NetBackup™ Troubleshooting Guide

UNIX, Windows, and Linux

Release 11.2

VERITAS
now part of Cohesity

NetBackup™ Troubleshooting Guide

Last updated: 2026-05-28

Legal Notice

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1

Introduction

This chapter includes the following topics:

Additional resources on NetBackup logging and status code information

The following material is available in the NetBackup Logging Reference Guide:

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

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.

Table 1-1 Steps for troubleshooting NetBackup problems

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

Step	Action	Description
Step 3	Record all information	Capture potentially valuable information: ■ NetBackup progress logs ■ NetBackup Reports ■ NetBackup Utility Reports ■ NetBackup debug logs ■ Media and Device Management debug logs ■ On UNIX NetBackup servers, check for error or status messages in the system log or standard output. ■ Error or status messages in dialog boxes ■ On Windows, NetBackup servers, check for error or status information in the Event Viewer Application and System log. Record this information for each try. Compare the results of multiple tries. A record of tries is also useful for others at your site and for Cohesity 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.
Step 4	Correct the problem	After you define the problem, use the following information to correct it: ■ Take the corrective action that the status code or message recommends. See the Status Codes Reference Guide. ■ If no status code or message exists, or the actions for the status code do not solve the problem, try these additional troubleshooting procedures: See "Troubleshooting NetBackup problems" on page 20.
Step 5	Complete a problem report for Cohesity Technical Support	If your troubleshooting is unsuccessful, prepare to contact Cohesity Technical Support by filling out a problem report. See "Problem report for Technical Support" on page 12. See "About gathering information for NetBackup-Java applications" on page 13. On UNIX systems, the `/usr/openv/netbackup/bin/goodies/support` script creates a file containing data necessary for Cohesity Technical Support to debug any problems you encounter. For more details, consult the usage information of the script by means of the `support -h` command.
Step 6	Contact Cohesity Technical Support	The Cohesity Technical Support website has a wealth of information that can help you solve NetBackup problems. Access Cohesity Technical Support at the following URL: https://support.cohesity.com/s/

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 primary and the media server are one and the same. Ignore references to a media server on a different host.

Problem report for Technical Support

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

Date: _____

Record the following product, platform, and device information:

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

  _____
  _____
  _____
  _____
  _____
  _____

Define the problem.

_____

_____

_____

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

_____

_____

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

_____

_____

_____

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

_____ Initial installation

_____ Configuration change (explain)

_____ System change or problem (explain)

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

_____

_____

_____

Logs or other failure data you have saved:

_____ All log entries report

_____ Media and Device Management debug logs

_____ NetBackup debug logs

_____ System logs (UNIX)

_____ Event Viewer Application and System logs (Windows)

Ways that you can communicate with us:

_____ MyVeritas.com - case management portal

_____ mft.veritas.com - File transfer portal for https uploads

_____ sftp.veritas.com - File transfer server for sftp transfers

For more information, see the following:

https://support.cohesity.com/s/article/article-100038665

_____ email

_____ WebEx

About gathering information for NetBackup-Java applications

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

The following scripts are available for gathering information:

`jnbSA` (NetBackup-Java administration application startup script)	Logs the data in a log file in `/usr/openv/netbackup/logs/user_ops/nbjlogs`. At startup, the script tells you which file in this directory it logs to. Normally, this file does not become very large (usually less than 2 KB). Consult the file `/usr/openv/java/Debug.properties` for the options that can affect the contents of this log file.
NetBackup-Java administration application on Windows	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`*`\Cohesity NetBackup\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`*`\Cohesity NetBackup\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`	Queries the host and gathers appropriate diagnostic information about NetBackup and the operating system. See "About the NetBackup support utility (nbsu)" on page 219.

The following example describes how you can gather troubleshooting data for Cohesity 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.

UNIX/Linux only: Still no response after several minutes.	Run `/usr/openv/java/get_trace` under the account where you started the Java application. This script causes a stack trace to write to the log file. For example, if you started `jnbSA` from the root account, start `/usr/openv/java/get_trace` as root. Otherwise, the command runs without error, but fails to add the stack trace to the debug log. This failure occurs because root is the only account that has permission to run the command that dumps the stack trace.
Get data about your configuration.	Run 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 Cohesity Technical Support	Provide the log file and the output of the `nbsu` command for analysis.

Chapter 2

Troubleshooting procedures

This chapter includes the following topics:

- 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 web UI and 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 issues with external certificate configuration
- 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
- Troubleshooting issues with email notifications for Windows systems
- Troubleshooting issues with KMS configuration
- Troubleshooting 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 Cohesity Technical Support site has a wealth of information that can help you solve NetBackup problems.

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 20. See "Verifying that all processes are running on UNIX or Linux 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 primary 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 primary server and client" on page 77.
- See "Example of host name and service entries on UNIX primary 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 investigate first and branches to other procedures as appropriate. These procedures do not try to cover every problem that can occur. However, they do recommend the methods that usually result in successful problem resolution.

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

Table 2-1 Steps for troubleshooting NetBackup problems

Step	Action	Description
Step 1	Verify operating systems and peripherals.	Ensure that your servers and clients are running supported operating system versions and that any peripherals you use are supported. See the NetBackup Compatibility Lists. In addition, the NetBackup release notes include a section "Required operating system patches and updates for NetBackup" that you should review. The release notes for your release are available here: https://support.cohesity.com/s/article/article-100040135

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

Step	Action	Description
Step 2	Use reports to look for errors.	Use the **All log entries** report and look 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* chapter in the NetBackup Web UI Administrator's Guide. If the problem involved a backup or archive, review the **Status of Backups** report. This report gives you the status code. (This report is available in the NetBackup Administration Console.) If you find a status code or message in either of these reports, perform the recommended corrective actions. See the Status Codes Reference Guide.
Step 3	Review the operating system logs.	Review the system log (UNIX/Linux) or the **Event Viewer** Application and System log (Windows) if the problem pertains to media or device management and one of the following is true: ■ NetBackup does not provide a status code. ■ You cannot correct the problem by following the instructions in NetBackup status codes and messages. ■ You cannot correct the problem by following the instructions in media and device management status codes and messages. These logs can show the context in which the error occurred. The error messages are usually descriptive enough to point you to a problem area.
Step 4	Review the debug logs.	Read the applicable enabled debug logs and correct any problems you detect. If these logs are not enabled, enable them before you retry the failed operation. See 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.

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

Step	Action	Description
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 253. See "About disk recovery procedures for Windows" on page 263.
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/Linux systems, use the `df` command to view disk partition information. On Windows systems, use Disk Manager or Explorer. Review the following disk partitions: ■ The partition where NetBackup software is installed. ■ On the NetBackup primary 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. More information is available on changing the logging level. See the NetBackup Logging Reference Guide.
Step 10	Determine which daemons or processes are running.	Follow the procedures for UNIX/Linux or Windows NetBackup servers. See "Verifying that all processes are running on UNIX or Linux servers" on page 22. See "Verifying that all processes are running on Windows servers" on page 25.

Verifying that all processes are running on UNIX or Linux servers

For NetBackup to operate properly, the correct set of processes (daemons) must be running on your UNIX or Linux 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 or Linux servers

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

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

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

Primary server

```
bpcd -standalone                    nbpem
bpcompatd                           nbproxy
bpdbm                               nbrb
bpjobd                              nbrmms
bprd                                nbsl
java                                nbstserv
nbars                               nbsvcmon
nbatd                               nbwmc
nbdisco (discovery manager)         pbx_exchange
nbemm                               postgres
nbevtmgr                            vmd
nbim (index manager)                vnetd -standalone
nbjm                                nbmqbroker
```

Media server

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

Note: Additional processes may also need to be running if other add-on products, database agents, and so forth are installed. For additional assistance, see https://support.cohesity.com/s/article/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/stopltid
```

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

Step	Action	Description
Step 1	Start all services on the primary servers.	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 *install_path*\NetBackup\bin\bpup.exe. Services on primary 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 Scale-Out Relational Database Connection Pool Service ■ NetBackup Scale-Out 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 ■ NetBackup Messaging Broker service **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://support.cohesity.com/s/article/article-100002166

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

Step	Action	Description
Step 2	Start all services on the media servers.	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 Web UI Administrator's Guide. If these processes are not running, stop and restart the NetBackup **Device Manager** service. Use the NetBackup **Activity monitor** or the Services application in the Windows Control Panel.

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

Step	Action	Description
Step 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 primary 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.

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

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

Step	Action	Description
Step 2	Determine if you can install NetBackup client software on the clients.	**Note:** Before you install or use NetBackup on a Linux client, verify that the `bpcd -standalone` and `vnetd -standalone` services are started on that computer. These services ensure proper communication between the NetBackup primary 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.

Table 2-4 Steps for troubleshooting configuration problems

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

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

Step	Action	Description
Step 3	Retry the operation and check for status codes and messages.	If you found and corrected any configuration problems, retry the operation and check for NetBackup status codes or messages in the following: ■ Check the **All log entries** report for NetBackup errors for the appropriate time period. This report can show the context in which the error occurred. Often it provides specific information, which is useful when the error can result from a variety of problems. If the problem involved a backup or archive, check the 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 2-5 Recommended actions for device configuration messages

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

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

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

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

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

Testing the primary 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 Web UI Administrator's Guide, Volume I.

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

Step	Action	Description
Step 1	Enable debug logs.	Enable the appropriate debug logs on the primary server. For information on logging, see the *NetBackup Logging Reference Guide*. If you do not know which logs apply, enable them all until you solve the problem. Delete the debug log directories when you have resolved the problem.
Step 2	Configure a test policy.	Configure a test policy 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 primary server as the client and a storage unit that is on the primary server (preferably a nonrobotic drive). Also, configure a volume in the NetBackup volume pool and insert the volume in the drive. If you don't label the volume by using the `bplabel` command, NetBackup automatically assigns a previously unused media ID.
Step 3	Verify the daemons and services.	To verify that the NetBackup daemons or services are running on the primary 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. 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*.

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

Step	Action	Description
Step 6	Consult information besides the debug logs.	If the debug logs do not reveal the problem, check the following: ■ Systems Logs 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.
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 235. 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 primary server and clients *(continued)*

Step	Action	Description
Step 11	Backup and restore a file.	Start a user backup and restore of a file by using the client-user interface on the primary server. Monitor the status and the progress log for the operation. If successful, this operation verifies that the client software is functional on the primary 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 primary server and clients *(continued)*

Step	Action	Description
Step 14	Verify communication between the client and the primary server.	Perform a user backup and then a restore from the client that is specified in step 8. These actions verify communications between the client and the primary 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.
Step 15	Test other clients or storage units.	When the test policy operates satisfactorily, repeat specific steps as necessary to verify other clients and storage units.
Step 16	Test the remaining policies and schedules.	When all clients and storage units are functional, test the remaining policies and schedules that use storage units on the primary server. If a scheduled backup fails, check the **All Log Entries** report for errors. Then follow the recommended actions as is part of the error status code.

Testing the media server and clients

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

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

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

Step	Action	Description
Step 1	Enable legacy debug logs.	Enable appropriate legacy debug logs on the servers, 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.

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

Step	Action	Description
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 primary server. Also, verify that all Media and Device Management daemons or services are running on the media server. To perform this check, do one of the following: ■ On a UNIX system, run: `/usr/openv/netbackup/bin/bpps -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 primary 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 primary server processes `nbpem`, `nbjm`, `nbrb`, EMM server process `nbemm`, and media server processes `bpcd`, `bpbrm`, `bpdm`, and `bptm`. ■ Communications between media server process `bpbrm`, `bpdm`, `bptm`, and client processes `bpcd` and `bpbkar`. For the failures that relate to drives or media, ensure that the drive is in an UP state and that the hardware functions.
Step 5	Verify communication between the primary server and the media servers.	If you suspect a communications problem between the primary 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)*

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

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

Step	Action	Description
Step 7	Include a robotic device in the test policy.	If you previously configured a non-robotic drive and a robot was attached to your media server, change the test policy to name the robot. Also, add a volume for the robot to the EMM server. Verify that the volume is in the NetBackup volume pool and in the robot. Start with step 3 to repeat this procedure for a robot. This procedure verifies that NetBackup can find the volume, mount it, and use the robotic drive. If a failure occurs, check the NetBackup **All Log Entries** report. Look for any errors that relate to devices or media. See the NetBackup Administrator's Guide, Volume I. If the **All Log Entries** report doesn't help, check the following: ■ On a UNIX server, the system logs on the media server ■ `vmd` debug logs on the EMM server for the robot ■ On a Windows system, the **Event Viewer** Application and System log In an initial configuration, verify that the robotic drive is configured correctly. Do not use a robot number that is already configured on another server. Try the test utilities. See "About the robotic test utilities" on page 235. 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 2-8 Steps for resolving network communication problems with UNIX clients

Step	Action	Description
Step 1	Create debug log directories.	During communication retries, the debug logs provide detailed debug information, which can help you analyze the problem. Create the following directories: ■ `bpcd` (on the primary server and clients) ■ `vnetd` (on the primary server and clients) ■ `bprd` (on the primary server) Use the `bprd` log directory to debug client to primary server communication, not client to media server communication problems.
Step 2	Test a new configuration or modified configuration.	If this configuration is a new or a modified configuration, do the following: ■ Check any recent modifications to ensure that they did not introduce the problem. ■ Ensure that the client software was installed and that it supports the client operating system. ■ Check the client names, server names, and service entries in your NetBackup configuration as explained in the following topic: See "Verifying host name and service entries in NetBackup" on page 73. You can also use the `hostname` command on the client to determine the host name that the client sends with requests to the primary server. Check the `bprd` debug log on the primary server to determine what occurred when the server received the request.

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

Step	Action	Description

Step 3	Verify name resolution.	To verify name resolution, run the following command on the primary 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 primary 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)*

Step	Action	Description

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 primary 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)*

Step	Action	Description

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 primary server(s) and media server(s), to test communication to the client.

Step 7	Identify the outbound socket on the server host.	On the primary 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)*

Step	Action	Description

Step 8	Confirm that the telnet connection reaches this client host.	On the primary 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 primary server.	To verify client to primary server communications, use the `bpclntcmd` utility. When `-pn` and `-sv` run on a NetBackup client, they initiate inquiries to the NetBackup primary server (as configured in the client `bp.conf` file). The primary server then returns information to the requesting client. More information is available about `bpclntcmd`. See "About the 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 primary 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:

Windows	Check the NetBackup client service port number. Start the **Backup, Archive, and Restore** interface on the client. On the **File** menu, click **NetBackup Client Properties**. In the **NetBackup Client Properties** dialog box on the **Network** tab, check the NetBackup client service port number. Verify that the setting on the **Network** tab matches the one in the services file. The `services` file is located in: `%SystemRoot%\system32\drivers\etc\services` (Windows) The values on the **Network** tab are written to the `services` file when the NetBackup client service starts.
UNIX NetBackup servers	The `bpcd` port number is in the `/etc/services` file. On Windows NetBackup servers, see the Client Properties dialog box in the **Host Properties** window. See "Using the Host properties 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 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 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 `bpclntcmd` utility to verify client to primary server communications. When the `-pn` and `-sv` options run on a client, they initiate inquiries to the primary server (configured in the server list on the client). The primary server then returns information to the requesting client.

See "About the bpclntcmd utility" on page 84.

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

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

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

Troubleshooting vnetd proxy connections

The Cohesity Network Daemon `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 Cohesity support representative.

vnetd proxy connection requirements

Note: To verify the settings for mapping NetBackup host IDs and for communication with 8.0 and earlier hosts, open the NetBackup web UI. At the top right, click **Settings > Global security**. The click on the **Secure communication** tab.

For communication within the same NetBackup domain, note these requirements:

- 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.
  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 names.
  As an alternative to the web UI, you can use the following command and option:
  Windows:
  install_path`\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.
  As an alternative to the web UI, you can use the following command and option:
  Windows:
  install_path`\NetBackup\bin\admincmd\nbseccmd -getsecurityconfig -insecurecommunication`
  UNIX:
  `/usr/openv/netbackup/bin/admincmd/nbseccmd -getsecurityconfig -insecurecommunication`
- The NetBackup web services on the primary server must be active. To confirm that they are active, use the following NetBackup command and option:
  Windows: *install_path*`\NetBackup\bin\nbcertcmd -ping`
  UNIX: `/usr/openv/netbackup/bin/nbcertcmd -ping`
- If the primary server is configured to use external CA-signed certificates, the hosts should enroll their external CA-signed certificates with the appropriate primary server domain.
  For more information on external CA support and certificate enrollment, refer to the *NetBackup Security and Encryption Guide*.

For Auto Image Replication, host ID-based certificates from the source primary server are required on all of the trusted primary servers in the destination domains.

If the primary server is configured to use external CA-signed certificates, ensure that trust is established between the source and target primary 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 76*xx* 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.

The following resources describe the status codes:

- The NetBackup Status Codes Reference Guide.
- In the Job details, clicking on the status code.

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
root  13608  1  0 Jun27 ?  00:00:06 /usr/openv/netbackup/bin/vnetd -proxy outbound_proxy
  -number 0
root  13610  1  0 Jun27 ?  00:00:06 /usr/openv/netbackup/bin/vnetd -proxy http_tunnel
```

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 `nbpxytnl` 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*\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 10.81.41.245:895 -> 10.81.40.148:1556
127.0.0.1:35386 -> 127.0.0.1:49429 PROXY 10.81.41.245:51325 -> 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@primary.example.com/O=vx
LOCAL_CERT_SUBJECT_COMMON_NAME = a753da9b-b1ff-4a5f-b57d-69a4e2b47e29
PEER_CERT_ISSUER_NAME = /CN=broker/OU=root@primary.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 = primary.example.com
EMM_SERVER = primary.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 primary 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\\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 primary.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@primary.example.com/O=vx
LOCAL_CERT_SUBJECT_COMMON_NAME = 7157d866-8eb2-45bb-bde8-486790c0b40c
PEER_CERT_ISSUER_NAME = /CN=broker/OU=root@primary.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:
primary.example.com, self name: connect-host: 0
        [PROXY] Encountered error (VALIDATE_PEER_HOST_PROTOCOL_RUNNING) while processing
        (ValidatePeerHostProtocol).: 1
Can't connect to host primary.example.com: cannot connect on socket (25)
```

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

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 2-9 `vnetd` proxy log files

Proxy	Component name	Originator ID
The inbound and the outbound proxies	`nbpxyhelper`	486
The HTTP tunnel	`nbpxytnl`	490

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*\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.

The following resources describe the status codes:

- The NetBackup Status Codes Reference Guide.
- In the Job details, clicking on the status code.

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 “Primary server security certificate is revoked” on page 63.

If you cannot determine the cause of problems, contact your Cohesity 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:

- `tpcommand` logs for configuration issues.
- `bptm` logs for backup and restore issues.
- `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 NetBackup Cloud Administrator’s Guide and ensure that you have met all the requirements for CRL.

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 certificate 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 primary 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 primary 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 global security settings. To verify these settings open the NetBackup web UI. At the top right, click **Settings > Global security**.

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 primary server is revoked.
- The CRL on the client, media server, or the primary server is corrupted or 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.)

6. In case of NetBackup CA-signed certificate, after you resolve the security issue, reissue the certificate for the revoked host. Certificate reissue is documented in the NetBackup Security and Encryption Guide.
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:
   - 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.
   - 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.

Primary server security certificate is revoked

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

- Jobs fail with network errors.
- Media servers deactivate spontaneously.
- The `vnetd` proxy process log files on hosts show that the primary server's certificate is revoked.
  See "Viewing the vnetd proxy log files" on page 56.
- The `bptestbpcd -host` *`primary_server`* command output may show that the primary server's certificate is revoked.
  See "Determining a NetBackup host's certificate state" on page 64.

If the primary 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 primary server's security certificate, and then return the primary server to service.
3. If you cannot resolve the issue and return the primary 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 primary server's certificate or enroll a new certificate for the primary 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 host itself	See "To verify a host's certificate" 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 primary_server_name]`

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

   To get a CRL from a NetBackup domain other than the default, specify the `-server primary_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 primary_server_name]`

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

   Use one or both of the following options if necessary:

`-cluster`	Use this option on the active node of a NetBackup primary server cluster to verify the certificate of the virtual host.
`-server`	Use this option with the *primary_server_name* argument to verify a certificate from a primary 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 primary 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

1. Open the NetBackup web UI.
2. On the left, click **Security > Certificates**.
3. Click the certificate name to examine the status 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 primary 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 primary 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, cleanup 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, name services such as NIS or 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 when making this decision.

For restores from the client, the client connects to the primary server. For example, on a UNIX computer, the primary server is the first one named in the `/usr/openv/netbackup/bp.conf` file. On a Windows computer, the primary 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 target host determines the peer host name of the connecting host. If the target host is the primary server, it also determines the client's configured name from the peer host name.

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 `getnameinfo()` network routine). This name is visible in the `bpcd` or `bprd` debug log when a connection is made as in the line:

