server.

Refer to the *NetBackup High Availability Guide*:
http://www.veritas.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 194.

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.veritas.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 204.

- Media server disk recovery procedures
  See “About recovering the NetBackup media server disk for Windows” on page 210.

- Client disk recovery procedures
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.veritas.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 204.

- 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 207.

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.veritas.com/docs/DOC5332

   **Note:** For the NetBackup Web Services, you must use the same user account and credentials that were used when you backed up the NetBackup catalog. More information is available:
   http://www.veritas.com/docs/000081350

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.veritas.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.veritas.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.veritas.com/docs/DOC5332
   
   ■ Update the device mapping files.
     See the *NetBackup Administrator’s Guide, Volume I*:
8 If the recovery scenario involves restoring the policy backups or catalog backups that were done to media, the appropriate recovery device(s) must be configured. Configuring the media may involve the following actions:

- Manually load the required media into a 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 225.

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.

**Note:** For the NetBackup Web Services, you must use the same user account and credentials that were used when you backed up the NetBackup catalog. More information is available:

http://www.veritas.com/docs/000081350

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.veritas.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.veritas.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.veritas.com/docs/DOC5332

   - Update the device mapping files.
     
     See the *NetBackup Administrator’s Guide, Volume I*:
     
     http://www.veritas.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.veritas.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 225.

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.


### 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.veritas.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.veritas.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\bpinetd
```

NetBackup creates logs in these directories.

7 Stop and restart the NetBackup Client service.

This action enables NetBackup to start logging to the `bpinetd` debug log.

8 Use the NetBackup Backup, Archive, and Restore interface to restore the system files and user files to the client system.

For example, if all files are on the `C` drive, restoring that drive restores the entire system.

To restore files, you do not need to be the administrator, but you must have restore privileges. For instructions, refer to the online Help or refer to the following:

See the **NetBackup Backup, Archive, and Restore Getting Started Guide**:

http://www.veritas.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 `bpinetd` program is no longer running.

11 Restart the NetBackup client system.

When the boot process is complete, the system is restored to the state it was in at the time of the last backup.

About clustered 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.veritas.com/docs/DOC5332

---

**Warning:** Contact technical support before you try these recovery procedures.

Recovering 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.veritas.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.veritas.com/docs/DOC5332

**Note:** For the NetBackup Web Services, you must use the same user account and credentials that are used on the other nodes of the cluster. More information is available:

http://www.veritas.com/docs/000081350

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.
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
```

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 207.

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>
```

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.veritas.com/docs/DOC5332](http://www.veritas.com/docs/DOC5332)

Configure required devices and media and recover the NetBackup catalogs.

Manually shut down and restart NetBackup on the active node.

Re-enable monitoring of the NetBackup resource group.

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.veritas.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.veritas.com/docs/DOC5332

   **Note:** For the NetBackup Web Services, you must use the same user account and credentials that were used when you backed up the NetBackup catalog. More information is available:

   http://www.veritas.com/docs/000081350

4. Configure the clustered NetBackup server.

   Refer to the *NetBackup High Availability Guide*:

   http://www.veritas.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 207.

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 (WSFC or VCS) is available.

   Refer to the *NetBackup High Availability Guide*:

   http://www.veritas.com/docs/DOC5332
Generating a certificate on a clustered master server after disaster recovery installation

After you complete the disaster recovery of a clustered master server, you must generate a certificate on the active node as well as all inactive nodes. This procedure is required for successful backups and restores of the cluster.

Generating the local certificate on each cluster node after disaster recovery installation

1 Add all inactive nodes to the cluster.
   If all the nodes of the cluster are not currently part of the cluster, start by adding them to the cluster. Please consult with your operating system cluster instructions for assistance with this process.
   More information about supported cluster technologies is available. Please see the NetBackup Clustered Master Server Administrator’s Guide.

2 Run the `nbcertcmd` command to store the Certificate Authority certificate.
   UNIX: `/usr/openv/netbackup/bin/nbcertcmd -getCACertificate`
   Windows: `install_path\Veritas\NetBackup\bin\nbcertcmd -getCACertificate`

3 Use the `bpnbat` command as shown to authorize the necessary changes.
   When you are prompted for the authentication broker, enter the virtual server name, not the local node name.
   `bpnbat -login -loginType WEB`

4 Use the `nbcertcmd` command to create a reissue token. The `hostname` is the local node name. When the command runs, it displays the token string value. A unique reissue token is needed for each cluster node.
   `nbcertcmd -createtoken -name token_name -reissue -host hostname`

5 Use the reissue token with the `nbcertcmd` command to store the host certificate.
   This command prompts you for the token string value. Enter the token string from the `nbcertcmd -createToken` command.
   `nbcertcmd -getCertificate -token`

Additional information is available. Please see the section on deploying certificates on master server nodes in the Veritas NetBackup Security and Encryption Guide.

See “Disaster recovery packages” on page 189.

See “About disaster recovery requirements” on page 188.
About restoring disaster recovery package

Disaster recovery packages contain the NetBackup master server host identity and are created during catalog backups. You require the host identity back after you install NetBackup on the master server after a disaster.

See “Disaster recovery packages” on page 189.

Important notes

- Catalog recovery does not recover the host identity. To restore the host identity or disaster recovery package, you must install NetBackup in the disaster recovery mode and import the required package. Once you have recovered the disaster recovery package, you can recover the catalog.

- After you have restored the disaster recovery package or the master server host identity, you must immediately perform catalog recovery.
  See “About recovering the NetBackup catalog” on page 225.

You can restore the disaster recovery package of the NetBackup master server either during installation or after installation.

- To restore the package during installation, select the disaster recovery mode of installation.
  You need to specify the disaster recovery package passphrase during installation. If you specify a wrong passphrase or the passphrase is lost, you need to deploy security certificates on all hosts after installation. The disaster recovery package cannot be restored during installation. To restore the disaster recovery package after installation, refer to the following article:
  http://www.veritas.com/docs/000125933

- To restore the package after installation, use the `nbhostidentity` command.
  See “Restoring disaster recovery package on Windows” on page 219.
  See “Restoring disaster recovery package on UNIX” on page 222.

**Note:** To restore the disaster recovery package of the NetBackup Appliance, use the `nbhostidentity` command.

About the DR_PKG_MARKER_FILE environment variable

In case, external CA was configured on the master server before the disaster and the DR installation is not successful, you can use this utility to reconfigure the
external CA configuration settings. This hook enables DR installation to wait after recovering the DR package and before the services are restarted. This provides a window to correct or reconfigure the external CA configuration settings as required.

For more information on external CA-signed certificates, refer to the NetBackup Security and Encryption Guide.

See “Restoring disaster recovery package on Windows” on page 219.

See “Restoring disaster recovery package on UNIX” on page 222.

To let the NetBackup Installer hold the installation process until you have made the required changes to the external CA configuration settings, you should set an environment variable called \texttt{DR_PKG_MARKER_FILE} with a touch file. After this environment variable is set, you can start the DR installation. The DR installation waits towards the end of the installation, before starting the NetBackup services as long it finds the touch file present on the filesystem. You can change the external CA configuration settings during this time. Once done, you must delete the touch file that contains the \texttt{DR_PKG_MARKER_FILE} environment variable to let the Installer resume the installation process.

\textbf{Note:} This marker file should be used only in case of DR installation failures.

\section*{Restoring disaster recovery package on Windows}

After a disaster, you need to restore disaster recovery package corresponding to the catalog backup that you want to restore. Disaster recovery package gets the master server host identity back. You need to restore the host identity before you perform catalog recovery.

\section*{Important notes}

- In a clustered master server setup:
  - The disaster recovery package contains the identity files and configuration only for the virtual name.
  - After the DR installation, the virtual name’s certificate is restored.
  - Cluster node-specific certificates and configuration options are not backed up and therefore are not recovered. You need to redeploy or reconfigure NetBackup or external certificates after the DR installation.

\section*{Prerequisites}

If external CA-signed certificates are used in your NetBackup domain, ensure the following:
The certificate file path is configured, accessible, and is the same as the one that was backed up.

You have configured the required certificate revocation lists (CRL) before you begin the disaster recovery installation, if applicable. Refer to the NetBackup Security and Encryption Guide.

You have copied the required external certificates in Windows certificate store, if applicable.

If an external certificate was configured on the master server before the disaster and DR installation fails, you can set the environment variable called `DR_PKG_MARKER_FILE` to enable you to correct the external certificate configuration towards the end of the DR installation. See “About the DR_PKG_MARKER_FILE environment variable” on page 218.

To restore the disaster recovery package during NetBackup installation

1. Start the NetBackup software installation.

   Refer to the Installing server software on Windows systems section from the NetBackup Installation Guide.

2. On the NetBackup License Key and Server Type screen, select the Disaster Recovery Master Server option.

3. On the NetBackup Disaster Recovery screen, specify the location of the disaster recovery package. Click Browse to select the package location that you want to restore.

4. Specify the passphrase that is associated with the disaster recovery package that you want to restore.

   Ensure that you specify the appropriate passphrase:

   - If you specify a wrong passphrase or the passphrase is lost, you need to deploy security certificates on all hosts after installation. The disaster recovery package cannot be restored during installation. To restore the disaster recovery package after installation, refer to the following article:
     [http://www.veritas.com/docs/000125933](http://www.veritas.com/docs/000125933)

   - If the passphrase is validated, continue with the installation.

5. If external CA-signed certificates were used in your NetBackup domain at the time of catalog backup before the disaster, during the DR installation, the Installer shows a WARNING message to configure the certificate revocation list (CRL). The CRL settings are also displayed that you can configure.

   - Review the value of the `ECA_CRL_CHECK` configuration option.

     For more information on catalog backup and external certificate configuration options, refer to the NetBackup Administrator's Guide, Volume I.
If the `ECA_CRL_CHECK` configuration option is set to `DISABLE`, you do not need to do the CRL configurations.

If the `ECA_CRL_CHECK` configuration option is enabled, you are prompted to configure the CRL. Configure the CRLs and continue with the DR installation.

Depending on the value that is specified for the `ECA_CRL_PATH` option, make the required CRLs available.

- If `ECA_CRL_PATH` is not specified, NetBackup uses the CRLs from CRL distribution point (CDP) of the peer host's certificate. Ensure that the URLs that are available in the CDP are accessible.
- If `ECA_CRL_PATH` is specified, NetBackup uses the CRLs that are available in the directory specified for this option. Copy the valid CRLs in the directory that you specify for `ECA_CRL_PATH`.

In case Windows certificate store was used to store the external CA-signed and this certificate was not backed up in the DR package, you can see a warning to configure the external CA-signed certificates. Configure the following external certificate configuration options on the master server as per the values provided in the Installer or in the corresponding disaster recovery email:

- `ECA_CERT_PATH`
- `ECA_PRIVATE_KEY_PATH`
- `ECA_KEY_PASSPHRASEFILE`
- `ECA_TRUST_STORE_PATH`
- `ECA_CRL_PATH`

For more information on catalog backup and external certificate configuration options, refer to the *NetBackup Administrator's Guide, Volume I.*

In case the `DR_PKG_MARKER_FILE` environment variable was set before the DR installation, the installer displays a message, which conveys that the touch file exists. Once the external certificate configuration is done, delete the touch file that you have set for the `DR_PKG_MARKER_FILE` environment variable.

NetBackup services are started.

Refer to the Installing server software on Windows systems section from the *NetBackup Installation Guide.*
To restore the disaster recovery package after NetBackup installation

1. Run the `nbhostidentity -import -infile file_path` command after NetBackup installation.
   
   Refer to the NetBackup Commands Reference Guide.

2. Clean up the whitelist cache and restart the NetBackup services on all hosts in the domain.

3. Carry out this step to remove the NetBackup certificate files in the following scenario:

   NetBackup was configured to use only external CA-signed certificates before the disaster and NetBackup was configured to use NetBackup certificates or both NetBackup and external certificates before you manually imported the disaster recovery package.

   Run the following command to remove NetBackup certificate files:

   ```
   configureWebServerCerts -removeNBCert
   ```

---

**Restoring disaster recovery package on UNIX**

After a disaster, you need to restore disaster recovery package corresponding to the catalog backup that you want to restore. Disaster recovery package gets the master server host identity back. You need to restore the host identity before you perform catalog recovery.

**Important notes**

- In a clustered master server setup:
  - The disaster recovery package contains the identity files and configuration only for the virtual name.
  - After the DR installation, the virtual name's certificate is restored.
  - Cluster node-specific certificates and configuration options are not backed up and therefore are not recovered. You need to redeploy or reconfigure NetBackup or external certificates after the DR installation.

**Prerequisites**

If external CA-signed certificates are used in your NetBackup domain, ensure the following:

- In case of file-based external certificates, ensure that the certificate file path is configured, accessible, and is the same as the one that was backed up.
If you used Windows certificate store as a certificate store before the disaster and the certificate files were not backed up during catalog backup, you need to manually configure the external certificate for the host after the disaster. Refer to the following article:

You have configured the required certificate revocation lists (CRL) before you begin the disaster recovery installation, if applicable. For more information on the CRLs, refer to the NetBackup Security and Encryption Guide.

If an external certificate was configured on the master server before the disaster and DR installation fails, you can set the environment variable called DR_PKG_MARKER_FILE to enable you to correct the external certificate configuration towards the end of the DR installation. See “About the DR_PKG_MARKER_FILE environment variable” on page 218.

To restore the disaster recovery package during NetBackup installation

1. Start the NetBackup software installation. Refer to the Installing server software on UNIX systems section from the NetBackup Installation Guide.

2. When the following message appears, press Enter to continue:

   Is this host a master server? [y/n] (y)

3. When the following message appears, select Y.

   Are you currently performing a disaster recovery of a master server? [y/n] (y)

4. When the following message appears, provide the name and the path of the disaster recovery package that you want to restore.

   Enter the name of your disaster recovery package along with the path, or type q to exit the install script:

   If external certificates are used in your domain, a warning message is displayed. When the installer waits during subsequent steps, configure the external certificate configuration options as per step 6.
5 When the following message appears, provide the passphrase that is associated with the disaster recovery package that you want to restore.

**Caution:** Ensure that you specify the appropriate passphrase.

If you specify a wrong passphrase or the passphrase is lost, you need to deploy security certificates on all hosts after installation. The disaster recovery package cannot be restored during installation. To restore the disaster recovery package after installation, refer to the following article:

http://www.veritas.com/docs/000125933

Enter your disaster recovery passphrase, or enter q to exit installation:

The following message appears:

Validating disaster recovery passphrase...

If the passphrase is validated, continue with the installation.

6 If external CA-signed certificates are used in your NetBackup domain, do the following:

- Review the value of the `ECA_CRL_CHECK` configuration option.
  For more information on catalog backup and external certificate configuration options, refer to the NetBackup Administrator's Guide, Volume I.

- If the `ECA_CRL_CHECK` configuration option is set to `DISABLE`, you do not need to do the CRL configurations.

- If the `ECA_CRL_CHECK` configuration option is enabled, you are prompted to configure the CRL.
  The UNIX installer does not wait for any action but proceeds to the next step in the installer. When the installer waits after the following step, you can configure the CRLs and continue with the DR installation.

Configure the CRLs and continue with the DR installation.

- Depending on the value that is specified for the `ECA_CRL_PATH` option, make the required CRLs available.

  - If `ECA_CRL_PATH` is not specified, NetBackup uses the CRLs from CRL distribution point (CDP) of the peer host's certificate. Ensure that the URLs that are available in the CDP are accessible.

  - If `ECA_CRL_PATH` is specified, NetBackup uses the CRLs that are available in the directory specified for this option. Copy the valid CRLs in the directory that you specify for `ECA_CRL_PATH`. 
In case the `DR_PKG_MARKER_FILE` environment variable was set before the DR installation, the installer displays a message, which conveys that the touch file exists. Once the external certificate configuration is done, delete the touch file that you have set for the `DR_PKG_MARKER_FILE` environment variable.

NetBackup services are started.

7 Refer to the Installing server software on UNIX systems section from the NetBackup Installation Guide.

To restore the disaster recovery package after NetBackup installation

1 Run the `nbhostidentity -import -infile file_path` command after NetBackup installation.

Refer to the NetBackup Commands Reference Guide.

2 Clean up the whitelist cache and restart the NetBackup services on all hosts in the domain.

3 Carry out this step to remove the NetBackup certificate files in the following scenario:

NetBackup was configured to use only external CA-signed certificates before the disaster and it was configured to use NetBackup certificates or both NetBackup and external certificates before you manually imported the disaster recovery package.

Run the following command to remove NetBackup certificate files:

```
configureWebServerCerts -removeNBCert
```

About recovering the NetBackup catalog

Before you recover the NetBackup catalog, you must do the following:

- Ensure that NetBackup is running in the recovery environment.
- Configure the recovery devices 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.
- Restore the NetBackup host identity by restoring the disaster recovery package. See “About restoring disaster recovery package” on page 218.
Caution: After successful catalog recovery, you must set the disaster recovery package passphrase, because the passphrase is not recovered during the catalog recovery.

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>
<thead>
<tr>
<th>Recovery option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Recover the entire catalog | Veritas recommends that you recover the entire catalog. Doing so helps ensure consistency among the various parts of the catalog. This method is most useful for recovering a catalog to the same environment from which it was backed up.  
See “About recovering the entire NetBackup catalog” on page 233. |
| Recover the catalog image files and configuration files | The image database contains information about the data that has been backed up. The configuration files (databases.conf and server.conf) are the flat files that contain instructions for the SQL Anywhere daemon.  
This type of recovery also restores the NetBackup relational database (NBDB) to the staging directory so that it is available for further processing if required.  
See “About recovering the NetBackup catalog image files” on page 247. |
| Recover the relational database files | The NetBackup database (NBDB) is also known as the Enterprise Media Manager (EMM) database. It contains information about volumes and the robots and drives that are in NetBackup storage units. The NetBackup relational database also contains the NetBackup catalog images files. The images files contain the metadata that describes the backups.  
Recover the relational database if it is corrupt or lost but the catalog image files exist and are valid.  
See “About recovering the NetBackup relational database” on page 262. |

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 229.  
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 274.
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 280.

Other procedures exist for special use cases.

See “Recovering the NetBackup catalog when NetBackup Access Control is configured” on page 272.

Other topics provide more information about catalog recovery.

See “About NetBackup catalog recovery on Windows computers” on page 227.
See “About NetBackup catalog recovery from disk devices” on page 227.
See “About NetBackup catalog recovery and OpsCenter” on page 228.

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/openv/netbackup/db -> /opt/VRTSnbu/netbackup/db
/usr/openv/db/staging -> /opt/VRTSnbu/db/staging
```

On Solaris systems only, you also must create the following symbolic links before you recover the catalog:

```
/usr/openv -> /opt/openv
```

If the symbolic links and their targets do not exist, catalog recovery fails.

### About NetBackup catalog recovery and OpsCenter

When the NetBackup catalog is recovered, NetBackup resets the job ID to 1. NetBackup starts assigning job numbers beginning with 1.
If you use NetBackup OpsCenter to monitor NetBackup activity, you may see duplicate job IDs in OpsCenter after a catalog recovery. To prevent duplicate job IDs, you can specify the job ID from which NetBackup should number jobs after the recovery.

See “Specifying the NetBackup job ID number after a catalog recovery” on page 229.

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 228.

To specify the NetBackup job ID number after a catalog recovery

1 If necessary, restore the OpsCenter database from a backup.
2 Determine the last job ID number that is recorded in OpsCenter.
3 Edit the NetBackup jobid file and set the value to one higher than the number from step 2. The following is the pathname to the jobid file:
   ■ UNIX: /usr/openv/netbackup/db/jobs/jobid
   ■ Windows: install_path\Veritas\NetBackup\db\jobs\jobid
   Because the recovery consumes job numbers, you must specify the number before the catalog recovery.
4 Recover the NetBackup catalog.

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.veritas.com/docs/DOC5332

The following is an example of a disaster recovery email after a successful catalog backup:

From: NetBackup@example.com
Sent: Thursday, January 3, 2019 05:48
To: NetBackup Administrator
Subject: NetBackup Catalog Backup successful on host master.example.com status 0
Attachments:  cat_backup_1438271286_INCR
              cat_backup_1438271286_INCR.drpkg

Server
    master.example.com

NetBackup Version
    8.1.X

Date
    4/27/2017 05:46:45 AM

Policy
    cat_backup

Catalog Backup Status
    the requested operation was successfully completed (status 0).
WARNING: External CA-signed certificates could not be backed up.
Refer to the following article to configure external CA-signed certificates
on the host after disaster recovery installation:

DR image file: /dr/nbu_dr_file/cat_backup_1438271286_INCR

To ensure that the NetBackup catalog data is protected through
1/3/2019 10:46:45 AM, retain a copy of each attached file, and the
media or files listed below:

Catalog Recovery Media

<table>
<thead>
<tr>
<th>Media Server</th>
<th>Disk Image Path</th>
<th>Image File Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>* media-server.example.com @aaaab</td>
<td>cat_backup_1438267080_FULL</td>
<td></td>
</tr>
<tr>
<td>* media-server.example.com @aaaab</td>
<td>cat_backup_1438271206_INCR</td>
<td></td>
</tr>
<tr>
<td>* media-server.example.com @aaaab</td>
<td>cat_backup_1438271286_INCR</td>
<td></td>
</tr>
</tbody>
</table>

DR file written to
    /dr/nbu_dr_file/cat_backup_1438271286_INCR

DR Package file written to
    /dr/nbu_dr_file/cat_backup_1438271286_INCR.drpkg

The CA configuration at the time of catalog backup is as follows:

The master server ch12auto28 is configured to use NetBackup and external
CA-signed certificates.
ECA_CERT_PATH = MY\ch12auto28.pne.ven.veritas.com
ECA_CRL_PATH = C:\Users\Administrator\Downloads\divgrt1.crl
ECA_CRL_PATH_SYNC_HOURS = 1
ECA_CRL_REFRESH_HOURS = 24
ECA_CRL_CHECK = 1
ECA_DR_BKUP_WIN_CERT_STORE = YES

The master server ms1.exampleveritas.com is configured to use the following Key Management Servers.

KMS Server Name = kms1.example.veritas.com , KMS Server Type = KMIP
KMS Server Name = kms2.example.veritas.com , KMS Server Type = KMIP
KMS Server Name = kms3.example.veritas.com , KMS Server Type = KMIP
KMS Server Name = kms4.example.veritas.com , KMS Server Type = KMIP
KMS Server Name = ms1.exampleveritas.com , KMS Server Type = NBKMS

* - 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 Package file and DR Image File

In the event of a catastrophic failure, use the following procedure to rebuild the previous NetBackup environment.

Important Notes:
- 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.
- Keep the passphrase associated with the DR Package file handy. This passphrase is set before the catalog backup policy configuration using the NetBackup Administration Console or the nbsecmd command.
- If this catalog backup is encrypted using a key from a Key Management Server, ensure that the Key Management Server is online before doing any of the following steps.

1. Install NetBackup.
   a. The installation procedure prompts you to confirm if this is a DR scenario.
      i. On the UNIX installer, you can see a prompt as "Do you want to do a disaster recovery on this master server? [y,n] (y)". Select "y"
      ii. On the Windows installer click the "Disaster Recovery Master Server" button.
   b. The installation procedure prompts you for the master server’s DR Package (refer to the /dr/nbu_dr_file/cat_backup_1438271286_INCR.drpkg mentioned earlier).
      Make sure that the Master Server can access the attached DR package file.
   c. Type the passphrase associated with the Master Server’s DR Package, when prompted.
      i. The installer validates the DR package using that passphrase
      ii. In case of errors in validation, the installer aborts the operation. To work around the issue, refer to the following article: http://www.veritas.com/docs/000125933

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.
5. Start the NetBackup Recovery Wizard from the NetBackup Administration Console. Or, start the wizard from a command line by entering bprecover -wizard.

WARNING: CRLs are not backed as part of the DR package backup.
Refer to the following article to manually add the CRLs:

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
   To recover from copy 1:
   \texttt{bpimport -create\_db\_info -stype AdvancedDisk -dp dp-advdisk -dv /storage/advdisk}
5. Run:
   \texttt{cat\_export -client client1.example.com}
6. Go to the following directory to find the DR image file
   \texttt{cat\_backup\_1438271286\_INCR: /usr\/openv\/netbackup\/db.export\/images\_/master.example.com\_/1438000000}
7. Open \texttt{cat\_backup\_1438271286\_INCR} file and find the BACKUP\_ID
   (for example: \texttt{master.example.com\_1438271286}).
8. Run:
   \texttt{bpimport [-server name] -backupid master.example.com\_1438271286}
9. Run:
   \texttt{bprestore -T -w [-L progress\_log] -C master.example.com -t 35 -p cat\_backup -X -s 1438271286 -e 1438271286 /}
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:
    \texttt{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 225.

About recovering the entire NetBackup catalog

Veritas 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:

<table>
<thead>
<tr>
<th>Backup Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full backup</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

**Note:** If the catalog was backed up on a NAT media server, you must carry out certain steps to establish a connection with the NAT media server before catalog recovery.

See “Establishing a connection with NAT media server before catalog recovery” on page 246.

For more information on NAT support in NetBackup, see the NetBackup Administrator’s Guide, Volume I.

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 234.

- The text-based wizard launched by the `bprecover -wizard` command and option.
  See “Recovering the entire NetBackup catalog using bprecover -wizard” on page 242.

The relational database transaction log is not applied during full catalog recovery. The parts of the NetBackup catalog are described in the administrator's guides.

### 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 225.

**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, Veritas recommends that you recover only the NetBackup image files.

See “About recovering the NetBackup catalog image files” on page 247.
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:
     ```bash
     /usr/openv/netbackup/bin/bp.start_all
     ```
   - On Windows:
     ```bash
     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.veritas.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.veritas.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.