```
bpcd: Connection from host peername ipaddress ...
```

```
bprd: Connection from host peername ipaddress ...
```

On a client, the peer host name for the connecting server must match a server or a media server entry in the local NetBackup configuration: Either as a string match or by comparison with the `getaddrinfo()` information for each server entry.

On the primary server, the comparison is more complex.

The client's configured name is then derived from the peer name by querying the `bpdbm` process on UNIX/Linux hosts, or the NetBackup Database Manager service on Windows hosts.

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 was run
- All clients in all policies

The comparison is first a string comparison. The comparison is verified by comparing the peer name to the list of client names.

If none of the comparisons succeed, a more brute force method is used, which compares all names and aliases that are found using `getaddrinfo()` for each client name in the list.

The configured name is the first comparison that succeeds.

If the comparison fails, in most cases `bprd` replaces the requesting client (as follows) with the peer name because the host names in the request are not under administrative control like the network and NetBackup configurations.

An example of a failed comparison:

The client has a new network interface and has changed the first server entry to take advantage of the new network. The name services on the primary server resolve the new source IP of the client to a peer name that is not a network alias for any client 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
- Source IP address of the connection to the server

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 either CLIENT_NAME or 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 is 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 primary 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 is true: a client has multiple network connections to the server and list or restore requests from the client fail because of a connection-related problem.

The `traceroute` (UNIX) and `tracert` (Windows) programs can often provide valuable information about the configuration of the network.

The primary 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 is unknown to the DNS on the primary server. The client and the server configurations can determine if this situation exists. The `gethostname()` function on the client may return an unqualified host name that the DNS on the primary server cannot resolve.

Although you can reconfigure name services, including the hosts file, this solution is not always desirable. For this reason, NetBackup provides a special file on the primary 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 peername 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.

- *peername* is the value to translate. This is the value to which `getnameinfo()` on the primary server resolved the source IP address from which the client connected.
- *client_as_known_by_server* is the name to substitute for *peername* when the client responds to requests. This name must be the name that is configured in the NetBackup configuration on the primary server, typically as a client in a policy. It should also be known to the name services used by primary server, and must be known to the network services of the media server that performs the backup.

This following is an example:

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

When the primary server receives a request for a configured client name (numeric key 0), the name always replaces the peer name.

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 primary 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 primary server in the list. If you add or modify server entries on the primary 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 primary 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 primary 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 primary server. If a host name is misspelled or cannot be resolved with `gethostbyname`, the following error messages are logged on the NetBackup error log:

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

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

See "Using the Host properties 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 primary server and each media server in the configuration. The primary server must be the first name in the list.
  If you add or modify `SERVER` entries on the primary server, stop and restart `bprd` and `bpdbm` before the changes take effect.
- The bp.conf of the primary server does not require the addition of other clients, other than the primary server as `CLIENT_NAME = primary 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 primary 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 primary server and client" on page 77.

See "Example of host name and service entries on UNIX primary 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.

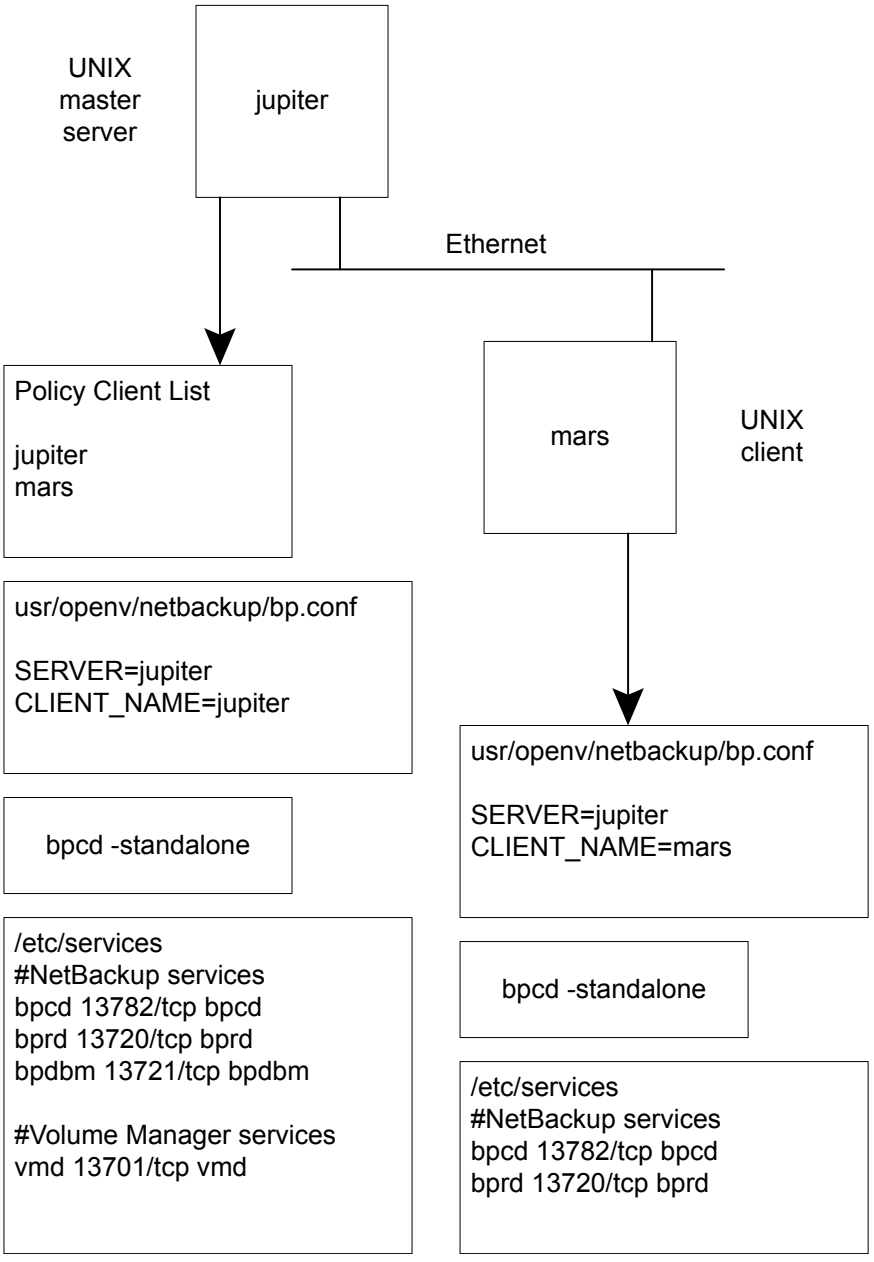
Note: FT (Fibre Transport) target devices are named based on the host name or domain name response from the device. If any alternate computer names for different VLAN network interface names appear in the SERVER/MEDIA_SERVER entries of the DNS (Domain Name System) or the host files, the primary name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

See "About the bpclntcmd utility" on page 84.

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

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

Figure 2-1 UNIX primary server and client



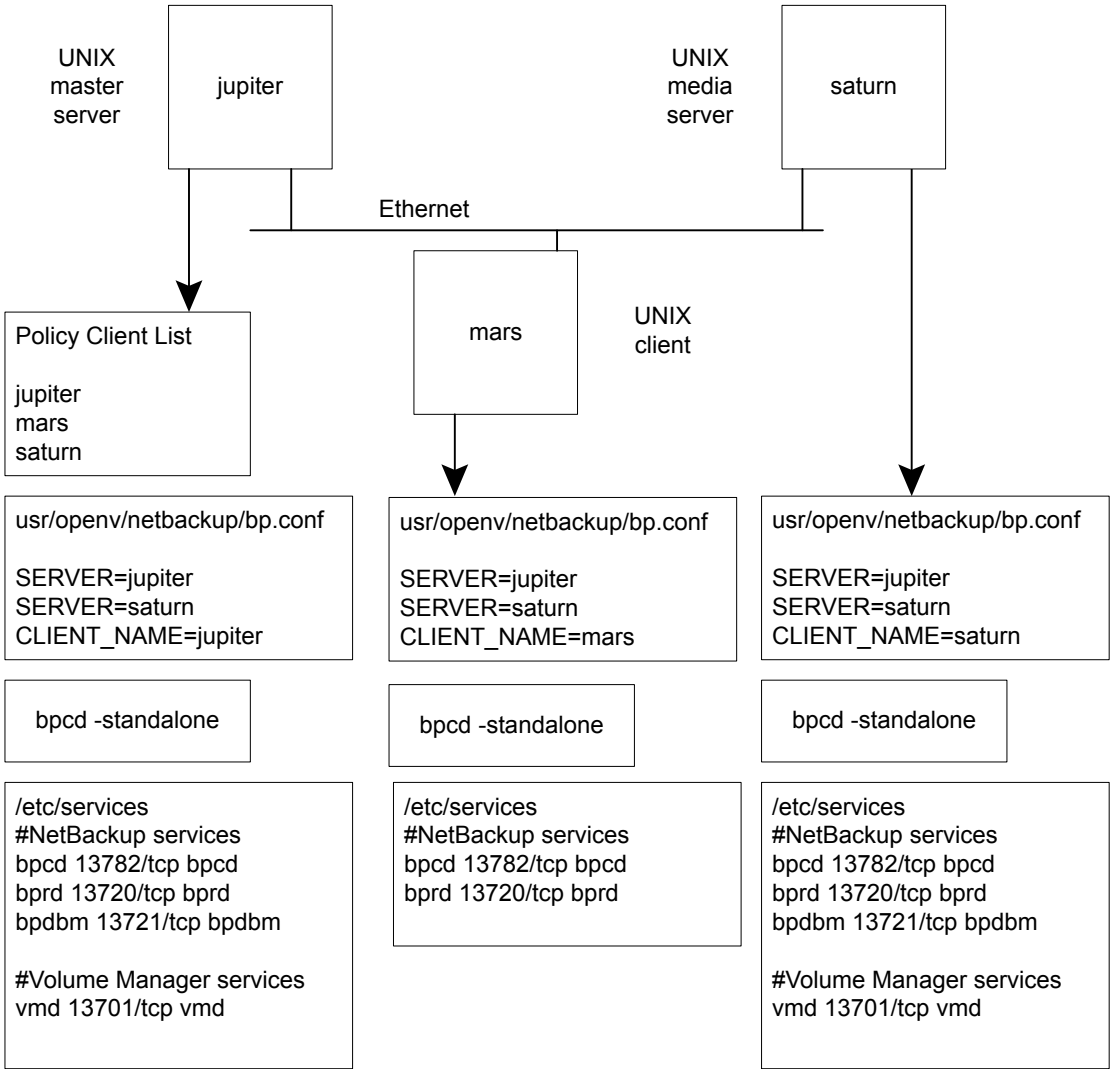
Consider the following about Figure 2-1:

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

Example of host name and service entries on UNIX primary 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 primary server *jupiter*.

Figure 2-2 UNIX primary and media servers



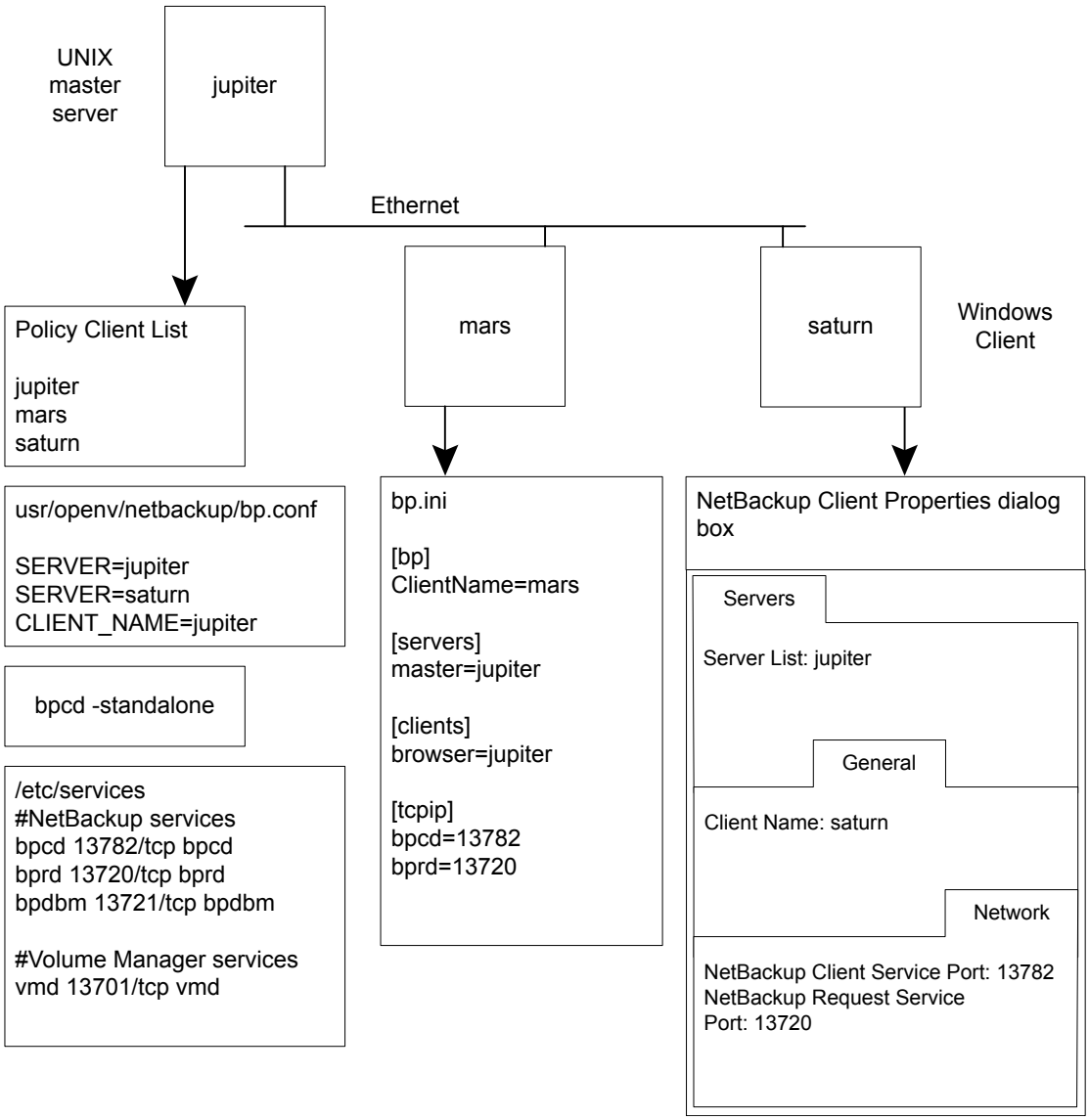
Consider the following about Figure 2-2:

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

Example of host name and service entries on UNIX PC clients

The following illustration shows a NetBackup primary 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



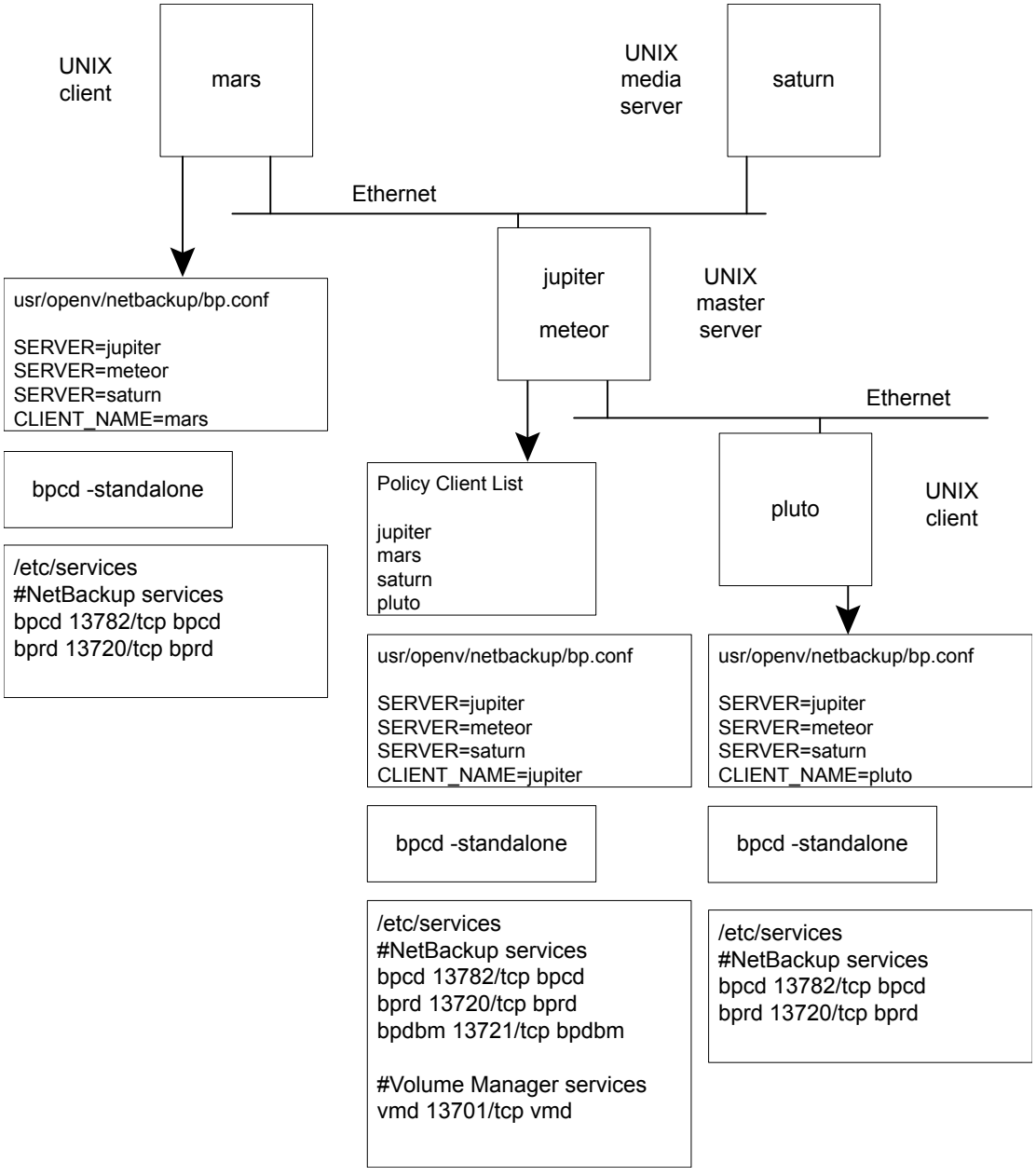
Consider the following about Figure 2-3:

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

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

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

Figure 2-4 UNIX server connects to multiple networks



Consider the following about Figure 2-4:

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

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

The NetBackup server list on the primary 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 (primary server name) is *jupiter* because that is the name used to back up the client on the primary 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 primary-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 bpclntcmd utility

The `bpclntcmd` utility resolves IP addresses into host names and host names into IP addresses. It uses the same system calls as the NetBackup application modules.

With the `-pn` option, `bpclntcmd` connects to the primary server and returns how the primary 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 `bpclntcmd` command in an MS-DOS command window so you can see the results.

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

-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 primary server.

-pn When the `-pn` option is run on a NetBackup client, it initiates an inquiry to the NetBackup primary 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 primary server and describes how the primary 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 primary server entry from the server list on the client.
- `dove.friendlyanimals.com` is the connection name (peer name) returned by the primary server. The primary 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 primary server.
- `57141` is the source port number of the connection from the client.

-verbose 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-faee9f9320d1
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 to access configuration settings

The **Host properties** allow you to 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 accessing these settings.

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** in the NetBackup web UI.

To use the host properties to access configuration settings

1. Sign in to the NetBackup web UI.
2. On the left, click **Hosts > Host properties**.
3. Select the host that you want to update and click **Connect**.
4. Depending on the host type, click one of the following:
   - **Edit primary server**
   - **Edit media server**
   - **Edit client**
5. Select the property that you want to edit and make the changes.

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 Scale-Out Relational Database Manager service is running.

This service is the `vrtsdbsvc_psql` daemon on UNIX.

3 If the NetBackup Scale-Out Relational Database Manager 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 Scale-Out Relational Database Manager service.

4 Verify that the NetBackup Scale-Out Relational Database Manager 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 -verbose`

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

If validation fails, contact Cohesity 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 Cohesity Technical Support.

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

If this validation fails, contact Cohesity Technical 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 Cohesity Technical 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. Set the verbosity for `bptm` on individual media servers by changing the logging levels in the host properties for each media server.

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 the 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 Cohesity Support website: netbackup.com/compatibility

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

Open the NetBackup web UI. On the left click **Hosts > Host properties**.

Open the properties for the media server.

Click **Media**.

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

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

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

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

  ```
  FREEZING media id 000067: it contains 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 the 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

     install_path/netbackup/bin/nbwmc
     ```

   - 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 primary server:

https://support.cohesity.com/s/article/article-000081350

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 unifed 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\Cohesity
NetBackup\NetBackup\var\global\wsl\credentials\tpcredentials\nbwebservice.jks]
due to [Illegal character in opaque part at index 2: C:\Program
Files\Cohesity
NetBackup\NetBackup\var\global\wsl\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 t 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 primary 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`*`\NetBackup\wmc\bin\setenv`

Communication can be successful in the following scenarios:

- The certificate contains all host names that the primary 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 primary server and validates that a client is connected to the primary 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\Cohesity\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\Cohesity\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 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 primary 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 primary 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`, `nbpem`, `nbrb`, or `nbjm`. The following is an example of an error that is related to PBX:

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

To access the PBX logs

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

   See also the NetBackup Logging Reference Guide for topics on unified logging.

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

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

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

   To check the current verbosity, enter the following:

   ```
   pbxcfg -p
   ```

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

   UNIX: `/opt/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
 5/12/2008 16:32:17.477 [Error] Unauthorized Server
```

To troubleshoot PBX security

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

   - On Windows:
     `install_path``\VxPBX\bin\pbxcfg -p`

- On UNIX:

```
/opt/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 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 Private Branch Exchange service.
6. Start NetBackup:
   - On Windows:

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

- On UNIX:

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

Determining if the PBX daemon or service is available

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

When a NetBackup service is not running and another process tries to connect to it, messages similar to the following appear in `/opt/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 this service, do the following:

   (UNIX/Linux) Enter the `nbemm` command.

   (Windows) Start the NetBackup Enterprise Media Manager service (**Start > Run**, then enter `services.msc`).

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

   - On Windows:

     install_path`\NetBackup\bin\bpdown`
     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 primary 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 primary 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 primary server.
  See the 'About the communication between a NetBackup client located in a demilitarized zone and a primary 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 primary 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 primary 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 primary 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: exampleprimary 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 primary 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

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:
  Host ID: zzzzzz-1271-4ea4-zzzz-5281a4f760e6
  Host: example1.com
  Master Server: example1.com
  OS Type: Windows
  Operating System: Microsoft Windows Server *yyyy* R*n* 64-bit Service Pack *n*, Build *nnn(nnnnnn)*
  NetBackup EEBs:
  Hardware Description : GenuineIntel Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz, 4 CPUs
  CPU Architecture: Intel x64
  Version: NetBackup_8.1
  Secure: Yes
  Comment:

Mapped Host Name	Approved	Conflict	Auto-discovered	Shared	Created On	Last Updated On
example1.com	No	No	Yes	No	Jul 28, 2017 03:53:30 PM	Jul 28, 2017 03:53:30 PM

- 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:

Mapped Host Name	Approved	Conflict	Auto-discovered	Shared	Created On	Last Updated On
example2.com	No	No	Yes	No	Jul 28, 2017 02:52:20 PM	Jul 28, 2017 02:52:20 PM

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

- Windows: *install_path*`\NetBackup\bin\admincmd\nbhostmgmt -add -hostid zzzzzz-1271-4ea4-zzzz-5281a4f760e6 -mappingname myprimary`

  Example output: `example1.com is successfully updated.`

- UNIX: `/usr/openv/netbackup/bin/admincmd/nbhostmgmt -add -hostid xxxxx-52e8-xxxx-ba92-7be20c6dceb9 -mappingname myprimary`

  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`
- UNIX: `/usr/openv/netbackup/bin/bpclntcmd -clear_host_cache`

Example output:

```
Successfully cleared host cache

Successfully cleared peer validation cache
```

Troubleshooting Auto Image Replication

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

Note: Although A.I.R. supports replication across different primary server domains, the Replication Director does not.

A.I.R. 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 A.I.R. 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. To verify that the image is on a disk volume that supports replication, in the NetBackup web UI open **Storage > Disk storage** and click on the **Disk pools** tab. If the disk volume is not a replication source, click **Update disk volume** to update the disk volume 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.

Action	Condition
A.I.R. replication jobs have not started	Verify the following: ■ The SLP is active. ■ The `nbstserv` daemon is running. ■ The image has not exceeded the extended retry count.
A.I.R. replication jobs are queued but have not started	No media server or I/O stream is available.
A.I.R. replication jobs fail, for example with status 191	Check the job details for more information about the failure. For more details, review the `bpdm` log on the media server that processed the replication job.

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

To troubleshoot Auto Image Replication jobs

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

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

Example output:

```
LSU Info:
Server Name: PureDisk: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:

```
# 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 the 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 the storage unit `PDstu` uses disk pool `PDpool`.

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

```
nbdevquery -listdp -stype PureDisk -dp PDpool -U
Disk Pool Name   : PDpool
Disk Pool Id     : PDpool
Disk Type        : PureDisk
Status           : UP
Flag             : Patchwork
...
Flag             : OptimizedImage
Flag             : ReplicationTarget
Raw Size (GB)    : 42.88
Usable Size (GB) : 42.88
Num Volumes      : 1
High Watermark   : 98
Low Watermark    : 80
Max IO Streams   : -1
Comment          :
Storage Server   : ss1.acme.com (UP)
```

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

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

```
# 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.

9 The last phase of validation is the storage lifecycle policy configuration. To run Auto Image Replication, the source copy must be on the 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 A.I.R. job flow, use the same command lines as you use for other jobs that are managed by a storage lifecycle policy. For example, to list the images that have been duplicated to remote primary run the following:

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

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

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

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

```
nbstlutil repllist -U
Image:
 Master Server            : 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
```

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

Rules for primary servers used with Auto Image Replication (A.I.R.) and SLPs

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

- If you want to replicate to specific targets (targeted A.I.R.), you must create the Import SLP on the target domain before you create the Auto Image Replication SLP on the source domain. You may then choose the appropriate import SLP.

  Note: Ensure that the Import SLP name contains fewer than 113 characters.

- The storage lifecycle policy's data classification in the source primary server domain must match the SLP policy's data classification in the target primary server domain.
- The duplicate-to-remote-primary copy in the source SLP must use hierarchical duplication and specify a source copy with a residence capable of replication. (The disk pool replication column must show the Source.)
- The SLP 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 SLP. The import copy may specify a storage unit group or a storage unit but not **Any available**.
- The SLP in the target domain must have at least one copy that specifies the Remote retention type.

Targeted A.I.R. trusted primary server operation fails with an external certificate configuration

A targeted A.I.R. trusted primary server operation can fail with an external certificate configuration. In this case you can troubleshoot the following operations:

- Troubleshoot adding or updating the trust
  See "Troubleshoot adding or updating the trust" on page 116.
- Troubleshoot removing the trust
  See "Troubleshoot removing the trust" on page 117.

Troubleshoot adding or updating the trust

This topic describes how to troubleshoot the issue when an operation fails to add or update the trust between the source and the target primary server.

Problem

Adding or updating the trust between the source and target primary server has failed.

Cause

The issue can occur because of the following reasons:

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

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

See "Troubleshooting Windows certificate store issues" on page 140.

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

To troubleshooting adding or updating the trust

1. Review the error message: `EXIT STATUS 5630: Failed to get version of remote primary server.`

   If the `vnetd` proxy service is down or the connection to the `vnetd` proxy has failed on the source primary server, review the logs in the following order:

   - Review the connection to the `vnetd` proxy of the remote primary server. To review the connection to the remote primary server's `vnetd` proxy, run the `bptestbpcd -host` *`remote_primary_server_name`* command.
   - Review the proxy logs:
     Windows: `C:\Program Files\Cohesity NetBackup\NetBackup\logs\nbpxyhelper\`*`log_file`*
     Linux: `/usr/openv/logs/nbpxyhelper/`*`log_file`*

2. Review the error message: `EXIT STATUS 5616: The local primary server is not reachable. The trust is unidirectional right now, the remote primary server trusts the local primary server, but the`

`local primary server doesn't trust the remote master. Please remove the trust`

If the `bprd` service is down on the source primary server, review the logs in the following order:

- Review the `bprd` logs.
  Windows: `C:\Program Files\Cohesity NetBackup\NetBackup\logs\bprd\log_file`
  UNIX: `/usr/openv/netbackup/logs/bprd/log_file`
- Review the proxy logs.
  Windows: `C:\Program Files\Cohesity NetBackup\NetBackup\logs\nbpxyhelper\log_file`
  Linux: `/usr/openv/logs/nbpxyhelper/log_file`
- Review the EMM database logs.
  Windows: `C:\Program Files\Cohesity NetBackup\NetBackup\logs\nbemm\log_file`
  Linux: `/usr/openv/logs/nbemm/log_file`

Troubleshoot removing the trust

This topic describes how to troubleshoot the issue when an operation fails to remove the target primary server from the trusted primary server database and from the configuration file as `TRUSTED_MASTER`.

Problem

The operation to remove the trust failed.

Cause

Failed to remove the target primary server from the trusted primary server database and from the configuration file as `TRUSTED_MASTER`.

Solution

To troubleshoot removing the trust:

- Review the error message: `EXIT STATUS 5616: The local primary server is not reachable. The trust is unidirectional right now, the remote primary server trusts the local primary server, but the local master server doesn't trust the remote primary. Please remove the trust.`
  The `bprd` service is down on the source primary server.
  Review the logs in the following order:

- Review the `bprd` logs.
  Windows: `C:\Program Files\Cohesity NetBackup\NetBackup\logs\bprd\log_file`
  Linux: `/usr/openv/netbackup/logs/bprd/log_file`
- Review the proxy logs.
  Windows: `C:\Program Files\Cohesity NetBackup\NetBackup\logs\nbpxyhelper\`*`log_file`*
  Linux: `/usr/openv/logs/nbpxyhelper/`*`log_file`*
- Review the EMM database logs.
  Windows: `C:\Program Files\Cohesity NetBackup\NetBackup\logs\nbemm\`*`log_file`*
  Linux: `/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
```

```
Backup Time              : 1280299412 (Wed Jul 28 01:43:32 2010)
Policy                   : (none specified)
Client Type              : 0
Schedule Type            : 0
Storage Lifecycle Policy : (none specified)
Storage Lifecycle State  : 1 (NOT_STARTED)
Time In Process          : 0 (Wed Dec 31 18:00:00 1969)
Data Classification ID   : (none specified)
Version Number           : 0
OriginMasterServer       : master_tlk
OriginMasterServerID     : 00000000-0000-0000-0000-000000000000
Import From Replica Time : 0 (Wed Dec 31 18:00:00 1969)
Required Expiration Date : 0 (Wed Dec 31 18:00:00 1969)
Created Date Time        : 1287678771 (Thu Oct 21 11:32:51 2010)

Copy:
  Master Server       : bayside.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)
  Residence           : (none specified)
  Copy State          : 1 (NOT_STARTED)
  Job ID              : 0
  Retention Type      : 0 (FIXED)
  MPX State           : 0 (FALSE)
  Source              : 0
  Destination ID      :
  Last Retry Time     : 0

  Fragment:
    Master Server     : bayside.example.com
    Backup ID         : gdwinlin04_1280299412
    Copy Number       : 1
    Fragment Number   : -2147482648
    Resume Count      : 0
    Media ID          : @aaaab
    Media Server      : bayside.example.com
    Storage Server    : bayside.example.com
    Media Type        : 0 (DISK)
    Media Sub-Type    : 0 (DEFAULT)
```

```
Fragment State    : 1 (ACTIVE)
Fragment Size     : 0
Delete Header     : 1
Fragment ID       : gdwinlin04_1280299412_C1_IM
```

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

Action	Condition
Automatic import jobs queue	No media server or I/O stream is available for this disk volume.
Automatic import jobs never start (copy stays at storage lifecycle state 1)	■ The storage lifecycle policy is inactive. ■ The storage lifecycle policy import destination is inactive. ■ The storage lifecycle policy is between sessions. ■ The image has exceeded the extended retry count and the extended retry time has not passed.
Automatic import event is discarded and the image is ignored	■ The event specifies a backup ID that already exists in this primary server catalog. ■ The event specifies a disk volume that is not configured in NetBackup for this storage server.
Automatic import job is started but the image is expired and deleted to clean up disk space in some cases. The event logs an error in the Problems Report or `bperror` output. An import job runs, but the import for this image fails showing a status code in the range 1532–1535.	■ The storage lifecycle policy that is specified in the event does not contain an import destination. ■ The storage lifecycle policy that is specified in the event has an import destination with a residence that does not include the disk volume 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 primary server. More information is available for the storage lifecycle policy configuration options. See the NetBackup Administrator's Guide, Volume I.

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

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
 Backup Time              : 1287610477 (Wed Oct 20 16:34:37 2010)
 Policy                   : two-hop-with-dup
 Client Type              : 0
 Schedule Type            : 0
 Storage Lifecycle Policy : woodridge2bayside2pearl_withdup
 Storage Lifecycle State  : 3 (COMPLETE)
 Time In Process          : 1287610714 (Wed Oct 20 16:38:34 2010)
 Data Classification ID   : (none specified)
 Version Number           : 0
 OriginMasterServer       : woodridge.example.com
 OriginMasterServerID     : f5cec09a-da74-11df-8000-f5b3612d8988
 Import From Replica Time : 1287610672 (Wed Oct 20 16:37:52 2010)
 Required Expiration Date : 1290288877 (Sat Nov 20 15:34:37 2010)
 Created Date Time        : 1287610652 (Wed Oct 20 16:37:32 2010)
```

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

```
Image:
 Master Server             : bayside.example.com
 Backup ID                 : gdwinlin04_1280299412
 Client                    : gdwinlin04
 Backup Time               : 1280299412 (Wed Jul 28 01:43:32 2010)
 Policy                    : (none specified)
 Client Type               : 0
 Schedule Type             : 0
 Storage Lifecycle Policy  : (none specified)
 Storage Lifecycle State   : 1 (NOT_STARTED)
```

```
Time In Process          : 0 (Wed Dec 31 18:00:00 1969)
Data Classification ID   : (none specified)
Version Number           : 0
OriginMasterServer       : master_tlk
OriginMasterServerID     : 00000000-0000-0000-0000-000000000000
Import From Replica Time : 0 (Wed Dec 31 18:00:00 1969)
Required Expiration Date : 0 (Wed Dec 31 18:00:00 1969)
Created Date Time        : 1287680533 (Thu Oct 21 12:02:13 2010)
```

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

Troubleshooting network interface card performance

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

Note: If the NIC in a NetBackup primary 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 primary or media server. That is, each computer that is listed as a `SERVER` must have either NetBackup primary 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 web UI and the NetBackup Administration Console

The following types of error messages can display in NetBackup.

Table 2-10 Error message types

Error type	Description
NetBackup status codes and messages	The operations that are performed in the **NetBackup web UI** or **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. **Note:** A status code does not always accompany the error message.
NetBackup Administration Console: application server status codes and messages	These messages have status codes in the 500 range. **Note:** A status code does not always accompany the error message.

Table 2-10 Error message types *(continued)*

Error type	Description
Java exceptions	Either the Java APIs or NetBackup Administration APIs generate these exceptions. Java exceptions usually appear in one of the following places: ■ The status line of the NetBackup Administration Console ■ The log file that the `jnbSA` or `jbpSA` commands generate

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 log in, status: 35 cannot make required directory"
  - "/bin/sh: null: not found (1) "
  - "An exception occurred: vrts.nbu.admin.bpmgmt.CommandOutputException: Invalid or unexpected class configuration data: *<the rest of the message will vary>*"
  - Empty warning dialog boxes

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 primary 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\\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\\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\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.
- Web service certificate's issuer and the issuer of the host certificate may not match.
  If both the certificates are not issued by the same external CA, certificate trust verification fails.

Review the following:

- It is mandatory to provide the path to the certificate file that contains the entire chain of certificates (except the root certificate).
- If chain is not specified, the certificate trust verification fails and the console is not able to connect to the web service.
- Ensure that the web server's certificate and the host certificate are issued by same external CA.

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 primary server to check if external CA is configured (ON) or not (OFF).
    install_path`/nbcertcmd -getSecConfig -caUsage`
    On Windows: *install_path*`\NetBackup\bin\nbcertcmd -getSecConfig -caUsage`
    On UNIX: `/usr/openv/netbackup/bin/netbackup/bin/nbcertcmd -getSecConfig -caUsage`
    For example: *install_path*`\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 primary server.

    `install_path``/goodies/nbsslcmd x509 -in` *`certificate_path`* `-noout -text -purpose`

    On Windows: *`install_path`*`\goodies\nbsslcmd x509 -in` *`certificate_path`* `-noout -text -purpose`

    On UNIX: `/usr/openv/netbackup/bin/netbackup/bin/goodies/nbsslcmd x509 -in` *`certificate_path`* `-noout -text -purpose`

    Validate whether the host certificate of the primary 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 primary 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-primary _ext

  DNS: nb-primary .some.domain.com

  DNS: nb-primary _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 primary server or include all names of the primary server that are known to the NetBackup domain in the certificate.

For more information, refer to the following article:

https://support.cohesity.com/s/article/article-000126751

Cause 2

Some of the NetBackup core services have not started.

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

Use 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`
  - `postgres` (UNIX) or NetBackup Scale-Out Relational Database Manager (Windows)
- Restart the `nbsl` and the `vnetd` services, if they are not running.
- Restart the NetBackup Scale-Out Relational Database, if it is not running.

On Windows:

Restart the `nbsl`, `vnetd`, and NetBackup Scale-Out Relational Database Manager services as follows:

```
install_path\bin\bpdown -e "NetBackup Service Layer" -f -v

install_path\bin\bpup -e "NetBackup Service Layer" -f -v

install_path\bin\bpdown -e "NetBackup Legacy Network Service" -f -v

install_path\bin\bpup -e "NetBackup Legacy Network Service" -f -v

install_path\bin\bpdown -e "NetBackup Scale-Out Relational Database
Manager" -f -v

install_path\bin\bpup -e "NetBackup Scale-Out Relational Database
Manager" -f -v
```

On UNIX:

Restart the `nbsl` service as follows.

```
/usr/openv/netbackup/bin/nbsl -terminate

/usr/openv/netbackup/bin/nbsl
```

Restart the `vnetd` service as follows.

For example:

```
# ps -fed | grep vnetd | grep standalone

root 16018 1 4 08:47:35 ? 0:01 ./vnetd -standalone

# kill 16018

/usr/openv/netbackup/bin/vnetd -standalone
```

Restart the NetBackup Scale-Out Relational Database as follows.

```
/usr/openv/netbackup/bin/nbdbms_start_server -stop

/usr/openv/netbackup/bin/nbdbms_start_server
```

If the problem persists, contact the Cohesity Technical Support.

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/nbsslcmd 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 `nbsslcmd` 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 volumeID 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 primary 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 *primary_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 *primary_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 *primary_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 *primary_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 primary 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 issues with external certificate configuration

This topic provides information on troubleshooting issues that are specific to external certificates, configuration, removal and so on.

For more information on external certificate configuration, see the *NetBackup Security and Encryption Guide*.

Table 2-11

Sr. No.	Issue	Possible reason	Resolution
1.	The following error is displayed when an external certificate is configured: `NetBackup Web Management Console service is down with error. nbcertcmd: The -ping operation failed. EXIT STATUS 26: client/server handshaking failed Ensure that NetBackup Web Management Console service is up and running before trying this operation.`	The NetBackup Web Management Console (nbwmc) service is down.	Start the NetBackup Web Management Console (nbwmc) service.

Table 2-11 *(continued)*

Sr. No.	Issue	Possible reason	Resolution
2.	No audit entries are created when external certificates are added or deleted.	The `configureWebServerCerts` command is run with the `-force` option.	Run the `configureWebServerCerts` command without the `-force` option
3.	The NetBackup Web Management Console (nbwmc) service does not start after external certificate is configured.	There may be some issue with external certificate configuration process.	Do the following: ■ Ensure that the external certificate parameters like certificate chain, private key, and trust store are in the correct format and try configuring the external certificate again. ■ If the issue persists, try configuring the external certificate with the `-force` option. ■ If the problem still persists, save all the error log information and contact Cohesity Technical Support.
4.	The command `./configureWebServerCerts -removeExternalCert -all` exited with one of the following errors: ■ EXIT STATUS 7724: The certificate cannot be removed. ■ EXIT STATUS 7733: External certificate of the NetBackup web UI cannot be removed. ■ EXIT STATUS 7734: External certificate of the NetBackup host cannot be removed.	Possible reasons: ■ There is no space left on the disk to back up the existing web server configuration. ■ There are issues with permissions to update the web server configuration at the following location: `NetBackup Install Directory/var/global/wsl/webserver/config`	Do the following: ■ Increase the disk space. ■ If the problem still persists, save all the error log information and contact Cohesity Technical Support.

Table 2-11 *(continued)*

Sr. No.	Issue	Possible reason	Resolution
5.	The `./configureWebServerCerts -addExternalCert -all -certPath file_path -privateKeypath file_path -trustStorePath file_path` command exited with one of the following errors: ■ `EXIT STATUS 7728: The input file of ECA configuration is not valid.` ■ `EXIT STATUS 7730: The private key cannot be added.` ■ `EXIT STATUS 7731: The trust bundle cannot be added.`	Possible reasons: ■ There is no space left on the disk to add the certificate. ■ There are issues with permissions to add certificate at the following location: `NetBackup Install Directory/var/global/wsl/credentials` ■ The primary server runs in FIPS mode and the files that are provided to configure the external certificate are not in the PEM format.	■ Increase the disk space. ■ If the primary server runs in FIPS mode, run the command using the PEM formatted files. ■ If the problem still persists, save all the error log information and contact Cohesity Technical Support.

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 primary 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 primary server domain.
- The primary 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 primary server certificate authority (CA) configuration using the `nbcertcmd -getsecconfig -caUsage` command, 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 primary 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 primary server domain or configure the web server to use both external and NetBackup certificates.
- Clear the cache memory on the hosts using the following command:
  `bpclntcmd -clear_host_cache`
- Check `vnet proxy` logs at: *`install_path`*`/logs/nbpxyhelper`.
- Check the web service logs at: *`install_path`*`/logs/nbwebservice`

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 primary 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 primary 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 primary 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/Linux: `/usr/openv/mqbroker/logs`
  Windows: *`Install_Path`*`/mqbroker/logs`
- Ensure that the `nbmqbroker` service is running on the primary server. Use the following commands:
  - Run the `bpps` command.
  - Run the `bptestbpcd -host` *`hostname`* command from the primary 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/Linux: `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 primary 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 primary 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 primary 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 primary server services are restarted

Do the following:

- Check the subscriber service logs at:
  UNIX/Linux: `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 primary 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:

- Run the *install_path*/bin/admincmd/bptestbpcd -host *hostname* from the primary 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:[primary 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 re
```

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

Do the following:

1. Run the following command on the primary server:

   `/user/openv/netbackup/bin/admincmd/bptestbpcd -host` *`host_name`*

2. Check the logs at `/user/openv/netbackup/logs/admin`.
3. Check if the media server is offline. Open the NetBackup web UI. On the left click **Storage > Media** servers. Then click the **Media servers** tab.

4. If the primary 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: primary 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 primary 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 primary 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 primary 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 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"`

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 the disaster recovery package on Linux” on page 282.

See “Restoring the disaster recovery package on Windows” on page 278.

New nbmqbroker service-specific notifications are not displayed in the NetBackup web UI on Linux

The nbmqbroker service logs show the following errors:

```
escript: exception error: undefined function rabbitmqctl_escript:main/1

in function  escript:run/2 (escript.erl, line 758)

in call from escript:start/1 (escript.erl, line 277)

in call from init:start_em/1

in call from init:do_boot/3
```

Root cause:

Certain configuration changes on the primary server may result into inconsistency in nbmqbroker service configuration. To resolve the issue, you need to reconfigure the nbmqbroker service.

To reconfigure the `nbmqbroker` service

1. Stop the `nbmqbroker` service by running the following command:

   `/usr/openv/mqbroker/bin/nbmqbroker stop`

2. Run the following command to configure the `nbmqbroker` environment:

   `/usr/openv/mqbroker/bin/install/configureMQEnv`

3. Run the following command to configure the `nbmqbroker` service:

   `/usr/openv/mqbroker/bin/install/configureMQ`

4. Start the `nbmqbroker` service by running any of the following commands:

   - `/usr/openv/mqbroker/bin/nbmqbroker start`
   - `bp.start_all command`

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

The NetBackup Messaging Broker service does not start on IPv6-only primary server

Reasons:

The primary sever name is possibly being resolved to both IPv4 and IPv6 addresses although only IPv6 address is used.

Run the following command to check if the output contains an IPv4 address:
`nslookup primary_server_name`

Sample output:

```
# nslookup primary-server.com

Server: 2600:100:f0a1:9000::a

Address: 2600:100:f0a1:9000::a#53

Non-authoritative answer:

Name: primary-server.com

Address: 10.200.100.60

Name: primary-server.com

Address: 2600:100:f0a1:9014::335
```

Expected output:

```
# nslookup primary-server.com

Server: 2600:100:f0a1:9000::a

Address: 2600:100:f0a1:9000::a#53

Non-authoritative answer:

Name: primary-server.com

Address: 2600:100:f0a1:9014::335
```

Do the following:

- Fix all the configurations to create an appropriate IPv6-only setup.
- If the issue still persists, do the following configuration changes to start the `nbmqbroker` service.

  With this configuration, the `nbmqbroker` service always attempts to first use the IPv6 address for name resolution.

To change the configurations

1 Do the following to create the required file.

Use an appropriate text editor (vi on Linux or Notepad on Windows) and create a file called `erl_inetrc` in the given directory:

On Linux, create the `erl_inetrc` file in the following directory:

```
/usr/openv/var/global/mqbroker/erl_inetrc
```

Run the following command:

```
cat > /usr/openv/var/global/mqbroker/erl_inetrc
```

On Windows, create the `erl_inetrc` file in the following directory:
NetBackup_Install_path\var\global\mqbroker\

2 Add the following line in the `erl_inetrc` file:

```
{inet6,true}.
```

Note that the trailing dot (.) is mandatory.

3 On UNIX, run the following command to check the permissions of the `/usr/openv/mqbroker/bin/setmqenv` file:

```
ls -l /usr/openv/mqbroker/bin/setmqenv
```

The output is as follows:

```
-rwxr-x---. 1 nbwebsvc nbwebgrp 3869 date
 /usr/openv/mqbroker/bin/setmqenv
```

4 Do the following:

On Linux:

Add the following lines in the `/usr/openv/var/global/mqbroker/advanced_setmqenv` file:

```
RABBITMQ_SERVER_ADDITIONAL_ERL_ARGS="-kernel inetrc
'/usr/openv/var/global/mqbroker/erl_inetrc' -proto_dist inet6_tcp"

RABBITMQ_CTL_ERL_ARGS="-proto_dist inet6_tcp"
```

On Windows:

Add the following lines in the *NetBackup_Install_path*`\var\global\mqbroker\advanced_setmqenv` file:

```
RABBITMQ_SERVER_ADDITIONAL_ERL_ARGS=-kernel inetrc
'E:/NetBackup/var/global/mqbroker/erl_inetrc' -proto_dist
inet6_tcp

RABBITMQ_CTL_ERL_ARGS=-proto_dist inet6_tcp
```

5 Ensure that the file permissions are not changed after the update.

6 Start the `nbmqbroker` service.

Troubleshooting 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.