   ![NetBackup Catalog Recovery Wizard](image)

   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 Retreiving 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.
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.

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 Cancel, fix the problem, and then run the wizard again.

Successful        Click Next to continue to the final wizard panel.

**Caution:** After successful catalog recovery, you must set the disaster recovery package passphrase, because the passphrase is not recovered during the catalog recovery.

The following warning is displayed if the disaster recovery package passphrase is not set:

WRN - Passphrase for the disaster recovery package is not set. You must set the passphrase for the catalog backups to be successful.

See “Disaster recovery packages” on page 189.

Do one of the following to set the passphrase:

- In the **NetBackup Administration Console**, expand **Security Management > Global Security Settings**. In the details pane, click the **Disaster Recovery** tab and specify the passphrase.

- Use the `nbseccmd -drpkgpassphrase` command to specify the passphrase.

10 On the panel that informs you that the recovery is complete, click **Finish**.
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 280.
- Before you restart NetBackup, Veritas 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.

Clean up whitelist cache on all hosts.

Stop and restart NetBackup services on the master server and other hosts, as follows:

- On UNIX and Linux:
  
  ```
  /usr/openv/netbackup/bin/bp.kill_all
  /usr/openv/netbackup/bin/bp.start_all
  ```

- On Windows:
  
  ```
  install_path\NetBackup\bin\bpdown
  install_path\NetBackup\bin\bpup
  ```

  If the NetBackup Administration Console is active on any of the hosts, the command that stops the NetBackup services shuts it down.

After the services are restarted, run the following command:

- If NetBackup (or host ID-based) certificates are used in your NetBackup domain, do the following:
  
  On a non-clustered setup:
  
  UNIX:
  
  ```
  /usr/openv/netbackup/bin/nbcertcmd -renewcertificate
  ```

  Windows:
  
  ```
  install_path\netbackup\bin\nbcertcmd -renewcertificate
  ```

  On a clustered setup:
If external CA-signed certificates are used in your NetBackup domain, do the following:

On a non-clustered setup

UNIX:
/usr/openv/netbackup/bin/nbcertcmd -enrollCertificate

Windows:
install_path\netbackup\bin\nbcertcmd -enrollCertificate

On a clustered setup:

UNIX:
/usr/openv/netbackup/bin/nbcertcmd -enrollCertificate -cluster

Windows:
install_path\netbackup\bin\nbcertcmd -enrollCertificate -cluster

If the command runs successfully, proceed with the next step.

If the command fails with the exist status 5988, refer to the following topic:
See “Steps to carry out when you see exit status 5988 during catalog recovery” on page 281.
Proceed with the next step.

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, Veritas recommends that you recover only the NetBackup image files. See “About recovering the NetBackup catalog image files” on page 247.

**Warning:** Do not run any client backups before you recover the NetBackup catalog.

To recover the entire catalog by using bprecover -wizard

1. If recovering the catalog to a new NetBackup installation, such as at a disaster recovery site, do the following:
   - Install NetBackup.
   - Configure the devices that are required for the recovery.
   - Add the media that are required for the recovery to the devices.

2. Start NetBackup.
   The following are the commands to start NetBackup:
   - UNIX and Linux:
     `/usr/openv/netbackup/bin/bp.start_all`
   - Windows:
     `install_path\NetBackup\bin\bpup.exe`
3 Start the `bprecover` wizard by entering the following command:
   - **UNIX and Linux:**
     `/usr/openv/netBbckup/bin/admincmd/bprecover -wizard`
   - **Windows:**
     `install_path\Veritas\NetBackup\bin\admincmd\bprecover.exe -wizard`

The following is displayed:

```
Welcome to the NetBackup Catalog Recovery Wizard!

Please make sure the devices and media that contain catalog
disaster recovery data are available
Are you ready to continue? (Y/N)
```

4 Enter **Y** to continue. The following prompt appears:

```
Please specify the full pathname to the catalog disaster recovery file:
```

5 Enter the fully qualified pathname to the disaster recovery file for the backup
that you want to restore. For example:

```
/mnt/hdd2/netbackup/dr-file/Backup-Catalog_1318222845_FULL
```

If the most recent catalog backup was an incremental backup, use the disaster
recovery file from the incremental backup. (There is no need to first restore
the full backup and then follow with the incremental backup.) Alternately, you
can recover from earlier version of the catalog.

If the pathname is to a valid DR file, a message similar to the following is
displayed:

```
vm2.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/openv/netbackup/logs/user_ops/root/logs/Recover1318344410.log

Caution: After successful catalog recovery, you must set the disaster recovery package passphrase, because the passphrase is not recovered during the catalog recovery.

The following warning is displayed if the disaster recovery package passphrase is not set:

WRN - Passphrase for the disaster recovery package is not set.
You must set the passphrase for the catalog backups to be successful.

Do one of the following to set the passphrase:

- In the NetBackup Administration Console, expand Security Management > Global Security Settings. In the details pane, click the Disaster Recovery tab and specify the passphrase.
- Use the nbsecmd -drpkgpassphrase command to specify the passphrase.

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 280.
- Before you restart NetBackup, Veritas 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 262.

9 Clean up whitelist cache on all hosts.

10 Stop and restart NetBackup services on the master server and other hosts, as follows:

The following are the commands to stop and restart NetBackup:

- On UNIX and Linux:
  
  `/usr/openv/netbackup/bin/bp.kill_all`
  `/usr/openv/netbackup/bin/bp.start_all`

- On Windows:
  
  `install_path\NetBackup\bin\bpdown`
  `install_path\NetBackup\bin\bpup`

11 After the services are restarted, run the following command:

- If NetBackup (or host ID-based) certificates are used in your NetBackup domain, do the following:
  
  On a non-clustered setup:
  UNIX:
  `/usr/openv/netbackup/bin/nbcertcmd -renewcertificate`

  Windows:
  `install_path\netbackup\bin\nbcertcmd -renewcertificate`

  On a clustered setup:
  UNIX:
  `/usr/openv/netbackup/bin/nbcertcmd -renewcertificate -cluster`

  Windows:
  `install_path\netbackup\bin\nbcertcmd -renewcertificate -cluster`
If external CA-signed certificates are used in your NetBackup domain, do the following:

On a non-clustered setup:

UNIX:

```
/usr/openv/netbackup/bin/nbcertcmd -enrollCertificate
```

Windows:

```
install_path\netbackup\bin\nbcertcmd -enrollCertificate
```

On a clustered setup:

UNIX:

```
/usr/openv/netbackup/bin/nbcertcmd -enrollCertificate -cluster
```

Windows:

```
install_path\netbackup\bin\nbcertcmd -enrollCertificate -cluster
```

- If the command runs successfully, proceed with the next step.
- If the command fails with the exist status 5988, refer to the following topic:
  - See “Steps to carry out when you see exit status 5988 during catalog recovery” on page 281.
  - Proceed with the next step.

12 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

**Establishing a connection with NAT media server before catalog recovery**

If the catalog was backed up on a NAT media server, you must carry out the following steps on the master server to establish a connection with the NAT media server before catalog recovery.

For more information on NAT support in NetBackup, see the NetBackup Administrator's Guide, Volume I.
To establish a connection with the NAT media server

1. Run the `configureMQ` command on the master server.

2. Use the `nbsetconfig` command to set the following configuration options on
   the master server:
   - Update `NAT_SERVER_LIST` with the NAT media server name where the
     catalog backup was taken.
   - Set `INITIATE_REVERSE_CONNECTION` to `TRUE`.

   For more information on configuration options, see the NetBackup
   Administrator’s Guide, Volume I.

3. Restart services on the master server.

4. Ensure whether a reverse connection between the master server and the NAT
   media server is established using the `bptestbpcd` command.

   See “About recovering the entire NetBackup catalog” on page 233.

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 271.
- Optionally, recovers the policy and the licensing data.

Table 4-4 is a list of the files that are included in a partial recovery.

---

**Note:** The image files are 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 228.
Veritas 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 262.

- 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:

<table>
<thead>
<tr>
<th>Backup Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full backup</td>
<td>The image files and configuration files that are listed in the disaster recovery file are recovered.</td>
</tr>
<tr>
<td>Incremental backup</td>
<td>Two recover scenarios exist, as follows:</td>
</tr>
<tr>
<td></td>
<td>- The catalog contains no information about the corresponding full backup and other incremental backups. NetBackup restores only the backup image .f files, configuration files, and NetBackup policy files that are backed up in that incremental backup. However, all of the catalog backup image .f files up to the last full catalog backup are restored. Therefore, you can restore the rest of the policy, image .f files, and configuration files by using the Backup, Archive and Restore interface.</td>
</tr>
<tr>
<td></td>
<td>- The catalog contains information about the corresponding full backup and other incremental backups. NetBackup restores all of the backup image .f files and the configuration files that were included in the related set of catalog backups.</td>
</tr>
</tbody>
</table>

**Catalog image files**

Table 4-4 lists the files that comprise a partial catalog recovery.
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 234.

- 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 242.

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 247.

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 247.

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:
     ```bash
     /usr/openv/netbackup/bin/bp.start_all
     ```
   - On Windows:
     ```bash
     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:
   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:
   c. Create symbolic links to match those in the original environment.
      See “About NetBackup catalog recovery and symbolic links” on page 228.
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.

![NetBackup Catalog Recovery Wizard](image)

   Click Next to continue. The Retrieving Disaster Recovery File panel appears.
6 The wizard searches for the media that are required to recover the catalog, and Retreiving 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.

7 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.

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 280.

- Before you restart NetBackup, Veritas 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 262.

14 Stop and restart NetBackup services on the master server, as follows:
15 After the services are restarted, run the following command:

On a non-clustered setup:

Windows:

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

UNIX:

```
/usr/openv/netbackup/bin/nbcertcmd -renewcertificate
```

On a clustered setup:

Windows:

```
install_path\NetBackup\bin\nbcertcmd -renewcertificate -cluster
```

UNIX:

```
/usr/openv/netbackup/bin/nbcertcmd -renewcertificate -cluster
```

If the command runs successfully, proceed with the next step.

If the command fails with the exit status 5988, refer to the following topic:

See “Steps to carry out when you see exit status 5988 during catalog recovery” on page 281.

Proceed with the next step.

16 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 247.

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 228.

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 Windows:
     ```
     install_path\NetBackup\bin\bpup
     ```
   - On UNIX and Linux:
     ```
     /usr/openv/netbackup/bin/bp.start_all
     ```

3. Start the NetBackup services on the master server by entering the following command:
On Windows:

\textit{install\_path\NetBackup\bin\bpup}

On UNIX and Linux:

\texttt{/usr/openv/netbackup/bin/bp.start\_all}

4 Start the \texttt{bprecover} wizard by entering the following command:

\texttt{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 \texttt{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.example.com_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/openv/netbackup/logs/user_ops/root/logs/Recover1318357550.log

10 When the recovery job is finished, each image file is restored to the proper image directory and the configuration files are restored. If you chose to recover the policy data and licensing data, it is restored also.

11 Export the image metadata from the relational database in the staging directory, as follows:

    cat_export -all -staging -source_master source-master-server-name

The export is required so that the image metadata can be imported into the relational database. A catalog image file recovery does not recover the relational database.
12 Import the image metadata into the relational database, as follows:

```bash
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 227.