Troubleshooting 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.primary.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 primary 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 storage: `MSDP_config_path/log/spoold/spoold.log`

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

For `nbkmiputil` 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 primary 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 primary 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 storage: `PDDE_Install_Path/log/spoold/spoold.log`

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

   Here are the log snippets:

```
[Debug] NB 51216 nbwebapi 495 PID:10984 TID:149 File ID:495 [No context] 5
 [com.netbackup.config.PeerInfoPopulatorFilter]
Request URL : https://<Primary-Server>:1556/netbackup/security/key-management-services/keys
Connection Info :ConnectionInfo

[Debug] NB 51216 nbwebapi 495 PID:10984 TID:149 File ID:495 [No context] 5
[com.netbackup.security.kms.resource.KMSConfigResource]
HTTP GET filter query string is :
KeyId eq 'bdc3492b015d4a9ab25426465b12adac6a834dfc6b4449c490922d6155719958'
 and kadlen eq 32

[Debug] NB 51216 nbwebapi 495 PID:10984 TID:149 File ID:495 [No context] 5
[com.netbackup.security.kms.resource.KMSConfigResource]
com.netbackup.security.kms.resource.KMSConfigResource getKeys() - NBKMSRecordNotFoundException
occured 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 storage: *PDDE_Install_Path*/log/spoold/spoold.log

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

   For `nbkmiputil` logs:

   - For NetBackup KMS,*Install_Path*/logs/nbkms

- For external KMS, *Install_Path*/netbackup/logs/nbkmiputil

Troubleshooting 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 : Initiating the NetBackup CA migration with 16384
bits key size.

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 : network connection timed out(Error code: 41)

06-19-2020,20:40:40 : Command returned status 41

06-19-2020,20:40:40 : "C:\Program Files\Cohesity NetBackup\NetBackup\bin\admi
\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 -keysize
  <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 Cohesity Technical Support.

Troubleshooting issues with the non-privileged user (service user) account

This topic provides troubleshooting information about the issues specific to the non-privileged, non-root, or service user.

Most of the primary server services can be run as non-privileged user, which is highly recommended. This new user is called service user.

For more information on the service user, see the NetBackup Security and Encryption Guide.

The `nbcertcmd` command option logs

The `nbcertcmd` command options internally run under the service user context. You can find the logs of the `nbcertcmd` command options in the `SERVICE_USER.xxxxxx_xxxxx.log` file.

Table 2-12 Troubleshooting service user issues

Sr. No.	Issue	Possible reason	Resolution
1	During NetBackup installation or upgrade on UNIX platform, unable to specify the service user even after three prompts.	Possible reasons are as follows: ■ Reason 1 - The service user does not exist locally, in LDAP, or in NIS. ■ Reason 2 - `nbwebsvc` is used as a service user. ■ Reason 3 - `nbwebgrp` is not a secondary group of the service user.	Resolutions are as follows: ■ Resolution 1 - Run the following command: id *service_user* The ID command must be successful. ■ Resolution 2 - Run the `nbgetconfig` command to check the NetBackup configuration file (`bp.conf`) for the `WEBSVC_USER` entry. The service user cannot be same as the value that is set for the `WEBSVC_USER` configuration option. ■ Resolution 3 - Run the `nbgetconfig` command to check the NetBackup configuration file (`bp.conf`) for the `WEBSVC_USER` entry. Run the following command: id *service_user* In the command output, ensure that gid is not equal to the gid of the WEBSVC_GROUP option value and groups have the value WEBSVC_GROUP.
2	During NetBackup installation on an inactive cluster node on UNIX platform, one of the following errors occurs: ■ `Service user name on active node does not match with service user name entered on inactive node.` ■ `SERVICE_USER_ID '10021' retrieved from active node does not match with the user ID '1002' of local user 'nonroot'.`	The service user name and the user ID do not match.	Ensure that the service user name and the user ID match on all cluster nodes and the same is provided during NetBackup installation on active and inactive nodes.

Table 2-12 Troubleshooting service user issues *(continued)*

Sr. No.	Issue	Possible reason	Resolution
3	During NetBackup upgrade of an inactive cluster node on UNIX platform, the following error occurs: `Failed to retrieve the 'SERVICE_USER' or 'SERVICE_USER_ID' entries from the configuration file on the server 'cluster_virtual_name'. You must provide the same 'SERVICE_USER' (daemon user name) that is configured on the active node.`	The `bpgetconfig` command could not retrieve the service user and the ID from active node.	Provide the service user as that of the active node and ensure that the service user has the same user ID on all cluster nodes.
4	During NetBackup installation or upgrade on UNIX platform, the following error occurs: The user `serviceuser` cannot be set as the owner of files in `/usr/openv`.	This may be because of the issues while changing the ownership of the installation directory.	Fix the errors specified in installation trace under the following heading: `Fix below errors and then retry`

5	NetBackup host communication does not work when external CA is configured with Windows Certificate Store and services run in a Local Service account context.	NetBackup services do not have access to the private key. Usually, the error in this case can be seen in the `nbpxyhelper` logs:
		The Windows API CryptAcquireCertificatePrivateKey fails with error 0x80090016: Keyset does not exist.
			Check private key permissions as follows:
			Right-click the certificate. Go to **All Tasks > Manage Private Keys**.
			All NetBackup services should have permissions to read the private key.
			Run the following command to set permissions:
			`nbcertcmd -setWinCertPrivKeyPermissions`
			Run the following command to validate the configuration:
			`nbcertcmd -ecaHealthCheck`

Table 2-12 Troubleshooting service user issues *(continued)*

Sr. No.	Issue	Possible reason	Resolution
6	The `setconfig` command fails with the following error: `Failed to open /usr/openv/netbackup/bp.conf.d53: Permission denied (13)`	Ownership of `/usr/openv/netbackup` is changed to the root user. Other possible reason may be that the language pack is installed using rpm.	Run the following command to fix the ownership issues: `/usr/openv/netbackup/bin/goodies/update_install_folder_perms`
7	■ Create or update operation fails for catalog backup policy. ■ Catalog backup fails. ■ Catalog recovery fails.	Service user account may not have access to the disaster recovery (DR) path specified in policy.	Review status code 9201 and 9202. Refer to the NetBackup Status Codes Guide. Refer to the NetBackup Security and Encryption Guide for giving access permissions to the service user account.
8	Disaster recovery fails.	The `NBHostIdentity -import` command fails.	Ensure the following: ■ The service user exists on the system prior to disaster recovery (DR). ■ The service user has access to the DR package.

Table 2-12 Troubleshooting service user issues *(continued)*

Sr. No.	Issue	Possible reason	Resolution
9	Any of the following commands fail with error: Ensure that the service user account [*service_user_name*] has access permissions on the specified paths and their contents. ■ `nbdb_admin` ■ `nbdb_move` ■ `nbdb_backup` ■ `nbdb_restore` ■ `nbdb_unload` ■ `create_nbdb` ■ `cat_export` ■ `cat_import` Path: For UNIX - *`Install_Path`*`/db/bin` For Windows - *`Install_Path`*`\netbackup\bin`	Service user account may not have access permissions on specified paths and their contents.	Refer to the NetBackup Security and Encryption Guide for giving access permissions to the service user account.
10	Adding VMware server operation fails	500 system error	Ensure that the temp directory (/tmp) is accessible to the service user account
11	Issue in `bpjava-test-login` workflow	File ownership is shown as 'root'	Change the ownership of the file to the service user account.
12	`nbcertcmd` operations fail.	Lack of permissions	Check if the `certmapinfo.json` file is created and owned by the service user.
13	`nbcertcmd` or `bpnbaz` fails with error code 123.	The private key file (PrivKeyFile-2048.pem), public key file (PubKeyFile-2048.pem), or access control list (ACL) update failed.	Ensure that NetBackup SIDs are configured and both public and private keys are present in AT_DATA_DIR.

Table 2-12 Troubleshooting service user issues *(continued)*

Sr. No.	Issue	Possible reason	Resolution
14	`nbserviceusercmd -changeUser` operation failed with authorization failure, when NBAC is configured.	The new service user is not part of the NBAC security admin group.	Add the new service user in the NBAC security admin group. Run the following command: `vssaz addazgrpmember --azgrpname \"Security Administrators\" --prplinfo` *`prplinfo`*
15	After NetBackup 9.1 installation and upgrade, NetBackup Administration Console login fails for root user, if NetBackup access control (NBAC) or Enhanced Auditing (EA) is enabled.	The user certificate directory is changed.	If NBAC or EA is enabled in your environment, you must run the `bpnbat -login` command after NetBackup upgrade.
16	The `nbcertcmd -enrollCertificate` command fails as external CA (ECA) health check fails. An error occurs while accessing the files at the following path: `certificates/private key/passphrase file/crl`	The `nbcertcmd -enrollCertificate` command runs under the service user context, however the service user does not have access to the associated files.	Provide the required access to the service user. It is recommended that you run the following command to verify the access rights before running the `enrollCertificate` command again: `nbcertcmd -ecaHealthCheck -serviceUser` *`user_name`*
17	Before upgrade or change user, the service user is deleted.	The service user may be deleted because of certain user actions.	Do the following: Reconfigure the user to restore the service user. Refer to the article. Run the following commands:: ■ `useradd -c 'NetBackup Services account' -d /usr/openv/ nbsvcusr -u` *`old uid`* ■ `usermod -a -G nbwebgrp nbsvcusr`
18	During backup or restore, operation error is encountered.	The media server version is earlier than the client version.	Upgrade the media server or use an alternate media server with the version that is later or same as the client version.

Troubleshooting issues with group name format in the `auth.conf` file

If the authorized **NetBackup Administration Console** operations (nodes) or Backup, Archive and Restore capabilities are not accessible as expected for a member in the user group that is defined in the `auth.conf` file, verify the group name format.

To verify that the group name format and correct it

1 Run the following command to verify the group name format that is defined in the `auth.conf` file.

On UNIX:

```
install_path/netbackup/sec/at/bin/vssat validateprpl -p user name
-d unixpwd -b broker host:1556:nbatd
```

On Windows:

```
install_path\NetBackup\sec\at\bin\vssat validateprpl -p user name
-d nt:domain name -b broker-host:1556:nbatd
```

The output of the command provides names of the groups that are associated with the user who cannot access certain nodes or operations in the **NetBackup Administration Console**.

2 To access the nodes as expected, copy the group names that appear in the command output and paste them in the `auth.conf` file.

Consider the following eExample:

```
vssat validateprpl -p user@addomain.com -d unixpwd -b
localhost:1556:nbatd
```

Using data directory: `/usr/openv/var/vxss/at`

Output:

```
ValidatePrincipal :

ID : <UID>

Name : user@addomain.com

Display Name : user@addomain.com

Domain :

Description : User

Group(s) Details :

Count : 2

Name(s) and ID(s) : group1@addomain.com

GID of group1 :

group2@addomain.com

GID of group2
```

Add the group name in the `auth.conf` file as per the following format:

```
<GRP> group1@addomain.com ADMIN=SUM+AM JBP=ALL
```

Troubleshooting the VxUpdate add package process

When you add NetBackup VxUpdate packages through either the NetBackup web UI or the API, the packages are processed in an asynchronous manner. You can check the status of the package add process with either the `GET` API or the `nbrepo` command. Both these options list the packages that are available. If one or more of the packages being added are not available after several minutes, use the steps that are shown to determine the cause of the failure.

To troubleshoot VxUpdate package add operations:

1. Use the API to confirm that the desired package is unavailable.

   `GET URL https://server/netbackup/deployment/packages`

   Or use the `nbrepo` command to list available packages.

   - Windows: *install_path*`\NetBackup\bin\admincmd\nbrepo.exe -l`
   - Linux: `/usr/openv/netbackup/bin/admincmd/nbrepo -l`

2. Confirm that troubleshooting logs are present.

   - Windows:

     install_path`\NetBackup\logs\bprd`

     install_path`\NetBackup\logs\nbwebservice`

   - Linux:

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

     `/usr/openv/logs/vxul/nbwebservice`

3. Review the log files around the approximate time of the package add attempt.

   Search through both the `nbwebservice` and the `bprd` log files for the requested VxUpdate SJA file name.

4. From the log files, determine the status code or status codes that the add attempt received.

5. Review the recommended action for the status code in the NetBackup Status Code Guide.

Example

The log section that is shown is from the `nbwebservice` log. It shows an example of one error that can occur during the VxUpdate package add (emphasis is added for clarity):

```
0,51216,495,495,10738,1633618954821,12920,229,16:5F6DBAD64588994B,393:PackagesServiceImpl.
validateCreatePackagesBulkInputs - The Package file for file path [\\nbserver_store\
vxupdate\NetBackup_9.1.2_VU_2of4\vxupdate_nb_9.1.2_windows_x64.sja] was not found, or is
not accessible to NetBackup processes on the primary server. If the file exists, it must
be in a location that is accessible to NetBackup, such as a local directory on the primary
server.,61:com.netbackup.deployment.packages.service.PackagesServiceImpl,50,51216,495,495,
10739,1633618954822,12920,229,16:5F6DBAD64588994B,11659:Raised exception The Package file
for file path [\\nbserver_store\vxupdate\NetBackup_9.1.2_VU_2of4\
vxupdate_nb_9.1.2_windows_x64.sja] was not found, or is not accessible to NetBackup
processes on the primary server. If the file exists, it must be in a location that is
accessible to NetBackup, such as a local directory on the primary server. - errorCode: 7284
```

The add attempt shown failed with a NetBackup Status Code 7284. The file in this example exists, but is on a network share that is not accessible to the primary server. NetBackup services such as `bprd` might not be active with an account that has adequate permissions to read file on UNC paths or network shares.

If you place the `.sja` file into a Windows profile directory, such as a user's desktop, NetBackup generates a similar error. The error is because the NetBackup services and processes do not have adequate permissions to that location.

Review the NetBackup Status Code Guide for recommended actions.

Troubleshooting issues with FIPS mode

ECA configuration with non-FIPS compliant key fails

The given private key in the ECA configuration is in non-FIPS compliant PKCS1 format that causes the ECA configuration to fail.

Reason:

The PKCS1 format that is used to encrypt the private key uses MD5 algorithm, which is not a FIPS-compliant algorithm. Therefore, the ECA configuration fails in FIPS mode.

Sample log message:

`PEM_read_PrivateKey failed to read private key from file`*`[C:\eca\private\key-pkcs1_ENCRYPTED.pem]`*`. Provided private key is not FIPS supported.`

Solution:

Use the private key with the PKCS8 format.

Launching NetBackup Administration Console on UNIX takes longer time than usual when the FIPS mode is enabled

This problem can occur if there is insufficient entropy on the host where the **NetBackup Administration Console** runs.

Entropy is the randomness collected by an operating system.

Reason:

The Java processes use `/dev/random` as a default character device to provide cryptographically secure random output in your NetBackup environment, which is the blocking call.

To check the status of entropy on the host where the **NetBackup Administration Console** runs, execute the following command. If the command returns the value less than 200, there is an entropy issue on that host.

```
cat /proc/sys/kernel/random/entropy_avail
```

Solution:

Set the `USE_URANDOM` option to `1` in the `nbj.conf` configuration file. The Java processes start using the `/dev/urandom` device.

The NetBackup Web Management Console service (nbwmc) takes unusually long time to start

This problem can occur if there is insufficient entropy on the host where the `nbwmc` service runs.

Entropy is the randomness collected by an operating system.

Reason:

The Java processes use `/dev/random` as a default character device to provide cryptographically secure random output in your NetBackup environment, which is the blocking call.

To check the status of entropy on the primary server, run the following command. If command returns value less than 200, there is a problem of entropy on that server.

```
cat /proc/sys/kernel/random/entropy_avail
```

Solution:

Set the `USE_URANDOM` option to `1` in the configuration file. The `nbwmc` service starts using the `/dev/urandom` device.

The NetBackup Web Management Console service (nbwmc) failed to start

Reason:

If NetBackup CA or ECA hierarchy key size is less than 2048 or more than 3072 while you try to enable the FIPS mode.

Sample log message:

```
Attempt to use RSA key with non-approved size: 1024: RSA
```

Solution:

Reconfigure the NetBackup CA hierarchy and use a key size that is supported for FIPS mode - either 2048 bits or 3072 bits.

Troubleshooting issues with malware scanning

Failed to get response from NetBackup malware utility

(*Applicable on scan host RHEL 8.x and NFS version 4.x*) When scanning large size backup (~ 200 million files), following error is displayed on the Web UI for failed job:

```
Failed to get response from NetBackup malware utility.
```

While scan is in progress on scan host, NFS mount points are not accessible from scan host. Scan job remains in progress and timeout after two days. NFS exports on storage server are accessible.

Workaround: Ensure that you use NFS version 3 for mounting IA mounts on scan host over NFS by setting the following configuration in `/etc/nfsmount.conf` file on scan host:

```
# grep Defaultvers /etc/nfsmount.conf Defaultvers=3
```

Failed to connect to the scan host

SSH connection to scan host from media server failed.

Workaround: Verify the following scan host credentials:

- RSA (SHA256) key
- User name
- Password

Refer to *NetBackup Web UI Administrator's Guide* for the scan host configuration.

Failed to determine the scan host OS

Error can be due to unsupported scan host.

Workaround: For a complete list of supported platforms for the scan host, refer to the *Software Compatibility list* document.

Failed to copy NetBackup malware utility to the scan host

- Not enough space is available on the scan host.
- SSH user does not have access to the required directories on the scan host.

Workaround

- On a Windows scan host, check for space availability in `C:\` folder.
- On a Linux scan host, check for space availability in `/tmp` folder.

Failed to get the scan host credentials

Media server is not able to fetch the credentials to access scan host from the Primary.

Workaround: Check that credentials for scan host are specified.

Time-out has occurred during the scan

Default scan operation time out is two days. Time to scan may vary depending on the factors sch as workload type, network bandwidth, backup size.

Workaround: Scan time-out is configurable and can be changed by setting the **MALWARE_SCAN_OPERATION_TIMEOUT** configuration key.

- Minimum value: 1 hour
- Maximum value: 30 days

Failed to get response from NetBackup malware utility

Mismatch between `nbmalwareutil` binary and the `ScanManager`.

Workaround:

Contact NetBackup support.

Failed to launch the scanner

Malware scanner-specific failure message.

Workaround: Refer to `nbmalwarescanner` logs on the media server for agentless host type pools, or on scan host if it is agent based scan.

Failed to mount the backup image

This error message appears for one of the following reasons:

- IA share is not accessible from the scan host.
  Workaround: Check IA configuration on storage server. Verify on activity monitor that IA job is successful.

Failed to unmount the backup image

IA share is busy or not accessible.

Workaround: Refer to `nbmalwarescanner` logs on the media server for agentless host type pools, or on scan host if it is agent based scan.

Failed to run a scan

Generic failure during the scan of a backup image.

Workaround: Refer to `nbmalwarescanner` logs on the media server for agentless host type pools, or on scan host if it is agent based scan.

Instant access mount created but not deleted by malware scan

Generic failure during the scan of a backup image.

Workaround:

- Verify if any scan is in progress.
- If no scan is in progress, then obtain the list of such instant access mounts with ID's of the instant access mount created using the GET IA API from the following directory:
  `/netbackup/recovery/workloads/{workload}/instant-access-mounts`
- Using the DELETE API, delete the instant access mount:
  `/netbackup/recovery/workloads/{workload}/instant-access-mounts/{mounId}`

All mount drives are exhausted

Only five backup images can be mounted at the same time on windows scan host.

Workaround:

- Ensure that scan host is not part of multiple NetBackup domains.
- Check if there are any Stale mounts on the scan host by running `net use`.
- Following drive letters are used for mounting the IA shares on the windows scan host. Ensure that they are not in use. `L:\ M:\ N:\ O:\ P:\`

Either the Windows Defender is not installed or the environment variable is not set

Microsoft Windows Defender is not installed on the scan host or not configured properly.

Workaround: Ensure that Microsoft Windows Defender is installed on scan host.

Refer *NetBackup Web UI Administrator's Guide* for the scan host configuration.

Either Symantec protection engine is not installed or the environment variable is not set

Symantec Protection Engine is not installed on the scan host or not configured properly.

Workaround: Ensure that Symantec Protection Engine is installed on scan host.

Refer *NetBackup Web UI Administrator's Guide* for the scan host configuration.

Failed to perform malware scan of the backup image

Generic error for Scan failure.

Workaround: Contact NetBackup support.

Net bios name can be at most 15 chars long

Storage server host name cannot be more than 15 characters for the SMB share support.

If Windows Server 2016 is used to set up Active Directory domain, then it does not allow a connection to a storage server with host name of length more than 15 characters.

Workaround: Ensure that the character limit is not more than 15 characters.

Failed to run a scan

Generic failure during scanning backup image.

Workaround: Check for the following errors:

- Refer to `nbmalwarescanner` logs on the media server for agentless host type pools, or on scan host if it is agent based scan.
- Check for space on media server storage.
- Check for NFS service failure on media server.

Too many infected files in the selected time range

Review the `nbmalwarescanner` to view the infected files list for the backup images in the selected date range.

Workaround: Update the date range or recovery files and folders selection to reduce the number of infected files. Retry the operation. You can also perform one of the following:

- Select the **Allow recovery of files impacted by malware** option which can be used to recover selective clean files.
- Skip that backup image from recovery.

Large number of infected files

- There are too many infected files in the selected scan result. If the scan result has infected files greater than 5000, the following message is displayed:

  `Large number of infected files. To view the complete list of infected files, export the list.`

  Workaround: Export the infected file list in `.csv` format and download it to view it.

- There are many infected files in the selected scan result or the infected file paths are long to be captured in the database. Following error message is displayed:

  `Large number of infected files.`

  Workaround: This result cannot be exported or viewed.

  : As the results cannot be exported or viewed, review the scan logs to view a detailed list of the infected files for the selected scan result.

Scan operation is divided into parts

For large size backup, scan operation is divided into parts. For example, if total number of files in the backup are 1,000,000, the scan operation will be divided into two parts of 500,000 files each.

Each part would be created and scanned separately. Each part can be assigned with different scan host. The Malware detection UI displays only single entry for backup.

Workaround: Each divided part details can be obtained by using the REST API.

The NB_MALWARE_SCANNER_PATH environment variable is missing

When performing a malware scan operation with the NetBackup Malware Scanner installed on the scan host, it fails with the following error message:

```
Missing environment variable NB_MALWARE_SCANNER_PATH
```

Workaround: Ensure that NetBackup Malware Scanner is installed. Note the install location.

Login on the scan host as user using the same user credentials that were provided during scan host configuration on the primary server. Add the following lines to `~/.bashrc`:

```
export
NB_MALWARE_SCANNER_PATH=<installLocation>/savapi-sdk-linux64/bin

export PATH=$PATH:$NB_MALWARE_SCANNER_PATH
```

Failed to perform malware scan on Windows scan host

Malware scanning on Windows scan host may fail if there are cygwin mks toolkit installed.

Workaround: UNIX utilities are installed, however, defined scanuser cannot have those UNIX utilities in the PATH variable.

Issues related to space and directory access on the scan host

Error/Issue	Description	Workaround
■ Failed to open the file. ■ Unable to create a directory. ■ Failed to generate the result file. ■ Failed to open the output file. ■ Unable to create directory for result file. ■ Failed to open the result file. ■ Unable to create mount destination directory. ■ Unable to create directory for a log file.	■ Not enough space is available on the scan host. ■ SSH user does not have access to the required directories on the scan host.	■ On a Windows scan host, check space availability in `C:\` ■ On a Linux scan host check space availability in `/tmp`

Issue related to NAS-Data-Protection

- When upgrading NetBackup from previous version to NetBackup version 10.3 or later with the following options selected, the `No images match the search criteria` message is displayed:

Options	Fields
Search by: Backup images	**Policy type**: NAS-Data-Protection **Copies**: Copy2 **Malware scan status**: Not scanned (Default)
Search by: Assets by policy type	**Policy type**: NAS-Data-Protection **Copies**: Copy2 **Scanner host pool**: Select the required scanner host pool. **Malware scan status**: Not scanned (Default)

Workaround

To view the images that are backed up, ensure that you select the **Malware scan status** option as **All** to scan the NAS-Data-Protection backup images created on earlier version of NetBackup media server.

- **File write error**

  File write error

  While running a malware scan on NAS-Data Protection Policy, a `.tar.gz` file (~13 GB) was skipped with the following error message:

  ```
  File write error
  ```

  The NetBackup Malware Scanner, also known as Avira, extracts the contents of compressed or archived files to a staging volume prior to scanning. If there is insufficient space in the staging volume to extract the compressed or archived files, those files may be skipped during the scanning process and will be reported as unscannable files. It is possible to export a list of unscannable files from the scan results. The reason for skipping a file will be indicated as follows:

  ```
  File write error
  ```

  Workaround:

  The default size of the staging volume is 10GB, which must be increased if there is a large number of compressed or archived files in the backup, or if the compressed or archived files are nested, such as a zip file containing `.jar` or `.war` files.

Issues in scan performance

When using Instant Access mount points for malware scan (traditional malware scan) in NetBackup versions prior to 10.3, performance issues were observed.

Workaround: Upgrade to NetBackup media and storage server 10.3 or later. NetBackup 10.3 introduces the **dynamic scan** feature. This improves the instant access time as well as the scan performance.

The following table provides the differences between the traditional malware scan and dynamic scan:

Key scanning procedure	Traditional malware scan using Instant Access mount points	Dynamic scan
Instant access stage.	Analyzes the tar stream and builds each file's header and extent map file (LMDB database), which is time consuming for large number of files in the backup.	Restores TIR (catalog database) and IM (image metadata) information from fragment.

Key scanning procedure	Traditional malware scan using Instant Access mount points	Dynamic scan
Instant access share (NFS/SMB) is mounted and user tries to list or access the file.	Accesses it's header file and reads the attribute from it.	Query's the directory from catalog database to get all the files and directories which are under this directory. It can also query each files and directories attribute to the output.
Scan host opens a file	Opens and loads the LMDB database.	Builds the index in memory and reads directly from data container. ■ To get file's extent by locating and reading the tar header and analyze the content. ■ To get SO list (PureDisk only) by searching the SO list from fragment FP map ■ To build mapping table by inserting the SO list (PureDisk only)
Scan host reads a file	Searches from LMDB database and reads from data container.	If storage server is 3rd party storage vendor, it reads data through OST interface directly. If storage server is PureDisk, it searches from mapping table and reads data from data container.

Details of log file location for errors

The following table provides the details for the respective log files to be viewed depending on the use case:

Table 2-13 Log file locations for Agentless scan host

Use case	Components on primary server	Components on media server	Log file path
Configurations	nbwebservice	ncfnbcs	For primary server: ■ /usr/openv/logs/nbwebservice ■ /usr/openv/netbackup/logs/bprd/ For media server: ■ /usr/openv/logs/ncfnbcs ■ /usr/openv/netbackup/logs/nbmalwarescanner/
Scan process	nbwebservice bprd	ncfnbcs nbmalwarescanner	
Recovery	nbwebservice bprd		

Table 2-14 Log file locations for NetBackup client as the scan host

Use case	Components on primary server	Components on the scan host client	Log file path
Configurations	nbwebservice	nbsubscriber	■ /usr/openv/netbackup/logs/nbscanhostconfigure/ ■ /usr/openv/logs/nbsubscriber/
Scan process	nbwebservice bprd	nbsubscriber	
Recovery	nbwebservice bprd		

SSH login is disabled by default

For VMWare VM backup scan, ensure that you use scan user with `uid=0`. SSH login is disabled by default and user may not enable it for security reasons.

Workaround

In above scenario, perform the following:

If SSH login is disabled for the root user, then non-root scan user can be added to group 0 (root) to be able to scan all the files.

For example, `uid=1001(scanuser) gid=1001(scanuser) groups=1001(scanuser),0(root)`

Malware status displayed as 'Not supported' for Hyper-V images

During upgrade, the malware status for Hyper-V images created in NetBackup version prior to 11.0.0.1 are displayed as **Not supported**. For newly backed up images post upgrade, default malware status for Hyper-V backup images will be displayed as **Not Scanned**.

Workaround

User can perform malware scan on the Hyper-V images displayed as **Not supported**.

NFS mount daemon issue after Flex Scale upgrade

After upgrading NetBackup Flex Scale from version 3.5 to later version, the NFS mount daemon (`nfs-mountd`) may not initialize correctly. As a result, malware scan operations fail with the following error message because the required Instant Access (IA) NFS mounts are unavailable on the scan host:

```
systemctl status nfs-mountd

* nfs-mountd.service - NFS Mount Daemon
 Loaded: loaded (/usr/lib/systemd/system/nfs-mountd.service; static;
 vendor preset: disabled)
 Drop-In: /etc/systemd/system/nfs-mountd.service.d
   `-override.conf
 Active: active (running) since Wed 2025-11-26 20:17:14 IST; 17h ago

 Main PID: 766 (rpc.mountd)

Nov 26 20:17:15 systemd[1]:
/etc/systemd/system/nfs-mountd.service.d/override.conf:2: Failed to
 add dependency on rpcb>
Nov 26 20:17:16 systemd[1]:
/etc/systemd/system/nfs-mountd.service.d/override.conf:2: Failed to
 add dependency on rpcb>
Nov 26 20:17:18 systemd[1]:
/etc/systemd/system/nfs-mountd.service.d/override.conf:2: Failed to
 add dependency on rpcb>
Nov 26 20:19:31 systemd[1]:
/etc/systemd/system/nfs-mountd.service.d/override.conf:2: Failed to
 add dependency on rpcb>
```

This issue occurs due to a service startup dependency timing issue between the following system services:

- `rpcbind`
- `nfs-mountd`

After the NetBackup Flex Scale upgrade, the `nfs-mountd` service may start before the `rpcbind` service is fully initialized, which results in improper NFS service initialization. This prevents NetBackup from successfully creating or accessing Instant Access NFS exports required for malware scanning.

Workaround:

Perform the following to reinitialize the NFS services:

1. Disable NFS version 3 server services :

   ```
   setting NFS disable-nfsv3
   ```

2. Enable NFS version 3 server services:

   ```
   setting NFS enable-nfsv3
   ```

The `nfs-mountd` service initializes successfully without `rpcbind` dependency errors.

Instant Access NFS mounts are created and accessible from the scan host. Malware scan operations complete successfully without failures.

Troubleshooting issues with NetBackup jobs that are enabled for data-in-transit encryption

The given NetBackup job can be of type backup, restore, duplication, replication, import, verify and so on. The job is enabled for data-in-transit encryption (DTE) through the global DTE setting or the client DTE mode.

For more details on DTE, see the *NetBackup Security and Encryption Guide*.

Issue: Operation fails with EXIT STATUS 23: socket read failed

The given operation can be backup, restore, import, verify, duplication, synthetic backup ans so on. The failure is in determining the DTE mode for the given operation. This is due to failure in fetching the global DTE mode as it is not refreshed in the `bpcd` process.

The following error is seen in `bpcd`:

```
The global data-in-transit encryption setting cannot be fetched (8304).
```

Table 2-15 Logs to be checked

Operation	Logs
Backup or archive	Primary server - `nbjm`, `bpcd`, `nbwebservice`
Restore	Primary server - `admin` (catalog recovery), `bprd`, `bpcd`, `nbwebservice`
Duplication, verify, synthetic backup, replication	Primary server - `admin`, `bpcd`, `nbwebservice`
Import	Primary server - `admin`, `bpcd`, `nbwebservice` Media server - `bpdm` or `bptm`

Logs for UNIX:

Legacy logs: `/usr/openv/netbackup/logs`

VxUL logs: `/usr/openv/logs`

Logs for Windows: *`install_path`*`\NetBackup\logs`

Cause

The NetBackup web service took more time to restart as a result of which the global DTE cache of `bpcd` is not refreshed. It results into a failure of the given operation while determining the DTE mode.

Resolution

Retry the operation after 2 minutes of the service restart so that the global DTE mode is successfully refreshed by the web service in the next iteration.

Issue: Cannot determine the data-in-transit encryption (DTE) mode, status 3000004

The failure is during determining the DTE mode for the given operation. This is because the media server DTE mode cannot be retrieved.

Table 2-16 Logs to be checked

Operation	Logs
Backup or archive	Primary Server - `nbjm`, `nbemm`
Restore	Primary Server - `bprd`, `nbemm`
Duplication, verify, synthetic backup, replication	Primary Server - `admin`, `nbemm`

Table 2-16 Logs to be checked *(continued)*

Operation	Logs
Import	Primary Server - `admin`, `nbemm` Media Server - `bpdm` or `bptm`

Logs for UNIX:

Legacy logs: `/usr/openv/netbackup/logs`

VxUL logs: `/usr/openv/logs`

Logs for Windows: *`install_path`*`\NetBackup\logs`

Cause

Failure in retrieving the media server DTE setting from EMM, resulting in failure of the operation.

Resolution

Retry the operation to successfully retrieve the media server DTE mode.

Issue: Operation fails with error - Failed to retrieve the pre-shared key which is required for TLS communication (8316)

Table 2-17 Logs to be checked

Operation	Logs
Backup or archive	Client - `bpbkar` or `dbclient`, `vnetd`, `bpclntcmd` Media server - `bptm`, `bpclntcmd`, `vnetd`
Restore	Client - `tar` or `dbclient`, `vnetd`, `bpclntcmd` Media server - `bpbrm`, `bptm`, `bpclntcmd`, `vnetd`
Duplication	Both media servers - `bptm` or `bpdm`, `vnetd`, `bpclntcmd`

Logs for UNIX: `/usr/openv/netbackup/logs`

Logs for Windows: *`install_path`*`\NetBackup\logs`

Cause

There is a failure while retrieving the pre-shared key that is required for TLS handshake between hosts. This is because of either of the following issues in `bpclntcmd` such as:

- storing the pre-shared key in `bpclntcmd` failed
- `bpclntcmd` failed to provide the pre-shared key

As a result of this issue, multiple NetBackup operations such as backup, restore or duplication fail.

Resolution

Stop the existing `bpclntcmd -store` process and retry the operation.

Issue: Duplication fails with error - cannot connect on socket (25) or the requested operation was partially successful (1)

Table 2-18 Logs to be checked

Operation	Logs
Duplication	Target media server - `bptm` or `bpdm`, `vnetd`

Logs for UNIX: `/usr/openv/netbackup/logs`

Logs for Windows: *`install_path`*`\NetBackup\logs`

Error in job details:

```
Jan 19, 2022 8:49:36 PM - Error bpdm (pid=18607) cannot connect to the
writing side process for duplication, Success Jan 19, 2022 9:37:02 PM - Error
(pid=1028) listen protocol error - couldn't accept from data socket,
The operation completed successfully. Jan 19, 2022 9:37:03 PM - Info bptm
(pid=1028) EXITING with status 25 <----------
```

Cause

When data-in-transit encryption (DTE) is enabled, `vnetd` process is responsible for setting up the pre-requisites required for DTE TLS handshake. On a busy machine, if `vnetd` spends more time doing this, `bptm` times out before `vnetd` forwards the connection. As a result of this, duplication fails.

Solution

On the target host, increase the timeout for accepting connection from `vnetd`. Use the `nbgetconfig` and `nbsetconfig` commands to increase the timeout of the `VNET_OPTIONS` configuration option.

For example, to change the timeout from 120 seconds to 300 run the following commands:

```
nbgetconfig VNET_OPTIONS VNET_OPTIONS = 120 3600 200 40 3 1 30 10
1793 32 0 0

nbsetconfig nbsetconfig> VNET_OPTIONS = 300 3600 200 40 3 1 30 10
1793 32 0 0
```

Only the first value is changed to '300'.

Troubleshooting issues with Unstructured Data Instant Access

Problem:

Failed to create the instant access with error code 4001 for Unstructured Data Instant Access in AKS (Azure Kubernetes Service) or EKS (Amazon Elastic Kubernetes Service) environment.

Cause:

The MSDP engine on which the backup data is stored may not be in a healthy state.

Sample response message:

```
{
  "errorCode": 4001,
  "errorMessage": "Failed to create the instant access mount.",
  "attributeErrors": {},
  "fileUploadErrors": [],
  "errorDetails": [
    "Failed to provision the backup. /usr/openv/pdde/vpfs/bin/vpfs_
     actions failed (1): Unable to getCatalog: ('Could not get
     catalog of backup
(test-mssql1_1654780591): /usr/openv/pdde/vpfs/bin/cata2map failed
(255): ', {'statusInfo': {'msgId': 'Failed to
get catalog', 'parameters': [{'type':
'string', 'name': 'backupId', 'value':
'test-mssql1_1654780591'}]}})\n"
  ]
}
```

Resolution:

Check if the MSDP engines are healthy in your AKS or EKS environment. Alternatively, you can create a new backup and create Unstructured Data Instant Access again using its API interface.

Troubleshooting issues with multifactor authentication

This topic provides information on troubleshooting issues that are specific to multifactor authentication in NetBackup.

For more information on multifactor authentication, see the NetBackup Web UI Administrator's Guide.

Table 2-19

Sr. No.	Issue	Possible reason	Resolution
1.	You attempt to log in to the NetBackup web UI but instead you land on the page to configure multifactor authentication.	NetBackup administrator has enforced multifactor authentication in the domain, however you have not configured it for your user account.	As multifactor authentication is enforced, you must configure multifactor authentication for your user account.
2.	During multifactor authentication configuration, you are not able to scan the QR code using multifactor authentication configuration UI.	There maybe some issue with the QR code or the QR code scanner.	If you are not able to scan the QR code from the multifactor authentication configuration UI, you can copy or see the secret key, and can manually insert the secret key in the authenticator application.
3.	During multifactor authentication configuration, the user is not able to see or copy the secret key from the multifactor authentication configuration UI.	There maybe some issue with the hide / show option or the copy option in the UI.	From the authenticator application, you can scan the QR code.
4.	During configuration of multifactor authentication, after specifying the correct one-time password and clicking **Configure**, the following error is displayed: `Failed to validate one-time password.`	There is a time difference between your handheld device and the NetBackup primary server or the specified one-time password is wrong.	Ensure that the time of your handheld device matches that of the primary server. Enter the correct one-time password before it expires.
5.	During multifactor authentication configuration, when you scan the QR code and try to overwrite the existing security information in the authenticator application, an error is displayed.	Authenticator application is not able to overwrite the security information.	Before scanning the QR code, ensure that a duplicate entry is not present.

Table 2-19 *(continued)*

Sr. No.	Issue	Possible reason	Resolution
6.	If multifactor authentication is configured, but the security entry in the authentication application is not present. As a result, you cannot see the one-time password and cannot authenticate.	One-time password cannot be generated in the authenticator application. The smart device is lost.	You must contact the NetBackup administrator to reset your multifactor authentication configuration. After the successful reset, reconfigure multifactor authentication for your user account.
7.	You are a NetBackup administrator and have configured multifactor authentication for your own user account, however one-time password is not available.	Security information is deleted from the authenticator application or the handheld device is lost.	You can request another administrator to reset your multifactor authentication configuration and then you can reconfigure multifactor authentication for your user account. Alternatively, you can request the OS Administrator to reset your multifactor authentication configuration using the following command: `nbseccmd -resetMFA -userinfo <domain type>:<domain name>:<user name>`
8.	The `bpnbat -login` CLI shows the following error: `AT authentication failed`	You have configured multifactor authentication for your user account, however the login type 'AT' does not support multifactor authentication.	Use the `bpnbat -login -logintype WEB` command if multifactor authentication is configured for your user account. It is recommended that you use the interactive mode (`bpnbat -login (-Interactive | -i )`) to login if multifactor authentication is configured.
9.	You have not configured multifactor authentication for your user account and `bpnbat -login` fails.	NetBackup administrator must have enforced multifactor authentication for all users in the domain.	If multifactor authentication is enforced, you have to configure it for your user account and run the `bpnbat -login (-Interactive | -i )` command to login.

Table 2-19 *(continued)*

Sr. No.	Issue	Possible reason	Resolution
10.	During the `bpnbat -login` operation, you have specified the correct username and password to logon to the NetBackup host that is earlier than 10.3, but authentication fails.	You have configured multifactor authentication for your user account.	You must provide the one-time password after the password when you run the `bpnbat -login` command.
11.	During the `bpnbat -login` operation, the cred file (-cf) is used, but login failed.	You have configured multifactor authentication for your user account.	You must use the `bpnbat -login (-Interactive | -i )` command to login when the cred file is used.
12.	During `bpnbat -login`, you have provided the correct user name, password, and one-time password, but authentication failed.	There is a time difference between your handheld device and the NetBackup primary server or the specified one-time password is wrong.	Ensure that the time of your handheld device matches that of the primary server. Enter the correct one-time password before it expires.
13.	During the **NetBackup Administration Console** login, the following error is displayed: "Failed to check whether multifactor authentication is enabled for the user account or not."	The web service is down or the it is unable to process the request.	Ensure that the web service up and running. Check the following logs: bpjava logs: `/usr/openv/netbackup/logs/bpjava-msvc` web service logs: `/usr/openv/logs/nbwebservice`
14.	During the **NetBackup Administration Console** login, the following error is displayed even when the correct username and password are specified: "Invalid username or password."	You have configured multifactor authentication for your user account.	You should provide the one-time password after the password.
15.	In the **NetBackup Administration Console**, the following error is displayed: `Failed to validate the one-time password.`	There is a time difference between your handheld device and the NetBackup primary server or the specified one-time password is wrong.	Ensure that the time of your handheld device matches that of the primary server. Enter the correct one-time password before it expires.
16.	When setting up trust between NetBackup primary server using `nbseccmd`, authentication failed.	You have configured multifactor authentication for your user account.	You should provide the one-time password after the password.

Table 2-19 *(continued)*

Sr. No.	Issue	Possible reason	Resolution
17.	The `nbdeployutil --gather` command failed for one or more primary servers.	You have configured multifactor authentication for your user account in a failed primary server.	Run the following command: Run the `nbdeployutil --gather` CLI with the `--apikey-file` option. The format of apikey key file should be *NetBackup Primary hostname* : *APIKey* For multiple NetBackup domains, ensure that apikeys are provided for all primary server hosts.
18.	When setup trust between primary servers fails from the NetBackup web UI, NetBackup Administration Console, or `nbseccmd` CLI	You have configured multifactor authentication for your user account.	If the user account is configured for multifactor authentication on the target host, append appropriate one-time password to the password.
19.	The following error is displayed when you use the validate OTP API: `The multifactor authentication request ID does not exist.`	The specified request ID does not exist.	Specify a valid request ID while using the validate OTP API.
20.	The following error is displayed when you use the validate OTP API: `The multifactor authentication request is not valid.`	The JWT token that is used for the subsequent API call is different than the earlier one.	Use the same JWT token for both the API calls.
21.	The following error is displayed when you change the NetBackup configuration: `The configuration cannot be changed using this host.`	Multifactor authentication is configured for the user account, however this host does not support multifactor authentication.	Use the NetBackup web UI to perform the operation.

Table 2-19 *(continued)*

Sr. No.	Issue	Possible reason	Resolution
22.	The following error is displayed when you execute the `nbcertcmd` or `nbseccmd` command: `EXIT STATUS 3676: invalid error number`	Multifactor authentication is configured for the user account, however this host does not support multifactor authentication.	Use the NetBackup web UI to perform the operation.
28.	The following error is displayed while you modify global security settings, create API keys, or run the `nbcertcmd` or `nbseccmd` command: `The multifactor authentication request has timed out.`	There was a delay in entering the one-time password.	During multifactor authentication, ensure that you enter the one-time password within 180 seconds. When you use APIs, ensure that you call the successive 'validate OTP' API within 180 seconds.

Troubleshooting issues with multi-person authorization

This topic provides information on how to troubleshoot issues that are specific to multi-person authorization process in NetBackup.

For more information on the multi-person authorization, see the NetBackup Security and Encryption Guide.

Table 2-20

Sr. No.	Issue	Possible reason	Resolution
1.	After enabling multi-person authorization, NetBackup Vault creation or modification operation fails in the **NetBackup Administration Console** with the following error: `Intermittent connectivity lost with the server.`	Multi-person authorization is enabled for the image expiration operation.	Contact the NetBackup Security Administrator to exempt the user from the multi-person authorization process.

Table 2-20 *(continued)*

Sr. No.	Issue	Possible reason	Resolution
2.	After enabling multi-person authorization, the `nbholdutil -delete` command on the earlier media server fails with the following error: `Permission Denied by Hold Service`	Multi-person authorization in enabled for the image hold deletion operation on the primary server.	Do one of the following: ■ Upgrade the media server to the current NetBackup version. ■ Ensure that the user is added as an exempted user for multi-person authorization. Refer to the 'Add exempted users' topic in the NetBackup Web UI Administrator's Guide. ■ Login (as exempted user) using `bpnbat -login`. ■ Run the `nbholdutil` command.
3.	One of the following operations fails with the exit status: 9382 Error: `The operation has failed because it is configured for multi-person authorization.` ■ On NetBackup10.3 or earlier host, one of the following commands fails: `bpexpdate`, `bpimage -deletecopy`, `nbdecommission` ■ The `nbdecommission -oldserver` *`serverName`* `-machinetype media` fails.	Multi-person authorization is enabled for the image expiration operation.	■ If the invoking host is earlier than NetBackup 10.0, image expiry operation is blocked for such hosts, even if the user is exempted from the multi-person authorization process. ■ If the invoking host is NetBackup 10.0 or later, contact the NetBackup Security Administrator to exempt the user from the multi-person authorization process. Sign into the NetBackup web UI again and retry the operation.
4.	A user that is exempted from the multi-person authorization process is not able to perform the multi-person authorization enabled operation using CLIs and the error with 5930 error code is displayed.	The user is not authenticated. The `bpnbat -login -logintype WEB` command is not run after adding the user to the exempted list.	Run the `bpnbat -login -logintype WEB` command to successfully load the current permission set and perform the multi-person authorization enabled operation using one of the following interfaces: ■ Using CLIs ■ Using the **NetBackup Administration Console** ■ Using the NetBackup web UI

Table 2-20 *(continued)*

Sr. No.	Issue	Possible reason	Resolution
5.	User is removed from the exempted users' list, however is able to run a multi-person authorization enabled operation without a second approval.	Removal of a user from the exempted user list creates a multi-person authorization ticket. However, the associated ticket is not yet approved.	Check if a ticket for multi-person authorization configuration is created. Request the multi-person authorization approver to approve the ticket. After the approval, the user is removed from the exempted list.
6.	An exempted user failed to expire an image (failed to perform a multi-person authorization enabled operation)	■ The user is not authorized to perform the operation. ■ A multi-person authorization ticket for an exempted user's request is not created. The issue may not be related to the multi-person authorization process.	Refer to the respective documentation.
7.	A multi-person authorization enabled operation is successful using the **NetBackup Administration Console** or CLIs.	The user must be in the exempted users' list.	If you want a multi-person authorization ticket to be created for this user, remove the user from the exempted users' list.
8.	Unable to add user groups to the exempted list.	Adding user groups to the exempted list is not allowed.	Add individual users to the exempted list.
9.	When trying to configure multi-person authorization from the NetBackup web UI, the following error is displayed: `The date is not within the allowed range that is between 01/01/1970 and the current date`	System date must not be set correctly.	Check the system date and specify a valid date that is between 01/01/1970 and the current date. Correct the date and restart the NetBackup services.
10.	Multi-person authorization tickets do not get expired even after the scheduled expiration period.	■ The NetBackup Web Management Console (`nbwmc`) service or daemon is down. ■ NetBackup PostgreSQL database services or daemons are down.	Start the NetBackup Web Management Console (`nbwmc`) and the NetBackup PostgreSQL database services or daemons.

Table 2-20 *(continued)*

Sr. No.	Issue	Possible reason	Resolution
11.	Multi-person authorization tickets do not get purged even after the scheduled purge period.	■ The NetBackup Web Management Console (`nbwmc`) service or daemon is down. ■ NetBackup PostgreSQL database services or daemons are down. ■ There are no tickets in the Expired, Done, Rejected, and Canceled states that have reached the purge period.	Start the NetBackup Web Management Console (`nbwmc`) and the NetBackup PostgreSQL database services or daemons.
12.	NetBackup image expiry operation execution failed using CLIs after enabling multi-person authorization.	If multi-person authorization is enabled for an operation on the primary server, that operation is allowed only using the web UI and APIs. If user tries to perform the operation using the **NetBackup Administration Console** or the command-line interface, the operation fails.	■ Perform the operation using the NetBackup web UI. ■ Contact the NetBackup Security Administrator to exempt the user from the multi-person authorization process.
13.	Not able to fetch a multi-person authorization ticket.	■ The specified ticket ID may not be valid. ■ NetBackup Postgres database services or daemons are down.	■ Specify a valid ticket ID. ■ Ensure that Check all the required services are up and running.
14.	Unable to update the state of the multi-person authorization ticket.	The multi-person authorization ticket cannot be updated, because the current state of the ticket cannot be changed to the proposed state.	Check the current state of the multi-person ticket and ensure that you are performing the operation based on the following state transitions that are allowed: Current state - Pending, Expired Proposed state - Approved, Rejected, Canceled, Pending

Table 2-20 *(continued)*

Sr. No.	Issue	Possible reason	Resolution
15.	Unable to update the multi-person authorization ticket.	If you are not the requester of the ticket or the multi-person authorization approver, you cannot approve, reject, cancel, or renew the ticket or add a comment.	Contact the NetBackup Administrator for the required permissions.
16.	While configuring multi-person authorization or performing any associated operations on a ticket, the following error is displayed: `Unable to connect to server`	The NetBackup Web Management Console service may be down.	Ensure that all the required NetBackup services are up and running.
17.	Image expiration operation using CLIs failed with error code 9387 after multi-person authorization is enabled.	If the multi-person authorization is enabled for the operation on the primary server, a ticket is generated when the operation takes place.	Check the current state of the multi-person authorization ticket by signing into NetBackup web UI. The ticket should be approved after which the operation is successful.
18.	A user is not able to perform the multi-person authorization enabled operation using CLIs and the error with 5930 error code is displayed.	The user is not authenticated. The `bpnbat -login -logintype WEB` command is not run.	Run the `bpnbat -login -logintype WEB` command to successfully load the current permission set and perform the multi-person authorization enabled operation using CLI:
19.	Image expiration operation using CLI did not create a ticket after multi-person authorization is enabled.	■ NBAC is enabled. ■ The user is exempted from multi-person authorization and the user has logged in using `bpnbat -login -lointypeWEB`.	■ Ensure that NBAC is not enabled. Multi-person authorization is not supported with NBAC. ■ Ensure that the user is not exempted. Tickets are not generated for exempted users when they perform multi-person authorization enabled operations.
20.	Image expiration operation through CLI using bid file failed with error code 20 after multi-person authorization is enabled.	The bid file is not in the required format.	Ensure that the bid file is in the required format and it contains up to 100 entries. A maximum of 100 images can be expired in a bulk when multi-person authorization is enabled.

Table 2-20 *(continued)*

Sr. No.	Issue	Possible reason	Resolution
21.	`nbcertcmd -setsecconfig`, `nbseccmd -setsecurityconfig` command fails on the media server and client. Request to set the certificate deployment level failed. Exit status: 5969 Error: `Response from the NetBackup Web Management Console service could not be parsed.`	Media server and client hosts are earlier than NetBackup 10.3	Upgrade NetBackup to the current version. Check if a ticket is created for the operation in the web UI.
22.	Unable to see UNCHANGED/UPDATED values in multi-person authorization ticket details.	Unable to read the JSON API payload.	Check if all fields in the API payload are passed as expected.
23.	Multi-person authorization ticket is created for exempted users after global security settings are modified.	Exempted users need to go through multi-person authorization when they modify multi-person authorization configuration, global security settings, or risk engine-based anomaly detection configuration.	Contact your MPA Approver for the ticket approval.
24.	Image expiry ticket is not marked as 'conflicting with' when there is a conflict	Tickets that are in pending state are not marked as 'conflicting with' for the following operations: multi-person authorization configuration, global security settings	Tickets for the following operations are not marked as 'conflicting with': Image expiry, WORM configuration change, WORM retention lock removal, remove image hold

Troubleshooting connections to the NetBackup Scale-Out Relational Database

If you see connection issues with your account and the NetBackup database, the account and password information in the pgbouncer's `userlist.txt` file may be out of sync with the NetBackup database. To resolve this situation, use the

`nbdb_admin -update-user-list` command to sync the information in the file and the database.

To sync the userlist.txt file with the NetBackup database

1. Run the following command:

   UNIX:

   `/usr/openv/db/bin/nbdb_admin -update_user_list`

   Windows:

   `install_path``\NetBackup\bin\nbdb_admin -update_user_list`

2. If you continue to see connection issues, restart the NetBackup services.

Troubleshooting issues with private key encryption

This topic provides information on how to troubleshoot issues that are specific to private key encryption.

Passphrases are used to encrypt and decrypt the private keys of NetBackup host ID-based certificates. Passphrase keys are used to encrypt and decrypt these passphrases.

The private key of the NetBackup certificate is stored in an encrypted format using AES_256_CBC encryption. The password that is used to encrypt the private keys is stored in file storage and is encrypted using AES_256_GCM encryption.

Private key encryption file paths

Keystore location:

On Windows: *`Install path`*`\NetBackup\var\vxss\credentials\keystore`

Linux: `/usr/openv/var/vxss/credentials/keystore`

Keystore location for cluster:

`/usr/openv/var/global/vxss/credentials/keystore`

Nbcert logs:

On Windows: *`Install path`*`\NetBackup\logs\nbcert`

On Linux: `/usr/openv/netbackup/logs/nbcert`

Passphrase file path: `keystorepath + .yekekp`

Passphrase key file path: `keystorepath + .yekcneekp`

certmapinfo.json file path:

On Windows: **`Install path`**`\NetBackup\var\vxss\certmapinfo.json`

On Linux: `/usr/openv/var/vxss/certmapinfo.json`

Table 2-21

Sr. No.	Issue	Possible reason	Resolution

1	Command: `nbcertcmd -listcertdetails`
	
	`Output:`
	`Private Key Encryption State: Encrypted with an unknown passphrase`
		The private key file is tampered.	**1** Clean up the private key file for the server.
			2 Run the following command on all the servers that are associated with the host:
			■ `nbcertcmd -getCertificate -token reissue_token -server server host name -force`

2	For the following problem scenarios, the reason and the resolution are the same:
	
	Command: `nbcertcmd -listcertdetails`
	
	Output:
	
	`Private Key Encryption State: Encrypted with an unknown passphrase`
	
	Command: `nbcertcmd -rotatePassphrasekey`
	
	`The passphrase key rotation failed. EXIT STATUS 1200: Internal error`
		The passphrase file or the passphrase key file is tampered.	**1** Check the last modification date of the passphrase file.
			2 Clean up the keystore folder including the hidden files.
			3 Run the following command on all the servers that are associated with the host:
			■ `nbcertcmd -getCertificate -token reissue_token -server server host name -force`

Table 2-21 *(continued)*

Sr. No.	Issue	Possible reason	Resolution

3	While you perform catalog restore after the fresh NetBackup installation, you can see both the newly-created private keys from the fresh installation and the restored ones.
	Command:
	`ls -la`
	`total 20 drwx------ 2 nbsvcusr nbsvcusr 171 Jun 19 19:38`
	`drwx------ 3 nbsvcusr nbsvcusr 133 Jun 19 19:25 ..`
	`-rw------- 1 nbsvcusr nbsvcusr 1858 Jun 19 19:38`
	`015b91f5-74b5-44fb-865f-6d65827cdb30-key.pem`
	`-rw------- 1 nbsvcusr nbsvcusr 1858 Jun 19 19:38`
	`015b91f5-74b5-44fb-865f-6d65827cdb3r-key.pem`
		Restoring the catalog reintegrates the existing private keys and passphrase files into the keystore. The keystore then includes both the newly-created private keys from the fresh installation and the restored ones.	■ Clear the private key files that do not have entry in the `certmapinfo.json` file.
			Location of the `certmapinfo.json` file on Unix:
			`/usr/openv/var/vxss/certmapinfo.json`

4	The following notification is seen on the NetBackup web UI: `Reissuing the host certificates during private key encryption failed for the following hosts: host1`	Reissue of the certificate is attempted during the private key encryption operation.	■ Run the following command: `nbcert -listCertDetails -json` The subsequent restart of the services may encrypt all the private keys and the output of this command shows all the keys in the Encrypted state. If all the keys are not encrypted, run one of the following commands for the private keys with state other than Encrypted: ■ `nbcertcmd -reissuecertificates -server server` ■ `nbcertcmd -getCertificate -token reissue_token -server server host name -force`

Table 2-21 *(continued)*

Sr. No.	Issue	Possible reason	Resolution
5		The restore operation failed because of the absence of backup files or an issue with the file rewrite process.	■ Check if the backup files are present(files that have the suffix '_bkup') in the same keystore folder. ■ Perform following: ■ Verify the status using `nbcertcmd -listcertdetails` ■ If all the primary servers are showing the private key encryption status as Encrypted, clean up the backup files manually and retry the rotation operation. ■ If the issue still persists, check the following: ■ If some of the primary servers show a private key and the encryption status is 'encrypted with unknown passphrase', restore the passphrase file and the corresponding private key files. ■ Again, check the status using `nbcertcmd -listcertdetails`. Verify if the correct encryption status is shown for the remaining private keys. If it does, retry the rotation operation. ■ If the issue still persists, check the following: ■ If backup files are not present and the command `nbcertcmd -listcertdetails` shows the incorrect encryption status, clean up the keystore. ■ Run `nbcertcmd -getCertificate` with the `reissueToken` option for all servers.

Table 2-21 *(continued)*

Sr. No.	Issue	Possible reason	Resolution

	The attempt to rotate the passphrase failed, the private key files and the passphrase file could not be restored.
	Command: [root@example keystore]
	`nbcertcmd -rotatepassphrase`
	This operation performs the rotation of passphrase that encrypts the private key of the host ID-based certificates.
	It is strongly recommended that you stop the NetBackup services before you perform this operation. Ensure that you restart the services after the operation is performed.
	Are you sure you want to proceed with this operation? (y/n) y
	`The passphrase rotation failed. EXIT STATUS 9141: Keystore is in inconsistent state.`
	`Command: ls -la total 20 drwx------ 2 nbsvcusr nbsvcusr 176 Jul 16 11:55 . drwx------ 3 nbsvcusr nbsvcusr 133 Jul 4 22:24 .. -rw------- 1 nbsvcusr nbsvcusr 1858 Jul 16 11:51 5176ec69-d3cb-44d7-a229-799555b7bd7e-key.pem -rw------- 1 nbsvcusr nbsvcusr 1858 Jul 16 11:54 5176ec69-d3cb-44d7-a229-799555b7bd7e-key.pem_bkup -rw------- 1 nbsvcusr nbsvcusr 1858 Jul 16 11:51 PrivKeyFile-2048.pem -rw-r--r-- 1 nbsvcusr`		

Table 2-21 *(continued)*

Sr. No.	Issue	Possible reason	Resolution
	`nbsvcusr 1072 Jul 16 11:51 .yekcneekp` `-rw-r--r-- 1 nbsvcusr nbsvcusr 271 Jul 16 11:52 .yekekp`		

Troubleshooting issues with the security configuration risk feature

Security configuration risk depends on the status of the security settings in your NetBackup domain. A higher configuration risk score indicates weaker security configurations. To minimize the risk, enable all the security settings.

For more information on the security configuration risk feature, refer to the NetBackup Security and Encryption Guide.

Table 2-22

Sr. No.	Issue	Possible reason	Resolution
1.	Internal server error in: `GET API /security/status`	Error in extracting the cluster name or client name for the given host through NetBackup Service Layer (NBSL). Check the logs to confirm the following: "Cannot retrieve hostName from system property"	Check if the NBSL service is up and running. Ensure that the Client name (virtual name in case of cluster) is properly set for the given primary server.
		Exception in searching for the given host by its host name in database. Check the logs to confirm the following: "Exception occurred: hostname not found."	Ensure that the NetBackup database services are up and running. Increase verbosity, and retry the operations. Contact Cohesity technical support.
		Failure in reading base state template from database. Check the logs to confirm the following: "Caught exception while reading security template json."	Ensure that the correct JSON file is present in the database in EMM_MAIN schema: `emm_hostconffileversiondata` No key should have a null value.
		Error in extracting number of hosts configured with service user from the database. Check the logs.	Ensure that the NetBackup database services are up and running. Increase verbosity, and retry the operations. Contact Cohesity technical support.
		API failed to extract malware configuration details for the host. Check the logs to confirm the following: "Exception raised from getting malware settings"	Increase verbosity, and retry the operations. Contact Cohesity technical support.
			Ensure the NetBackup database services are up and running. Increase verbosity, and retry the operations. Contact Cohesity technical support.

Table 2-22 *(continued)*

Sr. No.	Issue	Possible reason	Resolution
		API failed to extract number of hosts from the database. Check the logs to confirm the following: "Cannot retrieve number of hosts from database."	
		API failed to extract supported operations for MPA. Check the logs to confirm the following: "Error in fetching list of MPA supported operations."	Ensure the NetBackup database services are up and running. Increase verbosity, and retry the operations. Contact Cohesity technical support.
8.	Internal server error in `POST API /security/configuration-baseline`	Validation of the request DTO failed. Check the logs to confirm the following: "Request DTO validation failed."	Validate input JSON to the API. Refer to the following to check the possible states of settings: ■ "allowInsecureBackLevelHost": 0/1 ■ "certificateAutoDeployLevel": 0/1/2 ■ "mfaEnforced": false/true ■ "dteGlobalMode": "PREFERRED_OFF"/"PREFERRED_ON"/"ENFORCED" ■ "backupAnomalyDetection": "0/1" ■ "mpa" : "ENABLED"/"DISABLED" ■ "hostPercentageWithServiceUser": "<Precentage value 0 to 100>" ■ "hostPercentageWithDteEnabled": "<Precentage value 0 to 100>" ■ "malwareDetection": "NOT_CONFIGURED"/"CONFIGURED"
9.	Notifications for security configuration risk are not generated.	Security baseline may be changed within 10 seconds of the change in configuration settings.	Avoid changing security baseline within 10 seconds of changing the security settings state. Retry the operations. Contact Veritas technical support if the issue still persists. Collect web service logs and NetBackup audit logs.

Table 2-22 *(continued)*

Sr. No.	Issue	Possible reason	Resolution
10.	Exception with message: "The dashboard security status request or the data that is sent is not valid."	Possible reasons: ■ GET /security/status API refers to record EMM_MAIN. EMM_HostConfFileVersionData - whose VersionID has the highest value. This record may have incorrect JSON as part of field file contents.	Set the security baseline again.
		NetBackup database service is not running.	Ensure that the NetBackup database services are up and running.
		Anomaly management service is not running.	Ensure that Anomaly management service is up and running.
		`nbstserv` is not running.	Ensure that `nbstserv` is up and running.
		NetBackup Service Layer service is not running. The file should have service_user permissions.	Ensure that the NetBackup Service Layer (NBSL) is up and running.
		Validation of the request DTO failed. The payload provided was having one of the unsupported attributes (from API version 13.0) or invalid value.	Validate input JSON to the POST security/configuration-baseline API for request API Version 12.0. The following payload JSON is supported: { "data": { "type": "securityTemplateRequest", "attributes": { "securitySettingsTemplate": { "allowInsecureBackLevelHost": 0, "certificateAutoDeployLevel": 0, "mfaEnforced": false, "dteGlobalMode": "PREFERRED_OFF", "hostPercentageWithDteEnabled": 0, "backupAnomalyDetection": 0, "mpa": "ENABLED", "malwareDetection": "CONFIGURED", "hostPercentageWithServiceUser": 0 } } } }
		Validation of the request DTO failed. The payload was containing attribute with invalid value.	

Table 2-22 *(continued)*

Sr. No.	Issue	Possible reason	Resolution
			Validate input JSON to the POST security/configuration-baseline API for request API Version 13.0. The following JSON is supported: { "data": { "type": "securityTemplateRequest", "attributes": { "securitySettingsTemplate": { "allowInsecureBackLevelHost": 0, "certificateAutoDeployLevel": 0, "mfaEnforced": false, "dteGlobalMode": "PREFERRED_OFF", "hostPercentageWithDteEnabled": 0, "backupAnomalyDetection": 0, "mpa": "ENABLED", "malwareDetection": "CONFIGURED", "hostPercentageWithServiceUser": 0, "backupStoragePercentageWithEncryptionEnabled": 0, "isImmutableBackupStorageConfigured": true, "serverPercentageWithLatestNbuVersion": 0, "clientPercentageWithLatestNbuVersion": 0, "isCliAccessToOsAdmins": 0, "isWebUiAccessToOsAdmins": 0, "redirectedRestore": true } } } }
11.	Some settings do not have baseline value after upgrade	Some of the new security settings that are added in the NetBackup 11.0 do not have baseline set unless you set it explicitly.	Set the baseline values for all the security settings.

Troubleshooting issues with the risk engine-based anomaly detection options

The NetBackup risk engine detects certain system anomalies in a proactive manner and sends appropriate alerts. It helps you take corrective action before you face any security threat in your environment.

For more information on the risk engine, refer to the NetBackup Security and Encryption Guide.

Table 2-23

Sr. No.	Issue	Possible reason	Resolution
1.	NetBackup Administration Console login fails with the following error: `Unable to login, status: 501. You are not authorized to use this application.`	The **Detect unusual user sign in** option of risk engine-based anomaly detection is enabled and multi-person authorization ticket option is enabled for the anomaly. The user sign in is anomalous and therefore it is put on hold.	Do one of the following: ■ User must be added in exempted users' list for multi-person authorization to bypass the anomaly detection check. ■ The user must sign in during usual time. ■ Disable multi-person authorization ticket generation for unusual sign in.
2.	`bpnbat -login` fails with the following error: `You do not have permission to perform the requested operation. AT authentication successful, but web authentication failed.`	The **Detect unusual user sign in** option of risk engine-based anomaly detection is enabled. The user sign in request is from a client with an earlier version.	Do one of the following: ■ User must be added in exempted users' list for multi-person authorization to bypass the anomaly detection check. ■ Run the `bpnbat -login` command on the host with the latest NetBackup version, that is 11.0.
3.	`nbseccmd -setuptrustedmaster` fails with the following error: `The trust setup operation using NetBackup certificate failed. Trusted master operation failed EXIT STATUS 160: Authentication failed [root@exampleserver ~]#`	The **Detect unusual user sign in** option of risk engine-based anomaly detection is enabled. The user sign in request is from a client with an earlier version.	Do one of the following: ■ User must be added in exempted users' list for multi-person authorization to bypass the anomaly detection check. ■ Run the `nbseccmd -setuptrustedmaster` command on the host with the latest NetBackup version, that is 11.0.

Table 2-23 *(continued)*

Sr. No.	Issue	Possible reason	Resolution
4.	None of the users is able to log-in because of MPA restriction	The **Detect unusual user sign in** option of risk engine-based anomaly detection is enabled.	Run the following command: `nbseccmd -disableLoginAnomalyDetection`
5.	User is unable to perform policy update or delete operation from command-line interface.	The **Detect unusual updates to policies** option of risk engine-based anomaly detection is enabled.	Update or delete a policy using the `nbcmdrun` wrapper command from the host with latest NetBackup version, that is 11.0. For example: `nbcmdrun bppldelete P1`

Chapter 3

Using NetBackup utilities

This chapter includes the following topics:

About NetBackup troubleshooting utilities

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

Table 3-1 Troubleshooting utilities

Utility	Description
Analysis utilities for NetBackup debug logs	These utilities 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 214.
Log collection utility	This utility simplifies the gathering of evidence for support cases. For more information, see the following: ■ See "About the Log collection utility" on page 217. ■ NetBackup Logging Reference Guide ■ Logging Assistant FAQ
Network troubleshooting utilities	These utilities 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 218.
NetBackup support utility (`nbsu`)	This utility queries the host and gathers appropriate diagnostic information about NetBackup and the operating system. See "About the NetBackup support utility (nbsu)" on page 219.
NetBackup consistency check utility (`NBCC`)	This utility 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 223.
NetBackup consistency check repair (`NBCCR`) utility	This utility 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 231.
`nbcplogs` utility	This utility simplifies the gathering of logs to deliver to Cohesity technical support. See "About the `nbcplogs` utility" on page 234.
Robotic test utilities	These utilities communicate directly with robotic peripherals. See "About the robotic test utilities" on page 235.

About the analysis utilities for NetBackup debug logs

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

NetBackup jobs span multiple processes that are distributed across servers.

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

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

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

Table 3-2 Analysis utilities for NetBackup debug logs

Utility	Description
	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 primary 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 primary 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.

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

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

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

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

The analysis utilities have the following limitations:

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

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

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

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

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

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

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

daystamp.millisecs.program.sequence machine log_line

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

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

About the Log collection utility

For help on a NetBackup issue, you can use the **Log collection** utility to gather evidence for Technical Support. This utility is available from the **Help** menu and in the Activity monitor. Note that debug logs are for Technical Support to analyze.

For information on the **Log collection** utility, see the NetBackup Logging Reference Guide.

For information on the Logging Assistant, see the article Logging Assistant FAQ.

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

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

About the NetBackup support utility (nbsu)

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

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

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

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. Cohesity recommends use of the newer version (nbsu).

Cohesity 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 Cohesity 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 Cohesity 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 Cohesity Evidence Server. For additional assistance, see: https://support.cohesity.com/s/article/article-100038665
- 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: *<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 `nbsu` runs, `nbsu` bundles its output files into an archive file. If a supported compression utility is available, `nbsu` compresses the archive file. Otherwise, the individual output files remain unarchived and uncompressed.

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

```
/usr/openv/netbackup/bin/support/NBSU_host1_master_01172018_220505.tgz
```

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

`nbsu` supports tar for archive and gzip for compression.

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

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

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

```
NBU Install path: C:\Program Files\Cohesity NetBackup\
mywindowsvm is a master server
Collecting NBU_adv_disk info
Collecting NBU_all_log_entries info
Collecting NBU_altnames info
Collecting NBU_auth_methods_names info
Collecting NBU_available_media info
Collecting NBU_backup_status info
```

```
Collecting 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 Cohesity 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`

Cohesity 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 Cohesity 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 primary 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 225.