To fix the disk media IDs in the image headers, run the following command:

```bash
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 280.

- Before you restart NetBackup, Veritas 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 262.

15 Clean up whitelist cache for all hosts.

16 Stop and restart NetBackup services on the master server and other hosts, as follows:

- On Windows:

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

- On UNIX:
After the services are restarted, run the following command:

- If NetBackup (or host ID-based) certificates are used in your NetBackup domain, do the following:
  - On a non-clustered setup:
    - Windows:
      
      ```bash
      install_path\netbackup\bin\nbcertcmd -renewcertificate
      ```
    - UNIX:
      
      ```bash
      /usr/openv/netbackup/bin/nbcertcmd -renewcertificate
      ```
  - On a clustered setup:
    - Windows:
      
      ```bash
      install_path\netbackup\bin\nbcertcmd -renewcertificate -cluster
      ```
    - UNIX:
      
      ```bash
      /usr/openv/netbackup/bin/nbcertcmd -renewcertificate -cluster
      ```

- If external CA-signed certificates are used in your NetBackup domain, do the following:
  - On a non-clustered setup:
    - UNIX:
      
      ```bash
      /usr/openv/netbackup/bin/nbcertcmd -enrollCertificate
      ```
    - Windows:
      
      ```bash
      install_path\netbackup\bin\nbcertcmd -enrollCertificate
      ```
  - On a clustered setup:
    - UNIX:
      
      ```bash
      /usr/openv/netbackup/bin/nbcertcmd -enrollCertificate -cluster
      ```
    - Windows:
      
      ```bash
      install_path\netbackup\bin\nbcertcmd -enrollCertificate -cluster
      ```

- If the command runs successfully, proceed with the next step.
If the command fails with the exit status 5988, refer to the following topic:
See “Steps to carry out when you see exit status 5988 during catalog recovery” on page 281.
Proceed with the next step.

18 If the catalog recovery is part of a server recovery procedure, complete the remaining steps in the appropriate recovery procedure.

This procedure can include the following tasks:
■ Importing the backups from the backup media into the catalog
■ Write protecting the media
■ Ejecting the media and setting it aside
■ Freezing the media

About recovering the NetBackup relational database

The NetBackup database (NBDB) is also known as the Enterprise Media Manager (EMM) database. It contains information about volumes and the robots and drives that are in NetBackup storage units. The NetBackup relational database also contains the NetBackup catalog images files. The images files contain the metadata that describes the backups.

You can recover the NetBackup relational databases independently of an entire catalog backup.

Recover from a backup
See “Recovering NetBackup relational database files from a backup” on page 262.

Recover from the staging directory
See “Recovering the NetBackup relational database files from staging” on page 267.

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 11 and step 13 in the following procedure.
The database is corrupted. Follow all of the steps in the procedure only if 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/openv/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/openv/db/data`
   - Windows: `C:\Program Files\Veritas\NetBackupDB\data`

3. Configure SQL Anywhere so that it does not try to start automatically when the host is started, as follows:
   - UNIX: `/usr/openv/db/bin/nbdb_admin -auto_start NONE`
   - Windows: `install_path\NetBackup\bin\nbdb_admin -auto_start NONE`

4. Start the SQL Anywhere server, as follows:
   - UNIX: `/usr/openv/netbackup/bin/nbdbms_start_stop start`
   - Windows: `install_path\NetBackup\bin\bpup -e SQLANYs_VERITAS_NB`
Create the database. The command that you run depends on your scenario, as follows:

**Normal scenario**

**UNIX:** /usr/openv/db/bin/create_nbdb -drop

**Windows:** install_path\NetBackup\bin\create_nbdb -drop

**The database was relocated or the environment is clustered**

**UNIX:** /usr/openv/db/bin/create_nbdb -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/openv/db/bin/create_nbdb -drop -data VXDBMS_NB_DATA -index VXDBMS_NB_INDEX -tlog VXDBMS_NB_TLOG -staging VXDBMS_NB_STAGING

**Windows:** install_path\NetBackup\bin\create_nbdb -drop -data VXDBMS_NB_DATA -index VXDBMS_NB_INDEX -tlog VXDBMS_NB_TLOG -staging VXDBMS_NB_STAGING

Obtain the values for the option arguments from the vxdbms.conf file in the temporary directory that you created in step 2.

Start the NetBackup services, as follows:

**UNIX:** /usr/openv/netbackup/bin/bp.start_all

**Windows:** install_path\NetBackup\bin\bpup

Load the default device protocols and settings into the NetBackup Enterprise Media Manager (EMM) database by running the following command:

**UNIX:** /usr/openv/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/openv/db/data

**Windows:**  
`install_path\NetBackupDB\data`

9 Start the NetBackup device manager on the NetBackup master server, as follows:

**UNIX:**  
/usr/openv/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 I.* For disk storage types, see the guide that describes the option.  
      See the following website for NetBackup documentation:  
      [http://www.veritas.com/docs/DOC5332](http://www.veritas.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.veritas.com/docs/DOC5332](http://www.veritas.com/docs/DOC5332)

   c  Import the catalog backup from the media on which it resides.  
      See the *NetBackup Administrator's Guide, Volume I:*  
      [http://www.veritas.com/docs/DOC5332](http://www.veritas.com/docs/DOC5332)
11 Recover the catalog by running the following command on the master server:

UNIX: 
/usr/openv/netbackup/bin/admincmd/bprecover -r -nbdb

Windows: install_path\NetBackup\bin\admincmd\bprecover -r -nbdb

12 Clean up whitelist cache for all hosts

13 Stop and restart NetBackup services on the master server and other hosts, as follows:

UNIX: 
/usr/openv/netbackup/bin/bp.kill_all
/usr/openv/netbackup/bin/bp.start_all

Windows: install_path\NetBackup\bin\bpdown
install_path\NetBackup\bin\bpup

14 After the services are restarted, run the following command:

- If NetBackup (or host ID-based) certificates are used in your NetBackup domain, do the following:
  On a non-clustered setup:
  UNIX:
  
  /usr/openv/netbackup/bin/nbcertcmd -renewcertificate

  Windows:
  install_path\netbackup\bin\nbcertcmd -renewcertificate

  On a clustered setup:
  UNIX:
  
  /usr/openv/netbackup/bin/nbcertcmd -renewcertificate -cluster

  Windows:
  install_path\netbackup\bin\nbcertcmd -renewcertificate -cluster

- If external CA-signed certificates are used in your NetBackup domain, do the following:
  On a non-clustered setup
  UNIX:
  
  /usr/openv/netbackup/bin/nbcertcmd -enrollCertificate
Windows:

`install_path\netbackup\bin\nbcertcmd -enrollCertificate`

On a clustered setup:

UNIX:

`/usr/openv/netbackup/bin/nbcertcmd -enrollCertificate -cluster`

Windows:

`install_path\netbackup\bin\nbcertcmd -enrollCertificate -cluster`

If the command fails with the exit status 5988, refer to the following topic:

See “Steps to carry out when you see exit status 5988 during catalog recovery” on page 281.

**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 247.

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 271.

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 follows:

<table>
<thead>
<tr>
<th>The database is not corrupted</th>
<th>See “To recover relational database files from staging if the database is not corrupted” on page 268.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The database is corrupted</td>
<td>See “To recover relational database files from staging if the database is corrupted” on page 268.</td>
</tr>
</tbody>
</table>
To recover relational database files from staging if the database is not corrupted

1. Run the following command on the master server to recover NBDB from staging:
   
   **UNIX:** `/usr/openv/db/bin/nbdb_restore -dbn NBDB -recover -staging`
   
   **Windows:** `install_path\NetBackup\bin\nbdb_restore -dbn NBDB -recover -staging`
   
2. Stop and restart NetBackup, as follows:
   
   **UNIX:**
   
   `/usr/openv/netbackup/bin/bp.kill_all`
   `/usr/openv/netbackup/bin/bp.start_all`
   
   **Windows:**
   
   `install_path\NetBackup\bin\bpdowm`
   `install_path\NetBackup\bin\bpup`

To recover relational database files from staging if the database is corrupted

1. If the NetBackup services are running, stop them as follows:
   
   **UNIX:** `/usr/openv/netbackup/bin/bp.kill_all`
   
   **Windows:** `install_path\NetBackup\bin\bpdowm`
   
2. Move the *.db and *.log files from the following database file directories to a temporary directory:
   
   **UNIX:** `/usr/openv/db/data`
   
   **Windows:** `C:\Program Files\Veritas\NetBackupDB\data`
   
3. Configure SQL Anywhere so that it does not try to start automatically when the host is started, as follows:
   
   **Linux:** `/usr/openv/db/bin/nbdb_admin -auto_start NONE`
   
   **Windows:** `install_path\NetBackup\bin\nbdb_admin -auto_start NONE`
   
4. Start the SQL Anywhere server, as follows:
   
   **UNIX:** `/usr/openv/netbackup/bin/nbdbms_start_stop start`
   
   **Windows:** `install_path\NetBackup\bin\bpup -e SQLANYs_VERITAS_NB`
   
5. Create an empty database, as follows:
   
   **UNIX:** `/usr/openv/db/bin/create_nbdb -drop`
   
   **Windows:** `install_path\NetBackup\bin\create_nbdb -drop`
6 Stop and restart NetBackup, as follows:
   UNIX and Linux:
   
   /usr/openv/netbackup/bin/bp.kill_all
   /usr/openv/netbackup/bin/bp.start_all

   Windows:
   
   install_path\NetBackup\bin\bpdown
   install_path\NetBackup\bin\bpup

7 Run the NetBackup `tpext` command to update the device mapping files, as follows:
   UNIX: /usr/openv/volmgr/bin/tpext -loadEMM
   Windows: install_path\Volmgr\bin\tpext -loadEMM

8 If you used the `nbdb_move` command to relocate NetBackup database files, re-create the directories where the files were located when you backed up the catalog.

9 Start the NetBackup Device Manager, as follows:
   UNIX: /usr/openv/volmgr/bin/ltid -v
   Windows: Start the device manager service.

10 Run the following command on the master server to recover NBDB from staging:
    UNIX: /usr/openv/db/bin/nbdb_restore -dbn NBDB -recover -staging
    Windows: install_path\NetBackup\bin\nbdb_restore -dbn NBDB -recover -staging

11 Clean up whitelist cache for all hosts.

12 Stop and restart NetBackup services on all hosts, as follows:
   UNIX:
   
   /usr/openv/netbackup/bin/bp.kill_all
   /usr/openv/netbackup/bin/bp.start_all

   Windows:
   
   install_path\NetBackup\bin\bpdown
   install_path\NetBackup\bin\bpup

13 After the services are restarted, run the following command:
If NetBackup (or host ID-based) certificates are used in your NetBackup domain, do the following:

On a non-clustered setup:
UNIX:
/usr/openv/netbackup/bin/nbcertcmd -renewcertificate

Windows:
install_path\netbackup\bin\nbcertcmd -renewcertificate

On a clustered setup:
UNIX:
/usr/openv/netbackup/bin/nbcertcmd -renewcertificate -cluster

Windows:
install_path\netbackup\bin\nbcertcmd -renewcertificate -cluster

If external CA-signed certificates are used in your NetBackup domain, do the following:

On a non-clustered setup
UNIX:
/usr/openv/netbackup/bin/nbcertcmd -enrollCertificate

Windows:
install_path\netbackup\bin\nbcertcmd -enrollCertificate

On a clustered setup:
UNIX:
/usr/openv/netbackup/bin/nbcertcmd -enrollCertificate -cluster

Windows:
install_path\netbackup\bin\nbcertcmd -enrollCertificate -cluster

If the command fails with the exit status 5988, refer to the following topic:
See “Steps to carry out when you see exit status 5988 during catalog recovery” on page 281.
About processing the relational database in staging

A recovery of the NetBackup image files and configuration files also restores the NetBackup relational database (NBDB) to the staging directory. You can use the following NetBackup commands to further process the NBDB database if required:

**cat_import**

Use `cat_import` to import the image metadata that is in the legacy flat file format into an NBDB relational database. The NBDB database can be the actual production DB or an NBDB in a different NetBackup domain.

**cat_export**

Use `cat_export -staging` to extract the image metadata from the relational database. It writes the data to the `db.export` directory in the legacy flat file format. You can export all of the image metadata or a subset of the image metadata by client or backup ID. Then, you can use the `cat_import` command to insert the data into another NBDB database. *Another NBDB* can be the actual production DB or an NBDB in a different NetBackup domain.

**nbdb_restore -staging**

Use `nbdb_restore -staging` to recover the relational database from the staging directory.

See "Recovering the NetBackup relational database files from staging" on page 267.

**nbdb_unload -staging**

Use `nbdb_unload -staging` to unload the media table and related tables to a set of flat files. Then, you can use SQL tools to insert the subset of data into another NBDB. *Another NBDB* can be the actual production DB or an NBDB in a different NetBackup domain.

---

**Warning:** Veritas recommends that you manipulate or process the NetBackup relational database only when directed to do so by a Veritas Support Representative. For help with NetBackup domain merges and splits, contact the Veritas Information Management Consulting Services:

http://www.veritas.com/business/services/consulting_services.jsp

More information about the commands is available.

See the *NetBackup Commands Reference Guide*:

http://www.veritas.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 4-5
- Windows: Table 4-6

**Table 4-5** To recover the NetBackup catalog on UNIX when NetBackup Access Control is configured

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>If recovering to a master server on which NBAC is configured and operational, disable NBAC (that is, set it to PROHIBITED mode).</td>
<td>See the <em>NetBackup Security and Encryption Guide</em>: <a href="http://www.veritas.com/docs/DOC5332">http://www.veritas.com/docs/DOC5332</a></td>
</tr>
<tr>
<td>Step 2</td>
<td>Recover the NetBackup catalog from the online catalog backup using the Catalog Recovery Wizard or the <code>bprecover</code> command.</td>
<td>See “About recovering the entire NetBackup catalog” on page 233.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure NetBackup to use NBAC by setting it to AUTOMATIC or REQUIRED as per the security level desired.</td>
<td>See the <em>NetBackup Security and Encryption Guide</em>: <a href="http://www.veritas.com/docs/DOC5332">http://www.veritas.com/docs/DOC5332</a></td>
</tr>
<tr>
<td>Step 4</td>
<td>Restart NetBackup.</td>
<td><code>/usr/openv/netbackup/bin/bp.kill_all</code> and <code>/usr/openv/netbackup/bin/bp.start_all</code></td>
</tr>
</tbody>
</table>

**Table 4-6** To recover the NetBackup catalog on Windows when NetBackup Access Control is configured

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>If recovering to a master server on which NBAC is configured and operational, disable NBAC (that is, set it to PROHIBITED mode).</td>
<td>See the <em>NetBackup Security and Encryption Guide</em>: <a href="http://www.veritas.com/docs/DOC5332">http://www.veritas.com/docs/DOC5332</a></td>
</tr>
<tr>
<td>Step 2</td>
<td>Stop the NetBackup services.</td>
<td><code>install_path\Veritas\NetBackup\bin\bpdowm.exe</code></td>
</tr>
</tbody>
</table>
To recover the NetBackup catalog on Windows when NetBackup Access Control is configured (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>In Windows, change the startup type of the NetBackup Authentication Service and NetBackup Authorization Service to Disabled.</td>
<td>Instructions for configuring Microsoft Windows are beyond the scope of the NetBackup documentation. Refer to the appropriate Microsoft documentation.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Start the NetBackup services.</td>
<td>install_path\Veritas\NetBackup\bin\bpup.exe</td>
</tr>
<tr>
<td>Step 5</td>
<td>Recover the NetBackup catalog from the online catalog backup using the bprecover command. The NetBackup Authentication Service and NetBackup Authorization Service should be in the Disabled mode.</td>
<td>See “About recovering the entire NetBackup catalog” on page 233.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In Windows, change the startup type of the NetBackup Authentication Service and NetBackup Authorization Service to Automatic.</td>
<td>Instructions for configuring Microsoft Windows are beyond the scope of the NetBackup documentation. Refer to the appropriate Microsoft documentation.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Configure NetBackup to use NBAC.</td>
<td>The procedure depends on the environment, as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 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: bpnbaz -setupmaster This command provisions the Windows registry on all nodes with the required entries for NBAC.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ For recovery to a new installation, run the following command on the NetBackup master server: bpnbaz -setupmaster</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ For recovery in an existing environment, set NBAC to AUTOMATIC or REQUIRED as per the security level desired.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See the NetBackup Security and Encryption Guide:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.veritas.com/docs/DOC5332">http://www.veritas.com/docs/DOC5332</a></td>
</tr>
<tr>
<td>Step 8</td>
<td>Restart NetBackup.</td>
<td>install_path\Veritas\NetBackup\bin\bpdon.exe install_path\Veritas\NetBackup\bin\bpup.exe</td>
</tr>
</tbody>
</table>

See “About recovering the NetBackup catalog” on page 225.
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.
       ```bash
       nbcatsync -sync_dr_file disaster_recovery_file
       ```

2. Run the following NetBackup command to recover the catalog:
   ```bash
   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:

   ```bash
   bpimport -drfile -id media_id -drfile_dest fully_qualified_dir_name
   ```

   This command recovers all disaster recovery files from the specified media ID and places them in the specified directory. The ID can be either a tape media ID or the fully qualified location of a disk storage unit.

4. Verify that the correct disaster recovery file is available in the specified directory and that it is available from the NetBackup master server.

5. Continue with the normal catalog recovery procedure by running the Catalog Recovery Wizard or bprecover command, providing the disaster recovery file location when prompted.

Refer to the email as your primary source for recovery instructions, because they are the most current instructions for recovering your catalog. The instructions are sent when the catalog backup is completed, or when a catalog backup image is duplicated.

**Note:** If you restore catalog files directly by using bprestore on a Solaris system, use the following path: `/opt/openv/netbackup/bin/bprestore`.

The name of the online catalog backup policy is CatalogBackup. The email is written to the following file:

```
/storage/DR/CatalogBackup_1123605764_FULL
```

The file name itself indicates if the backup was full or not.

See “NetBackup disaster recovery email example” on page 229.
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:

   - `master_server`: Use the exact name that is specified in NetBackup configuration for the master server.
   - `media_server`: The location of the robot or disk storage unit that is used for catalog backup.
   - `timestamp`: The four most significant digits in the DR file name and six zeroes attached.
   - `media`: The location of the catalog backup media as specified by the disaster recovery file under the FRAGMENT keyword.
   - `backup_id`: Found in the DR file under BACKUP_ID.

**Example:**

file: Hot_Backup_1122502016_INCR

timestamp: 1122000000
4. Create the DR recovery directory on the master server.

UNIX:

/usr/openv/netbackup/db/images/master_server/timestamp/tmp

Windows:

C:\Program Files\VERITAS\NetBackup\db\images\master_server\timestamp\tmp

Copy the DR file to the newly created directory.

5. Edit the DR file in `netbackup/db/images/master_server/timestamp/tmp` as follows:
   - Change the value of `IMAGE_TYPE` to 1.
   - Change the value of `TIR_INFO` to 0.
   - Change the value of `NUM_DR_MEDIAS` to 0.
   - Remove ALL lines containing `DR_MEDIA_REC`.

6. If your catalog recover media is on tape, run the `vmquery` command to assign the media to the media server.

   `vmquery -assigntohost media timestamp master_server`

   Example:

   `vmquery -assigntohost DL005L 1122000000 klingon`

7. To recover the catalog .f file from the hot catalog backup, run a Phase II import on the media that is specified by the disaster recovery file.

   `bpimport -server master_server -backupid backup_id`

8. If your catalog backup was incremental, recover all the other catalog backup images up to and including the most recent Full Catalog backup.

   - Open the Backup, Archive, and Restore client interface for NetBackup. Select NBU-Catalog as the policy type. Set the source clients and destination clients to your master server.
   - Search the backups and restore all files that are located in the following directory:

     `install_path/netbackup/db/images/master_server`

   - Verify that all files are restored successfully on the master server.
9 Restore your critical data by using the Backup, Archive, and Restore client interface or the command line.

- Restore the catalog backup images for each media server which requires data recovery.

- To restore the backup images, select NBU-Catalog as the policy type. Source and destination clients should be your master server. Refresh your view in the BAR GUI. Traverse the file system for the master server to the following:

  \[\text{install\_path}/\text{netbackup/db/images}\]

  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:

  \[\text{bprecover -r -nbdb}\]

  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:

  \[\text{bpmedia -freeze -m media -h master\_server}\]

  Run \text{bpmedialist} to verify that the media is frozen.
13 Recover your policies and configuration data on each master server and media server.

Before recovering NetBackup policy files, ensure that you have recovered all of your critical data, or protected the media that contains your critical data. When policy information is recovered, NetBackup starts to run the scheduled jobs that may overwrite the media that was written after the last catalog backup.

Open the Backup, Archive, and Restore client interface for NetBackup and select NBU-Catalog as the policy type.

For each server to be restored, set the source clients and destination clients to your server, starting with the master server.

Restore all files that are backed up by the hot catalog backup on each server.

14 Clean up whitelist cache for all hosts.

15 Stop and restart the NetBackup services on all hosts.

16 After the services are restarted, run the following command:

- If NetBackup (or host ID-based) certificates are used in your NetBackup domain, do the following:
  
  On a non-clustered setup:
  
  UNIX:
  
  `/usr/openv/netbackup/bin/nbcertcmd -renewcertificate`
  
  Windows:
  
  `install_path\netbackup\bin\nbcertcmd -renewcertificate`

  On a clustered setup:
  
  UNIX:
  
  `/usr/openv/netbackup/bin/nbcertcmd -renewcertificate -cluster`
  
  Windows:
  
  `install_path\netbackup\bin\nbcertcmd -renewcertificate -cluster`

- If external CA-signed certificates are used in your NetBackup domain, do the following:
  
  On a non-clustered setup
  
  UNIX:
  
  `/usr/openv/netbackup/bin/nbcertcmd -enrollCertificate`

  Windows:
  
  `install_path\netbackup\bin\nbcertcmd -enrollCertificate`
install_path\netbackup\bin\nbcertcmd -enrollCertificate

On a clustered setup:
UNIX:

/usr/openv/netbackup/bin/nbcertcmd -enrollCertificate -cluster

Windows:

install_path\netbackup\bin\nbcertcmd -enrollCertificate -cluster

If the command fails with the exit status 5988, refer to the following topic:
See “Steps to carry out when you see exit status 5988 during catalog recovery” on page 281.

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.

See “About recovering the NetBackup catalog” on page 225.

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 225.
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`

Steps to carry out when you see exit status 5988 during catalog recovery

Use this procedure when you come across exit status 5988 during catalog backup.

To resolve the issue

1. Run the following command:

   Windows: `install_path\NetBackup\bin\nbcertcmd -ping`

   UNIX: `/usr/openv/netbackup/bin/nbcertcmd -ping`

   - If it is executed successfully, proceed to the next step.
   - If it fails with status 8509 (The specified server name was not found in the web service certificate), follow the steps in this article:
Proceed to the next step.