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\Cohesity NetBackup\
> 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
             falconstorvtl5
2.5  Building NetBackup storage unit list...
     Detected Storage Unit for NetBackup for NDMP media server
         reabl3
       and NDMP Host
```

```
        falconstorvtl5
      Detected disk media storage unit host
        lidabl11
      Detected Disk Pool
        lidabl11_pdde_pool
    ...
2.6 Obtaining Disk Pool information...
      Detected Disk Pool
        lidabl11_pdde_pool
          host
            lidabl11
          Detected Disk Pool lidabl11_pdde_pool member
            lidabl11
    ...
2.7 Obtaining tpconfig Storage credential information...
      Detected the master server hostname
        lidabl11
      and associated Storage server hostname
        lidabl11
    ...
2.8 Obtaining tpconfig NDMP configuration information...
      Detected the EMM NDMP Host hostname
        fas3240a
      Detected the EMM NDMP Host hostname
        fas3240b
    ...
2.9 Analyzing EMM master and/or media servers and configured
    Storage Units...
      The following EMM server entries do not have configured
      Storage Units or Disk Pools:

      Media server - lidabl14

2.10 Obtaining NetBackup unrestricted media sharing status...
      Configuration state = NO
2.11 Obtaining NetBackup Media Server Groups...
      No Server Groups configured
2.12 Building NetBackup retention level list...
3.0 Obtaining NetBackup version from media servers
      lidabl11...
      lidabl14...
      reabl3...
      virtualization5400a...
```

```
      ...
3.1  Gathering required NetBackup catalog information
       Start time = 2013-02-27 09:41:07
3.2  Gathering NetBackup EMM conflict table list
       Found 0 EMM conflict records
3.3 Gathering list of all tapes associated with any Active Jobs
       Building NetBackup bpdbjobs list
3.4 Gathering all TryLog file names from the
     C:\Program Files\netbackup\db\jobs\trylogs
     directory
       Found 10 TryLogs for 10 active jobs.
       TryLogs found for all Active Jobs
3.5  Building NetBackup Image database contents list
       Reading Image number 1000
       Reading Image number 2000
       Reading Image number 3000
       Reading Image number 4000
       Found 4014 images in the Image database
3.6  Building EMM database Media and Device configuration
     attribute lists
       Obtaining the EMM database Media attribute list for disk
       virtual server
         lidabl11 ...
         There were 0 bpmedialist records detected for media server
         lidabl11
           Getting device configuration data from server
         lidabl11 ...
     ...
3.7  Building EMM database Unrestricted Sharing Media attribute lists
         Found 0 Unrestricted Sharing media records in the EMM database
3.8  Building the EMM database Volume attribute list...
       Getting the EMM database Volume attributes from EMM server
         mlbnbu ...
       Found 43 Volume attribute records in the EMM database
3.9  Building NetBackup volume pool configuration list
       EMM Server lidabl11
3.10 Building NetBackup scratch pool configuration list
       EMM Server lidabl11
3.11 Gathering NetBackup EMM merge table list
       Found 0 EMM merge table records

     Summary of gathered NetBackup catalog information
       End time = 2013-02-27 09:44:16
```

```
       Number of Images gathered = 4014
       Number of database corrupt images gathered = 0
       Number of EMM database Media attribute records gathered = 38
       Number of EMM database Volume attribute records gathered = 43

       Catalog data gathering took 189 seconds to complete

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

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

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

4.0  Verifying required catalog components were gathered

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

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

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


       Summary of NBCC EMM Server processing
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+ 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 lidaclvm1                                                       +
+ EMM tape media record extract attempted = yes                            +
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

       Summary of NBCC Media server processing
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+ Primary hostname:                                                        +
+ lidabl14                                                                 +
+ Alias hostnames:                                                         +
+ lidabl14.acme.com                                      +
```

```
+ Sources:                                                                +
+ nbemmcmd bpgetconfig                                                    +
+ Media server = yes                                                      +
+ EMM NetBackup version = 8.1.0.0                                         +
+ NBCC NetBackup version = 8.1                                            +
+ Tape STU detected = no - Disk STU detected = no                         +
+ EMM tape media record extract attempted = yes                           +
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

...

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

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

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

About the NetBackup consistency check repair (NBCCR) utility

The NetBackup consistency check repair (NBCCR) utility is a command line tool that processes database-catalog repair actions. It automates the application of approved suggested repair actions. Cohesity 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, Cohesity technical support interacts with the customer to determine which repairs are needed. Undesirable repair actions are deleted or commented out of the SRA file. Each line of the SRA file contains one repair action that is paired with an associated parameter.

The NBCCR utility executes each repair action in several stages.

Table 3-4 Stages of repair

Stage	Name	Description
Stage 1	Data collection	NBCCR first collects the information that is required to perform a repair.

Table 3-4 Stages of repair *(continued)*

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

NBCCR resides in the following location:

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

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

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

Input file

NBCCR accepts as input the Suggested Repair Action (SRA) file named *primaryname*_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/`*`primaryname`*`_nbccr_`*`timestamp`* On Windows: *`install_path`*`\NetBackup\bin\support\output\nbccr\`*`primaryname`*`_nbccr_`*`timestamp.`* After repair processing is complete, NBCCR relocates the SRA file to the same directory. NBCCR also creates the following output files and places them in the same directory. ■ `NBCCR` creates `NBCCR.History.txt`, which is a history file of all the repair actions attempted. ■ `NBCCR` creates `NBCCR.output.txt`.
Temporary file	While it runs, the `NBCCR` utility uses `KeepOnTruckin.txt`, which appears in the same location as the output files described in this table. To terminate `NBCCR` while it processes repairs, delete this file. This action causes NBCCR to complete the current repair, then shut down. Any other interruption causes undetermined results.

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

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

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

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

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

```
  found on tape
MContents ULT000 status: ActionFailed
```

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

About the nbcplogs utility

When you troubleshoot a problem, you must gather and copy the correct logs to debug the issue. The log types (legacy, vxul, vm, pbx,...) may be in many places. The process of getting the logs to Cohesity 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 Cohesity Evidence Server. For additional assistance, see:

https://support.cohesity.com/s/article/article-100038665

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

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

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

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

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

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

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

About the robotic test utilities

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

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

Robotic tests on UNIX

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

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

- Execute the following command:

  `/usr/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	`/usr/openv/volmgr/bin/acstest -r` *`ACSLS_hostpath`* for `acstest` to work on UNIX and Linux, `acssel` and `acsssi` must be running
TLD	`/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:

  install_path\Volmgr\bin\robtest.exe

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

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

ACS	*install_path*\Volmgr\bin\acstest -r *ACSLS_HOST*
TLD	*install_path*\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.

Usage is:

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

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

About the NetBackup Smart Diagnosis (nbsmartdiag) utility

You can use the NetBackup Smart Diagnosis (nbsmartdiag) utility to detect performance issues, such as high CPU utilization, high memory usage, and deadlocks for the registered NetBackup processes. When nbsmartdiag detects an issue, the appropriate evidence is collected for further troubleshooting, without any user intervention. nbsmartdiag is a service or a daemon that can be deployed on a NetBackup primary server, a media server, or a client.

Note: The nbsmartdiag service is supported only on Windows and Linux (RHEL and SUSE) platforms.

Evidence

Evidence is a set of information which is collected to help troubleshoot the performance of NetBackup.

A single set of evidence collected that contains:

On Windows

- A process dump of the process exhibiting performance issues.
- Memory Performance counters in the form of a CSV file.
- Network Performance counters in the form of a CSV file.
- Disk Performance counters in the form of a CSV file.
- netstat command outputs for network issues.

On Linux

- A process dump of the process exhibiting performance issues.
- vmstat, free, top, etc. command output for memory details.
- gstack, pmap of the process.
- mpstat, iostat command output for Disk I/O details.
- netstat command outputs for network issues.

Evidence examples:

- *Sample of collected evidence on Windows.*

Directory of NBSD_EVIDENCE_PATH\nbsmartdiag\bpdbm\5004\Evidence1

04/08/2021 02:07 AM <DIR> .

04/08/2021 02:07 AM <DIR> ..

04/08/2021 02:08 AM 197,979,709 5004_08-04_02.07.38_Deadlock.dmp

04/08/2021 02:07 AM 4,363 5004_08-04_02.07.38_DiskPerf_Deadlock.csv

04/08/2021 02:07 AM 1,530 5004_08-04_02.07.38_MemeoryPerf_Deadlock.csv

04/08/2021 02:07 AM 5,572 5004_08-04_02.07.38_Netstat_Deadlock.log

04/08/2021 02:07 AM 23,249 5004_08-04_02.07.38_NetworkPerf_Deadlock.csv

5 File(s) 198,014,423 bytes

2 Dir(s) 188,446,031,872 bytes free

- *Sample of collected evidence on Linux:*

Cmd$ ls -l /root/NBTestData/nbsd.evd/nbsmartdiag/vnetd/29696/Evidence1 total 1154144

-rw-r--r-- 1 root root 1180858264 Apr 8 15:25 29696_08-04_15.24.43_CPU.29696

-rw-r--r-- 1 root root 197 Apr 8 15:24 29696_08-04_15.24.43_CPU.DiskPerf_iostat

-rw-r--r-- 1 root root 193 Apr 8 15:24 29696_08-04_15.24.43_CPU.DiskPerf_mpstat

-rw-r--r-- 1 root root 560374 Apr 8 15:24 29696_08-04_15.24.43_CPU.MemoryPerf

-rw-r--r-- 1 root root 185787 Apr 8 15:24 29696_08-04_15.24.43_CPU.Netstat

-rw-r--r-- 1 root root 214191 Apr 8 15:24 29696_08-04_15.24.43_CPU.ProcessData

Important notes about nbsmartdiag

- NetBackup Design does not allow the bpup command to start the nbsmartdiag service.
- Cyrillic characters in the evidence path are not supported.
- You can run nbsmartdiag service under local system account on Windows and under root privileges on Linux.
- Java processes have a common run time name, to monitor NetBackup Admin Console use adminconsole and to NetBackup Web Management Service use nbwmc in the process names.

Workflow to use the nbsmartdiag utility for NetBackup host communication

Carry out the following steps in the given order to configure nbsmartdiag to detect the issues while troubleshooting:

Table 3-5 Workflow to use nbsmartdiag for troubleshooting issues:

Step	Description
Step 1	Ensure the following: ■ Your platform should support the nbsmartdiag service. The following operating systems support nbsmartdiag: ■ Windows ■ RHEL ■ SUSE **Note:** For Windows, you must install the nbsmartdiag service on Windows Server 2012 R2 or latest version. If you try to install the nbsmartdiag service on older version of Windows Server, then the installation fails with a error message. ■ For Linux, the following commands must be present on the system to collect all supporting evidence: ■ gcore ■ gstack ■ iostat ■ mpstat ■ netstat ■ pmap ■ top ■ vmstat For more information about the commands, refer to the *NetBackup Commands and Reference Guide* : https://support.cohesity.com/s/article/article-100040135

Step 2	Install nbsmartdiag `nbsmartdiag -install` on the primary server, media server, or client.
	`nbsmartdiag demo $ /usr/openv/netbackup/bin/nbsmartdiag -install.`
	`Performing the install operation.`
	`Performed the install operation successfully.`

Table 3-5 Workflow to use nbsmartdiag for troubleshooting issues: *(continued)*

Step	Description

Step 3	Start nbsmartdiag service `nbsmartdiag -start`.
	On Windows, the nbsamartdiag service starts from the Service Control Manager.
	`Nbsmartdiag demo $ /usr/openv/netbackup/bin/nbsmartdiag -start Performing the start operation.`
	`Info:Daemon is running.`
	`Performed the start operation successfully.`

Step 4	Collect the evidence from the folder nbsmartdiag at the location which is given in NBSD_EVIDENCE_PATH bp.conf value. ■ For each instance of the process, a subfolder is created inside the process folder. ■ Under the process ID folder, the evidence is collected for each event occurrence. For more information about the bp.configuration options, refer to the *NetBackup Administrator's Guide, Volume I*: https://support.cohesity.com/s/article/article-100040135
Step 5	Stop the nbsmartdiag service once you have finished collecting evidences. Run the following command:`nbsmartdiag -terminate`

Uninstallation of the nbsmartdiag utility

You can uninstall the NetBackup Smart Diagnosis service using following command:

Run `nbsmartdiag -uninstall` to uninstall the service on Windows and the daemon on Linux.

About log collection by job ID

NetBackup includes a command line interface and API option of gathering relevant logs by specifying a job ID, and then uploading the gathered logs. With the specified job ID, logs within the job run time frame are gathered from the primary server, media server, and clients if reachable.

Legacy logs and try file logs may include logs outside of job run time frame as those logs do not honor the time duration filter. Logs from all the hosts that are involved in a job hierarchy are gathered by specifying a job ID of the hierarchy. Cohesity recommends that you use time synchronization for log collection on all hosts that are included in the job time duration. A valid job ID must be present in the Activity monitor. By default, a job ID is removed one week after the job is completed. The `nblogadm` utility cannot gather the logs of a job ID if `bpdbjobs` or the Activity monitor cannot retrieve the job details of the specified job ID. In addition, the logs gathering command line interface and API option do not support **Backup Now** jobs. The VxUL logs are not gathered from a back-level media server or a client.

The gathered logs include NetBackup product and NetBackup support utility (`nbsu`) logs. The log gathering supports one record ID at a time, no concurrent log gathering from multiple record IDs.

To avoid filling up the file system on primary server, media server, and client during log gathering, Cohesity recommends that you use the `KEEP_LOGS_SIZE_GB` option. Cohesity recommends that you specify the size of NetBackup logs that are retained before you gather the logs. See the *NetBackup Administrator's Guide, Volume I* for more information.

A time-based log cleanup process is introduced in NetBackup 10.2. When logs are not removed 7 days after they are gathered, this process removes those gathered logs and the log record. To have a shorter log retention period of 5 days on a primary server or a media server, set the `LOG_RECORD_EXPIRY_DAYS` to `5` with `bpsetconfig`. To have a shorter log retention period of 5 days on a client, set the `LOG_RECORD_EXPIRY_DAYS` to `5` with `nbsetconfig`. The smaller number takes precedence. NetBackup may not remove logs from a back-level media server or a client if it encounters errors during the log cleanup process. Cohesity recommends that you remove the left behind logs manually when you encounter this situation.

To avoid the gathered logs filling up the file system on a primary server, a predefined 10GB free space watermark is used. NetBackup uses this watermark to check and prevent the start of log gathering when the available disk space is less than the sum of watermark and the estimated size of the gathered logs. Additionally, the log gathering process stops when the available space on a primary server falls under the sum of watermark and the estimated size of the gathered logs. In this release, the check of available space is extended to media servers and clients. To reduce the free space watermark to 5GB, set the `HIGH_WATERMARK_TRB_LOG_RECORDS = 5` with `bpsetconfig` command.

You have two options to gather higher verbosity logs. You can manually enable logging and configure the desired logging level as documented in the *NetBackup Logging Reference Guide*. Or you can use the command line interface and API option to gather and to configure the logging level values on a primary server, a media server, or a client. Then restart the job and start a log gathering task. The

feature includes an API option to retrieve the job ID of a new job after the originally specified job is restarted.

Two log record IDs are required to gather higher verbosity logs. The first log record ID (Record ID 1) is used for enabling logging and configuring the desired logging levels to the hosts of a job ID (Job ID 1). After logging levels are configured and the original job (Job ID 1) is restarted, a new job ID (Job ID 2) is generated. The second log record ID (Record ID 2) is used for gathering logs within the new restarted job (Job ID 2) run time frame from the primary server, media server, and clients if reachable. On a backup domain that consists of multiple media servers and clients, the media servers or clients of Record ID 1 and Record ID 2 may not be the same due to the job scheduling algorithms.

In NetBackup 10.2 and later, a SHA256 checksum of each collected log is included in the `Progress.txt` file of the directory shown. The checksum fails to compute on a media server or a client with back-level of NetBackup installed.

Location of the `Progress.txt` file:

- Linux and UNIX
  `/usr/openv/netbackup/logs/nblastaging/record ID-timestamp: YYYYMMDD-HHMMSS`
- Windows
  install_path`\NetBackup\logs\nblastaging\record ID-timestamp: YYYYMMDD-HHMMSS`

NetBackup 10.2 and later includes a space usage enhancement to the required log storage space on a primary server. The log files that are gathered from a primary server, a media server, and a client are no longer stored on the primary server. The files reside with each host in the directory shown.

- Linux and UNIX
  `/usr/openv/netbackup/logs/nblaevidence/nbla-`*hash*
- Windows
  install_path`\NetBackup\logs\nblaevidence\nbla-`*hash*

Supported job types:

- Backup
- Backup from Snapshot
- Snapshot

Supported workload types:

- File System
- Hadoop (logs are only collected from primary and media servers)

- Microsoft Exchange (logs are only collected from primary and media servers)
- Windows Server Failover Cluster (WSFC)
- Microsoft SQL Server Availability Group
- NDMP (logs are only collected from primary and media servers)
- Oracle
- Snapshot Manager (logs are only collected from primary and media servers)
- VMware

When you set the `disableIPResolution` option on a primary server, logs on the protected virtual machines are not gathered when you specify the job ID of the VMware workload type. See https://docs.cohesity.com/docs/netbackup/10.1.1/21902280-158271263-0/v38310204-158271263 for more details of the setting.

Gathering logs from distributed workloads with multiple clients is supported with this release. Examples of distributed workloads include Oracle RAC and MSSQL availability groups.

You can upload the gathered logs to the Cohesity Technical Support organization with the command line interface and the API options as well as a valid support case ID. See https://support.cohesity.com/s/article/article-100038665 for more details.

The password that is provided to the API to upload the logs is stored as a credential object in the **NetBackup credential management** pane. It is removed after logs are uploaded.

A single tar file consisting of gathered logs is uploaded to the Cohesity Technical Support organization's SFTP server or the specified SFTP server. If the Cohesity Technical Support organization does not manage the SFTP server, the upload operation fails if a `tar` file with the same name exists on the SFTP server.

Use the `nblogadm` log to debug or troubleshoot log collection by job ID. Use the `nblogadm` log for both the command line interface and API option. To collect logs from the `nblogadm` process, confirm that the directory that is shown is present:

- Linux and UNIX

  `/usr/openv/netbackup/logs/nblogadm`
- Windows

  `install_path``\NetBackup\logs\nblogadm`

Table 3-6 New command line interface flags introduced to `nblogadm` utility

Command line interface	Description
`nblogadm --action getactivecollections --json`	Get the number of records that are in-progress. (Does not collect logs for more than one record ID at a time)
`nblogadm --action createrecord --jobid job ID --json`	Take a job ID, create an empty log record, and return the created record ID.
`nblogadm --action collectlogsforjob --recid record ID --runnbsu --json`	Create a task to gather the logs for the specified record ID.
`nblogadm --action startupload --recid record ID --sftp_host sftp host --sftp_port sftp port --supportcase support case ID --target_folder sftp host folder --fingerprint sftp host fingerprint, use comma as delimiter without spaces --passcredentials --json`	Create a task to upload the logs for the specified record ID and SFTP server access information.
`nblogadm --action deleterecord --recid record ID --json`	Delete the collected logs and record for the specified record ID. This action also terminates any in-progress task.
`nblogadm --action casedetail --recid record ID --json`	Get the log gather and the log upload task details for the specified record ID.
`nblogadm --action getlogging --recid record ID --json`	Get the list of hosts, their components, and the corresponding logging level values for the specified record ID.
`nblogadm --action getlogging --recid record ID [--hostandlog MASTER|MEDIA|CLIENT:hostname] --json`	When you specify the `--hostandlog` parameter, this command returns the components' logging level values of the specified host for the specified record ID. Without the `--hostandlog` parameter, the command returns the components' logging level values for the list of hosts for the specified record ID.

Table 3-6 New command line interface flags introduced to `nblogadm` utility *(continued)*

Command line interface	Description
`nblogadm --action setlogging --recid record ID --hostandlog MASTER|MEDIA|CLIENT:hostname@legacy component1=legacy component1 level,vxul component1=debug level%diagnostic level,misc type=misc type value --json`	Update the component's logging level settings of the specified host for the specified record ID. Separate calls are required to update each host. The specified legacy and `vxul` component names must be in lower case.

Chapter 4

Disaster recovery

This chapter includes the following topics:

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, Cohesity recommends that you contact technical support.

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

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

The specific procedures that replace failed disks, build partitions and logical volumes, and reinstall operating systems can be complicated and time consuming. Such

procedures are beyond the scope of this manual. Appropriate vendor-specific information should be referenced.

Recommended backup practices

The following backup practices are recommended:

Selecting files to back up	In addition to backing up files on a regular basis, it is important to select the correct files to back up. Include all files with records that are critical to users and the organization. Back up system and application files, so you can quickly and accurately restore a system to normal operation if a disaster occurs. Include all Windows system files in your backups. In addition to the other system software, the Windows system directories include the registry, which is needed to restore the client to its original configuration. If you use a NetBackup exclude list for a client, do not specify any Windows system files in that list. Do not omit executables and other application files. You may want to save tape by excluding these easy-to-reinstall files. However, backing up the entire application ensures that it is restored to its exact configuration. For example, if you have applied software updates and patches, restoring from a backup eliminates the need to reapply them.
Bare Metal Restore	NetBackup Bare Metal Restore (BMR) protects client systems by backing them up with a policy configured for BMR protection. A complete description of BMR backup and recovery procedures is available. See the *NetBackup Bare Metal Restore Administrator's Guide*: https://support.cohesity.com/s/article/article-100040135
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. 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	Cohesity 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*:
	
	https://support.cohesity.com/s/article/article-100040135
	
	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.
Primary and media server backups	The NetBackup catalog backup protects your configuration data and catalog data. Set up backup schedules for the primary servers and media servers in your NetBackup installation. These schedules protect the operating systems, device configurations, and other applications on the servers. Primary 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 primary and media servers should not include NetBackup binaries, configuration or catalog files, or NetBackup database data.

Requirements and notes for disaster recovery

Note the following information and requirements before you perform disaster recovery:

- Cohesity strongly recommends that during NetBackup installation in a disaster recovery mode after a disaster, you use the same primary server name that is available in the disaster recovery email.
- For cluster environments, you must manually deploy certificates on all cluster nodes using a reissue token after you install NetBackup in a disaster recovery mode. Certificates for active and inactive nodes are not recovered during catalog recovery.
  See "Generating a certificate on a clustered primary server after disaster recovery installation" on page 276.
- 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 251.
  - The passphrase for that specific disaster recovery package.

  If the passphrase is lost, refer to the following article to get the host identity back.
  https://support.cohesity.com/s/article/article-100033743

- If a non-privileged user (or service user) account is configured, ensure that the service account has the write access permissions on the directory where the disaster recovery package resides.
  For more information on the service user account, refer to the NetBackup Security and Encryption Guide.
- 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 the Windows certificate store, if they were not backed up during catalog backup.
- Be aware that NetBackup does not support push, remote, or silent installation for the disaster recovery of primary servers. Exception: NetBackup supports these installation methods for hosts in a NetBackup primary 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 (DR) package stores the identity of the primary server host. NetBackup requires this package to get the identity of the primary 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 primary server certificate and the NetBackup certificate authority (CA) certificate
- Information about the hosts in the domain
- Security settings
- External CA-signed certificates
  External CA-signed certificates from Windows certificate store, if applicable
- NetBackup configuration options that are specific to external CA-signed certificates
- Key management service (KMS) configuration

Note: By default, the KMS configuration is not backed up during catalog backup. Set the KMS_CONFIG_IN_CATALOG_BKUP configuration option to 1 to include the KMS configuration as part of the disaster recovery package during catalog backup.

Note: You must set a passphrase for the disaster recovery package for the catalog backups to be successful.

About disaster recovery settings

For increased security, a disaster recovery package is created during each catalog backup.

See "Disaster recovery packages" on page 251.

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 primary 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

Setting	Description
Enter passphrase	Enter the passphrase to encrypt disaster recovery packages. ■ By default, the passphrase must contain a minimum of 8 and a maximum of 1024 characters. You can set the passphrase constraints using the `nbseccmd -setpassphraseconstraints` command option. ■ The existing passphrase and the new passphrase must be different. ■ 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: ~ ! @ # $ % ^ & * ( ) _ + - = ` { } [ ] | : ; ' , . / ? < > "
Confirm passphrase	Re-enter the passphrase for confirmation.

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.
- The passphrase that you provide when you install NetBackup on the primary server in the disaster recovery mode after a disaster must correspond to the disaster recovery package from which you want to recover the primary server host identity.

About disk recovery procedures for UNIX and Linux

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

- Primary server disk recovery procedures
  See "About recovering the primary server disk on Linux" on page 253.
- Media server disk recovery procedures
  See "About recovering the NetBackup media server disk for UNIX" on page 259.
- Client disk recovery procedures
  See "Recovering the system disk on a UNIX client workstation" on page 260.

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 with the NetBackup import feature. See the information on importing NetBackup images in the NetBackup Web UI Administrator's Guide. 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 primary server disk on Linux

The following procedures explain how to recover data if the system disk fails on a Linux NetBackup primary 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 primary server when root is intact" on page 254.
- 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 primary server when the root partition is lost" on page 257.

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

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

See the NetBackup Bare Metal Restore System Administrator's Guide.

Recovering the primary server when root is intact

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

To recover the primary 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.