2 Perform the user logon on the master server. Use the following command:

```
install_path\netbackup\bin\bnpbat -login -loginType WEB
```

For example:

```
install_path\netbackup\bin\bnpbat -login -loginType WEB
```

Authentication Broker [abc.example.com is default]:
Authentication port [0 is default]:
Authentication type (NIS, NISPLUS, WINDOWS, vx, unixpwd, ldap) [WINDOWS is default]:
Domain [abc.example.com is default]:
Login Name [administrator is default]:
Password:
Operation completed successfully.

3 Note the value of key Client_Name for the master server. For a clustered master server, note the value of key Cluster_Name.

This value can be found at:

Windows:
HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\NetBackup\CurrentVersion\Config

UNIX: /usr/openv/netbackup/bp.conf

This value can be either a FQDN or a short name.

For example:

abc.example.com

4 Note the host ID of the master server. You can obtain its value by running the following command:

```
install_path\netbackup\bin\nbcertcmd -listCertDetails
```

For a clustered master server, run the following command:

```
install_path\netbackup\bin\nbcertcmd -listCertDetails -cluster
```

This command can return multiple records (if only one record is returned, select the host ID provided in that record).

- If the host name that was obtained in step 3 is the FQDN, pick the record where the “Issued By” entry matches its short name.
- If the host name that was obtained in step 3 is the short name, pick the record where the “Issued By” entry matches its FQDN.
Example:

```
install_path\netbackup\bin\nbcertcmd -listCertDetails
```

Master Server : abc
Host ID : 78f9eed4-xxxx-4c6a-bb40-xxxxxxxxxx
Issued By : /CN=broker/OU=root@abc/O=vx
Serial Number : 0x62e108c9000000c
Expiry Date : Aug 21 08:42:54 2018 GMT

Master Server : xyz
Host ID : 5a8dde7b-xxxx-4252-xxxx-d3bedee63e0a
Issued By : /CN=broker/OU=root@xyz.example.com/O=vx
Serial Number : 0x6ede87a7000000a
Expiry Date : Aug 21 09:52:13 2018 GMT
Operation completed successfully.

Here, two records are fetched.
For the first record, the issuer name in the “Issued By” field matches the short name of the client_name obtained in step 3.
Hence select the host ID that is provided in the record.

5 Add host ID-to-host name mapping for the master server. Map the host ID obtained in step 4 with the host name obtained in step 3.

Use the following command:

```
install_path\netbackup\bin\nbhostmgmt -a -i host ID -hm hostname
```

Alternately, you can also add this host-ID-to-host name mapping using the NetBackup Administration Console. Use the Security Management > Host Management > Hosts tab.

6 Do the following to renew the certificates:

- To renew the NetBackup (or host ID-based) certificate of the master server, use the following command:

  `install_path\netbackup\bin\nbcertcmd -renewCertificate`
For a clustered master server, run the following command:

```
install_path\netbackup\bin\nbcertcmd -renewCertificate -cluster
```
A

about restoring disaster recovery package 218
acstest 184
AdvancedDisk 193, 204
Alternate client restores
  host.xlate file 72
archiving
  for NBCC 173
  for nbsu 170
Auth User
  for PBX 101
auto-configuration problems 31

B

Bare Metal Restore 191, 194, 210
bp.conf
  SERVER entries 124
bp.kill_all 103–104
bp.start_all 104
bpdown command 103–104, 206, 209
bpps 23
bpup command 104
bundling
  NBCC output 173
  nbsu output 170

C

catalog backups
  disaster recovery packages 189
catalog recovery
  catalog image files 247
  clustered master server 247
certificate revocation list
  determining if a certificate is revoked 64
client
  NetBackup
    configured name 70
    installation problems 29
    multiple hostnames 69
    peername 70
client (continued)
  NetBackup (continued)
    testing configuration 34, 38
Client Properties dialog 87
client, NetBackup
  Windows disk recovery 210
communications problems
  PC clients 46
  UNIX clients 42
compression
  for NBCC 173
  for nbsu 170
configuration problems 29

D

detected logs
  analysis utilities 161
detected
  NBCC 172
  nbsu 168
device configuration problems 31
Device Configuration Wizard 205
disk configuration
  preparing for disaster 187
disk recovery package 189
disk full 87
disk recovery
  Windows client 210
disk space
  for logs and temporary files 126
duplex mode and performance 122

E

E-mail 192
extra disk space for logs and temporary files 126

F

full disk 87
full duplex mode 122
Half duplex and poor performance 122
host name entries
  checking 73
Host Properties 87
host validation logs 106
host.xlate file 72

ifconfig
  for checking NIC duplex mode 123
inetd 29
Information E-mail 192
installation
  Linux 29
installation problems 28
ipconfig
  for checking NIC duplex mode 123

jobs
  queued for long periods 87

KMS configuration
  troubleshooting 154

Linux 29
log analysis utilities
  debug logs 161
  limitations 164
  output format 165

master server
  test procedure 34, 38
media server
  test procedure 38

NB_dbsrv daemon 88
NBCC
  archiving and compression 173
  does the following 171
  introduction 171

NBCC (continued)
  location of 171
  nbcc-info.txt file 172
  Notes on running 172
  output 173
  progress display 173
  troubleshooting 172
  when to use 171
  nbcc-info.txt file 172
  nbdb_move 205
  nbemm 24
  nbftclnt
    and bp.conf 124
  nbjm 24
  nbpem 24
  nbrrb 24, 88
  nbsu
    archiving and compression 170
    bundling 170
    introduction 167
    location of 167
    nbsu_info.txt file 168
    output files 169
    progress display 170
    troubleshooting 168
    when to use 167
  nbsu_info.txt file 168
NetBackup
  if unresponsive 87
NetBackup Administration Console
  errors 125
NetBackup Authentication service
  start and stop 26
NetBackup Client Service
  start and stop 26–27
NetBackup Compatibility service
  start and stop 26
NetBackup consistency check
  see NBCC 171
NetBackup Database Manager service
  start and stop 26
NetBackup Deduplication Engine service
  start and stop 27
NetBackup Deduplication Manager service
  start and stop 27
NetBackup Device Manager service
  start and stop 27
NetBackup Discovery Framework service
  start and stop 26
NetBackup Enterprise Media Manager service
start and stop 26
NetBackup Event Manager service
start and stop 26
NetBackup Indexing Manager service
start and stop 26
NetBackup Job Manager service
start and stop 26
NetBackup Legacy Client Service
start and stop 27
NetBackup Policy Execution Manager service
start and stop 26
NetBackup Relational Database Manager 88
NetBackup Relational Database Manager Service
start and stop 26
NetBackup Remote Manager and Monitor Service
start and stop 26–27
NetBackup Request Daemon service
start and stop 26
NetBackup Resource Broker service
start and stop 26
NetBackup Service Layer service
start and stop 26
NetBackup Service Monitor service
start and stop 26
NetBackup Storage Lifecycle Manager service
start and stop 26
NetBackup Support Utility
see nbsu 167
NetBackup Vault Manager service
start and stop 26
NetBackup Volume Manager service
start and stop 26–27
NetBackup Web Management Console service
start and stop 26
NetBackup Deduplication Multi-Threaded Agent service
start and stop 27
network connections
multiple 69
network interface cards 122
network problems
PC clients 46
UNIX clients 42
NIC cards and full duplex 122

P
patches (installing during recovery) 212
PBX
Auth User 101
logging 101
Secure Mode 101–102
starting 100
starting/stopping 103
troubleshooting 98
pbx_exchange 100
pbxcfg 100
peer validation failure 56
preliminary troubleshooting procedure 20
Private Branch Exchange (PBX) 98
Private Branch Exchange service
start and stop 26–27
procedures
recovery
Windows client disk 210
troubleshooting
communications problems 42, 46
host names and services 73
installation and configuration 28
introduction 18
master server and clients 34
media server and clients 38
preliminary 20

Q
queued jobs 87

R
recording information 11
recovery procedures
  Windows client disk 210
RedHat 29
relational database 88
remote host validation issues
troubleshooting 105
restoring disaster validation issues
UNIX 222
Windows 219
revoked certificate failure 54–55
robotic test utility 183
acstest 184
tldtest 183–184
robtest 183–184

O
OpenStorage 193, 204
SAN client and bp.conf 124
Secure Mode for PBX 101
server
  installation problems 28
  test procedure for master 34, 38
  test procedure for media server 38
SERVER entries
  bp.conf 124
services entries
  checking 73
SharedDisk 193, 204
slow performance and NIC cards 122
starting NetBackup processes 104
stderr 125
stdout 125
stopping NetBackup processes 103–104
storage units 124
SuSE 29

utility
  robotic test 183

vnetd proxy
  troubleshooting 52
vnetd proxy connections
  peer validation failure 56
  revoked certificate failure 54–55
  troubleshooting 50
Volume Configuration Wizard 206
vxpbx_exchanged 103

web services account
  during recovery 194, 197, 201, 203, 205, 208, 214, 216

xinetd 29