   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:

   https://support.cohesity.com/s/article/article-100023872

   If you used a custom `nbsvcuser` or `nbwebgrp` you must populate the NetBackup installation answer file with the custom names before you begin the installation. Refer to the *NetBackup Installation Guide* for additional details. See the **web services** requirement in the **NetBackup requirements for UNIX and Linux** table. This table is located in the **Installation requirements for UNIX and Linux** section.

   Note: You must use the same service user account that was used when you backed up the NetBackup catalog.

   For more information on the service user account, refer to the NetBackup Security and Encryption Guide.

   ---

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

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

   ---

4. If the catalog directories differ from those in the NetBackup catalog backups, recreate that directory structure on the disk before you recover the catalog. For example, if you used symbolic links as part of the NetBackup catalog directory structure.
5. If the recovery scenario involves restoring policy or catalog backups, the appropriate recovery devices 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.
- Discover and configure the recovery device in NetBackup.
  See the NetBackup Administrator's Guide, Volume I.
- Use the NetBackup `tpautoconf` command to discover and configure the recovery device in NetBackup.
  See the NetBackup Commands Reference Guide.
- Update the device mapping files.
  See the NetBackup Administrator's Guide, Volume I.

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

See the NetBackup Administrator's Guide, Volume I.

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

- Manually load the required media into a 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.
- Inventory the media contents of a robotic device.
- Use the vendor-specific robotic control software to load the media into the required recovery devices.

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 "Options to recover the NetBackup catalog" on page 286.

8 Stop and restart all NetBackup daemons.

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

9 Restore other files to the server as desired.

You can use the NetBackup web UI, the NetBackup Backup, Archive, and Restore interface, or the bp command. When the files are restored, you are done.

Recovering the primary 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 can then 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 primary 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 the components resided on the original disk. These components include NetBackup, its catalogs (if applicable), and the databases. 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:

   https://support.cohesity.com/s/article/article-100023872

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 the disk before you recover the catalog. For example, if you used symbolic links as part of the NetBackup catalog directory structure.
7. If the recovery scenario involves restoring policy or catalog backups, the appropriate recovery devices 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.
- Discover and configure the recovery device in NetBackup.
  See the NetBackup Administrator's Guide, Volume I.
- Use the NetBackup `tpautoconf` command to discover and configure the recovery device in NetBackup.
  See the NetBackup Commands Reference Guide.
- Update the device mapping files.
  See the NetBackup Administrator's Guide, Volume I.

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

See the NetBackup Administrator's Guide, Volume I.

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

- Manually load the required media into a 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.
- Inventory the media contents of a robotic device.
- Use the vendor-specific robotic control software to load the media into the required recovery devices.

9 Recover the NetBackup catalogs to the alternate disk.

See “Options to recover the NetBackup catalog” on page 286.

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

10 Restore other files to the server as desired.

You can use the NetBackup web UI, the NetBackup Backup, Archive, and Restore interface, or the bp command. When the files are restored, you are done.

Restore these files from the backup of the primary 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.

```
/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 database directories from the alternate disk. Or, unhook that disk, if it is a spare.

About recovering the NetBackup media server disk for UNIX

NetBackup media servers store information in the NetBackup 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 260.

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*:

https://support.cohesity.com/s/article/article-100040135

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

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

Table 4-2 Cluster failure and recovery scenarios

Scenario	Procedure
Node failure	See "Replacing a failed node on a UNIX or Linux cluster" on page 261.
Shared disk failure	See "Recovering the entire UNIX or Linux cluster" on page 262.
Cluster failure	See "Recovering the entire UNIX or Linux cluster" on page 262.

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*:

https://support.cohesity.com/s/article/article-100040135

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*:

   https://support.cohesity.com/s/article/article-100040135

   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:

   https://support.cohesity.com/s/article/article-100023872

   ---

7. Install any Maintenance Packs and patches that are required to bring the newly installed node to the same patch level as the other cluster nodes.
8. Bring the NetBackup Resource group online on a node other than the freshly installed node.

9 Log onto the node on which the NetBackup resource group is online and run the following command:

```
/usr/openv/netbackup/bin/cluster/cluster_config -s nbu -o
add_node -n node_name
```

node_name is the name of the freshly installed node.

10 Switch the NetBackup resource group to the replacement node.

11 Freeze the NetBackup group.

12 Ensure that the appropriate low-level tape device and robotic control device configuration necessary for your operating system has been performed. Information is available for your operating system.

Refer to the *NetBackup Device Configuration Guide*:

https://support.cohesity.com/s/article/article-100040135

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*:

https://support.cohesity.com/s/article/article-100040135

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*:

https://support.cohesity.com/s/article/article-100040135

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*:

   https://support.cohesity.com/s/article/article-100040135
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*:

   https://support.cohesity.com/s/article/article-100040135

   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:

   https://support.cohesity.com/s/article/article-100023872
4. Configure the clustered NetBackup server.

   Refer to the *NetBackup High Availability Guide*:

   https://support.cohesity.com/s/article/article-100040135
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 primary server when root is intact" on page 254.
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*:

   https://support.cohesity.com/s/article/article-100040135

About disk recovery procedures for Windows

The three different types of disk recovery for Windows are as follows:

- Primary server disk recovery procedures
  See "About recovering the primary server disk for Windows" on page 264.
- Media server disk recovery procedures
  See "About recovering the NetBackup media server disk for Windows" on page 270.
- Client disk recovery procedures
  See "Recovering a Windows client disk" on page 270.

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*:

https://support.cohesity.com/s/article/article-100040135

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 primary 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 primary 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 primary server with Windows intact" on page 265.
- All disk partitions are lost. Windows must be reinstalled, which is a total recovery. These procedures assume that the NetBackup primary disk was running a supported version of Windows and that the defective hardware has been replaced.
  See "Recovering the primary server and Windows" on page 267.

For NetBackup primary 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 primary server with Windows intact

This procedure shows how to recover the NetBackup primary server with the Windows operating system intact.

To recover the primary 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.

   See the NetBackup Installation Guide.

   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:

   https://support.cohesity.com/s/article/article-100023872

   ---

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 the disk before you recover the 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.
   - Discover and configure the recovery device in NetBackup.
     See the NetBackup Administrator's Guide, Volume I.
   - Use the NetBackup `tpautoconf` command to discover and configure the recovery device in NetBackup.
     See the NetBackup Commands Reference Guide.

- Update the device mapping files.
  See the NetBackup Administrator's Guide, Volume I.

8 If the recovery scenario involves restoring the policy backups or catalog backups that were done to media, the appropriate recovery devices 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.
  - Inventory the media contents of a robotic device.
  - Use the vendor-specific robotic control software to load the media into the required recovery devices.

9 Recover the NetBackup catalogs.

  See "Options to recover the NetBackup catalog" on page 286.

10 When catalog recovery is complete, stop and restart the NetBackup services. Use the following `bpdown` and `bpup` commands 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 following directories:

```
install_path\NetBackup\db install_path\NetBackupDB
install_path\NetBackup\varinstall_path\Volmgr\database
```

These directories were recovered in step 9 and overwriting them with regular backups leaves the catalogs in an inconsistent state. If the databases were relocated using `nbdb_move` from *install_path*`\NetBackupDB\data`, they are recovered in step 10 and should not be restored in step 12.

If the NetBackup databases 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:

  - Open the NetBackup web UI on the primary server.
  - Click **Recovery**. Then click **Regular recovery**. Select the appropriate policy type.

- 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 following directories:
  install_path\NetBackup\db *install_path*\NetBackupDB (or relocated NetBackup database path)
  install_path\NetBackup\var
  install_path\Volmgr\database
  See the previous warning 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.

12 Restart the system, which replaces any files that were busy during the restore. When the restart process is complete, the system is restored to the state it was in at the time of the last backup.

Recovering the primary server and Windows

This procedure assumes that all disk partitions in Windows are lost.

To recover the primary 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 the 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\Cohesity NetBackup` 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:

   https://support.cohesity.com/s/article/article-100023872

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 the disk before you recover the 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.
   - Discover and configure the recovery device in NetBackup.
     See the NetBackup Web UI Administrator's Guide, Volume I.
   - Use the NetBackup command `tpautoconf` to discover and configure the recovery device in NetBackup.
     See the NetBackup Commands Reference Guide.
   - Update the device mapping files.
     See the NetBackup Web UI Administrator's Guide, Volume I
9. If you must restore from the policy backups or catalog backups that were done to media, the appropriate media may have to be configured in NetBackup.

   See the NetBackup Administrator’s Guide, Volume I.

   When you configure the media, you may have to do some or all of the following:

- Manually load the required media into a standalone recovery device.
- Use the NetBackup utilities such as `robtest` or vendor-specific robotic control software to load media into the required recovery devices.
- 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. How you recover the catalog depends on which part or parts of the catalog you want to recover.

See "Options to recover the NetBackup catalog" on page 286.

11 When the catalog recovery is complete, stop and restart the NetBackup services. Use the following `bpdown` and `bpup` commands, the **Activity monitor**, 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 following directories:

install_path\NetBackup\db
install_path\NetBackup\var
install_path\NetBackupDB
install_path\Volmgr\database

These directories were recovered in step 10 and overwriting them with regular backups leaves the catalogs in an inconsistent state. If the databases 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:

- Open the NetBackup web UI on the primary 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 following directories:
  install_path\NetBackup\db *install_path*\NetBackupDB (or relocated NetBackup database path)
  install_path\NetBackup\var
  install_path\Volmgr\database
  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 restart 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 database. If you need to recover the system disk on a NetBackup media server, the recommended procedure is similar to disk recovery for the client.

See "Recovering a Windows client disk" on page 270.

Recovering a Windows client disk

The following procedure explains how to perform a total recovery of a Windows NetBackup client in the event of a system disk failure.

NetBackup Bare Metal Restore (BMR) protects client systems by backing them up with a policy configured for BMR protection. A complete description of BMR backup and recovery procedures is available.

See the Bare Metal Restore System Administrator's Guide/

This procedure assumes that the Windows operating system and NetBackup are reinstalled to boot the system and perform a restore.

The following are additional assumptions:

- The NetBackup client was running a supported Microsoft Windows version.
- The NetBackup client was backed up with a supported version of NetBackup client and server software.
- The NetBackup primary 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 primary 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 primary 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 primary 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 primary 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.

See the NetBackup Installation Guide.

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 web UI or 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.

NetBackup restores the registry when it restores the Windows system 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*:

https://support.cohesity.com/s/article/article-100040135

Warning: Contact technical support before you try these recovery procedures.

Replacing a failed node on a Windows VCS cluster

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

Refer to topics about configuring NetBackup in the *NetBackup High Availability Guide*:

https://support.cohesity.com/s/article/article-100040135

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*:

   https://support.cohesity.com/s/article/article-100040135

   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:

   https://support.cohesity.com/s/article/article-100023872

4 Ensure that the node is a member of an existing cluster and that it performs the necessary configuration automatically.

5 Install any Maintenance Packs and patches that are required to bring the newly installed node to the same patch level as the other cluster nodes.

6 Unfreeze the NetBackup service and verify that it can be brought up on the replacement node.

Recovering the shared disk on a Windows VCS cluster

The following procedure is applicable in situations where the configured cluster nodes remain available but the NetBackup catalog, database files, or both on the shared disk have been corrupted or lost.

Check the following conditions before you proceed with this procedure:

- The shared storage hardware is restored to a working state, so that the shared disk resource can be brought online with an empty shared directory.
- Valid online catalog backups exist.

To recover the shared disk on a Windows cluster that uses VCS

1 Clear the faulted NetBackup resource group, disable monitoring, and bring up the shared disk and virtual name resources on a functioning node.

2 Ensure that all NetBackup shared disks are assigned the same drive letters that were used when NetBackup was originally installed and configured.

3 To reconfigure NetBackup for the cluster, initialize the database by running the following commands in sequence on the active node:

```
bpclusterutil -ci
tpext
bpclusterutil -online
```

4 Use the appropriate NetBackup catalog recovery procedure to restore the NetBackup catalog information on the shared disk.

See "Recovering the primary server and Windows" on page 267.

5 If the clustered NetBackup server is a media server, verify that the restored vm.conf file contains the correct host-specific MM_SERVER_NAME configuration entry for the active node. If MM_SERVER_NAME is different from the local host name, edit the file and change the server name to the local host name:

MM_SERVER_NAME=<local host name>

6 Use NetBackup to restore any data on the shared disks.

7 Configure required devices and media and recover the NetBackup catalogs.

8 Manually shut down and restart NetBackup on the active node.

9 Re-enable monitoring of the NetBackup resource group.

10 Verify that the NetBackup server can now be brought online on all configured nodes.

Recovering the entire Windows VCS cluster

The following procedure applies to the clustered NetBackup server environment that must be re-created from scratch.

Before you proceed, ensure that you have valid online catalog backups.

To recover the entire Windows VCS cluster

1 Configure the hardware, system software, and cluster environment on the replacement cluster.

2 Ensure that the appropriate low-level tape device and robotic control device configuration necessary for your operating system has been performed.

Refer to the *NetBackup Device Configuration Guide*:

https://support.cohesity.com/s/article/article-100040135

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*:

https://support.cohesity.com/s/article/article-100040135

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:

https://support.cohesity.com/s/article/article-100023872

---

4 Configure the clustered NetBackup server.

Refer to the *NetBackup High Availability Guide*:

https://support.cohesity.com/s/article/article-100040135

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 primary server and Windows" on page 267.

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*:

https://support.cohesity.com/s/article/article-100040135

Generating a certificate on a clustered primary server after disaster recovery installation

After you complete the disaster recovery of a clustered primary server, you must generate a certificate on the active node as well as all inactive nodes. Additionally, failover to the secondary node is expected behavior in a cluster environment. This procedure is required for successful backups and restores of the cluster.

For additional information on deploying certificates on primary server nodes see the NetBackup Security and Encryption Guide.

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. Consult with your operating system cluster instructions for assistance with this process.

More information about supported cluster technologies is available. See the NetBackup Clustered Primary 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`*`\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
```

About the DR_PKG_MARKER_FILE environment variable

If an external CA was configured on the primary server before a disaster and the DR installation is not successful, you can configure the DR installation to wait to restart the services after it recovers the DR package. This window provides the opportunity to correct or reconfigure the external CA configuration settings.

For more information on external CA-signed certificates, refer to the NetBackup Security and Encryption Guide.

Note: Only use this marker file if you encounter DR installation failures.

To configure the DR_PKG_MARKER_FILE environment variable to hold the installation process

1 Set an environment variable with the name `DR_PKG_MARKER_FILE` with a touch file.

2 Start the DR installation.

Towards the end of the DR installation, NetBackup finds the touch file present on the file system and waits before it starts the NetBackup services.

3 Change the external CA configuration settings.

4 After you complete the changes, delete the touch file that contains the `DR_PKG_MARKER_FILE` environment variable.

5 The Installer resumes the installation process.

Restoring the disaster recovery package on Windows

After a disaster, you need to restore the disaster recovery package that corresponds to the catalog backup that you want to restore. This package is created during the catalog backup and contains the NetBackup primary server host identity.

Important notes

Note the following about restoring the disaster recovery package and catalog recovery:

- To restore the disaster recovery package, you must install NetBackup in the disaster recovery mode and import the required package. After you recover the disaster recovery package, you can recover the catalog.
- After you restore the disaster recovery package, you must immediately perform catalog recovery.
- Note the following when you want to recover a clustered primary server:
  - 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 must redeploy or reconfigure NetBackup or external certificates after the DR installation.
- 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 340.

Prerequisites

If any 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 the Windows certificate store, if applicable.
- In some cases when an external certificate was configured on the primary server before the disaster, the DR installation fails. You can set an environment variable that lets you correct the external certificate configuration.
  See "About the DR_PKG_MARKER_FILE environment variable" on page 277.

Options for restoring the disaster recovery package on Windows

You can restore the disaster recovery package of the NetBackup primary server either during installation or after installation.

See the section called "Restore the disaster recovery package during NetBackup installation on Windows" on page 279.

See the section called "Restore the disaster recovery package after NetBackup installation on Windows" on page 281.

Restore the disaster recovery package during NetBackup installation on Windows

The following procedure describes how to restore the disaster recovery package during the installation of NetBackup.

To restore the disaster recovery package of the NetBackup Appliance, you must follow a different procedure.

See the section called "Restore the disaster recovery package after NetBackup installation on Windows" on page 281.

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 in 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 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:

https://support.cohesity.com/s/article/article-100033743

---

5 (Conditional) Note the following if any external CA-signed certificates were used in your NetBackup domain at the time of the 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 the 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 that is specified for this option. Copy the valid CRLs in the directory that you specify for `ECA_CRL_PATH`.
- Note the following if you used a Windows certificate store to store the external CA-signed certificates and they were not backed up in the DR package. A warning indicates that you must configure the external CA-signed certificates. Configure the following external certificate configuration options on the primary server according to the valued that are 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 external certificate configuration options, refer to the NetBackup Administrator's Guide, Volume I.

- (Conditional) If the DR_PKG_MARKER_FILE environment variable was set before the DR installation, a message indicates that the touch file exists. After you complete the external certificate configuration, delete the touch file.
  NetBackup services are started.

6 (Conditional) If the key management service (KMS) was configured on the primary server before the disaster, run the following command to start the KMS service:

```
Install_path\bin\nbkmscmd -discoverNBKMS
```

7 Refer to the Installing server software on Windows systems section from the NetBackup Installation Guide.

Restore the disaster recovery package after NetBackup installation on Windows

The following procedure describes how to restore the disaster recovery package after the installation of NetBackup.

Use this option to restore the disaster recovery package of the NetBackup Appliance.

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 allowed list cache and restart the NetBackup services on all hosts in the domain.

3 Refresh the certificate revocation list (CRL) using the following command:

```
nbcertcmd -getcrl
```

4 If the key management service (KMS) was configured on the primary server before the disaster, run the following command to start the KMS service:

```
Install_path\bin\nbkmscmd -discoverNBKMS
```

5 Carry out the given 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.

Remove the NetBackup certificate files using the following command:

```
configureWebServerCerts -removeNBCert
```

Restoring the disaster recovery package on Linux

After a disaster, you need to restore the disaster recovery package that corresponds to the catalog backup that you want to restore. This package is created during the catalog backup and contains the NetBackup primary server host identity. You must restore the host identity before you can perform a catalog recovery.

Important notes

Note the following about restoring the disaster recovery package and catalog recovery:

- 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. After you recover the disaster recovery package, you can recover the catalog.
- After you restore the disaster recovery package, you must immediately perform catalog recovery.
- Note the following when you want to recover a clustered primary server:
  - 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 must redeploy or reconfigure NetBackup or external certificates after the DR installation.
- 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 340.

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.
- Note the following if you used a Windows certificate store as a certificate store before the disaster and the certificate files were not backed up during catalog backup. You must manually configure the external certificate for the host after the disaster. Refer to the following article:
  https://support.cohesity.com/s/article/article-100044249
- 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.
- In some cases when an external certificate was configured on the primary server before the disaster, the DR installation fails. You can set an environment variable that lets you correct the external certificate configuration.
  See “About the DR_PKG_MARKER_FILE environment variable” on page 277.

Options for restoring the disaster recovery package on Linux

You can restore the disaster recovery package of the NetBackup primary server either during installation or after installation.

See the section called “Restore the disaster recovery package during NetBackup installation on Linux” on page 283.

See the section called “Restore the disaster recovery package after NetBackup installation on Linux” on page 285.

Restore the disaster recovery package during NetBackup installation on Linux

The following procedure describes how to restore the disaster recovery package during the installation of NetBackup.

To restore the disaster recovery package of the NetBackup Appliance, you must follow a different procedure.

See the section called “Restore the disaster recovery package after NetBackup installation on Linux” on page 285.

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 in 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 you are prompted, 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:

   https://support.cohesity.com/s/article/article-100033743

   ```
   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. (Conditional) 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 the 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 that is specified for this option. Copy the valid CRLs in the directory that you specify for ECA_CRL_PATH.
- (Conditional) If the DR_PKG_MARKER_FILE environment variable was set before the DR installation, a message indicates that the touch file exists. After you complete the external certificate configuration, delete the touch file.
  NetBackup services are started.

7 (Conditional) If the key management service (KMS) was configured on the primary server before the disaster, run the following command to start the KMS service:

```
/usr/openv/netbackup/bin/nbkmscmd -discoverNBKMS
```

8 Refer to the “Installing server software on UNIX systems” section in the NetBackup Installation Guide.

Restore the disaster recovery package after NetBackup installation on Linux

The following procedure describes how to restore the disaster recovery package after the installation of NetBackup.

Use this option to restore the disaster recovery package of the NetBackup Appliance.

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 allowed list cache and restart the NetBackup services on all hosts in the domain.

3. Refresh the certificate revocation list (CRL) using the following command:

   ```
   nbcertcmd -getcrl
   ```

4. If the key management service (KMS) was configured on the primary server before the disaster, run the following command to start the KMS service:

   ```
   /usr/openv/netbackup/bin/nbkmscmd -discoverNBKMS
   ```

5. Carry out the given 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.

   Remove the NetBackup certificate files using the following command:

   ```
   configureWebServerCerts -removeNBCert
   ```

Options to recover the NetBackup catalog

How you recover the catalog depends on which part or parts of the catalog you want to recover, as follows:

Table 4-3 Catalog recovery options

Recovery option	Description
Recover the entire catalog	Cohesity 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 295.
Recover the catalog image files and configuration files	The image database contains information about the data that has been backed up. This type of recovery also restores the data and the metadata for the NetBackup databases (BMRDB, NBAZDB, and NBDB) so that it is available for further recovery processing. See "About recovering the NetBackup catalog image files" on page 306.

Table 4-3 Catalog recovery options *(continued)*

Recovery option	Description
Recover the NetBackup databases	NetBackup stores information in the NetBackup database (NBDB). The metadata includes information about the data that has been backed up, and about where the data is stored. Recover the NetBackup database if it is corrupt or lost but the catalog image files exist and are valid. See "About recovering the NetBackup databases" on page 320.

The parts of the NetBackup catalog are described in the NetBackup Web UI Administrator's Guide.

Other procedures exist for special use cases.

See "Recovering the NetBackup catalog when NetBackup Access Control is configured" on page 331.

Prerequisites for recovering the NetBackup catalog or NetBackup catalog image files

Caution: NetBackup Catalog Recovery is a critical process. During the catalog recovery process, you must not perform any other operation using the NetBackup web UI or the **NetBackup Administration Console**. The NetBackup database and all the services will be down during the process.

Caution: Do not run any client backups before you recover the NetBackup catalog or catalog image files.

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 340.

Before you recover the NetBackup catalog or NetBackup catalog image files, review the following requirements and information:

- Ensure that NetBackup is running in the recovery environment.
- Configure the recovery devices in NetBackup.

- Ensure that the media on which the catalog backups exist are available to NetBackup.
- If the NetBackup primary server is part of a cluster, ensure that the cluster is functional.
- You must be logged on to the primary server from which you want to recover the catalog.
- 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.
- To recover the catalog from the web UI, you must have the Administrator role or similar permissions. To use the `bprecover` command, you must have root (administrative) privileges.
- 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 288.
- Ensure that you have the location of the disaster recovery file.
  Recovery of the entire catalog or the catalog image files relies on the disaster recovery information. This file contains the NetBackup primary server host identity. The location of the disaster recovery file is configured in the catalog backup policy and is saved in a file during the catalog backup.
  See "NetBackup disaster recovery email example" on page 290.
  If you do not have the disaster recovery file, you can still 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 333.

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 primary server to establish a connection with the NAT media server before catalog recovery.

To establish a connection with the NAT media server

1. Run the `configureMQ` command on the primary server.
2. Use the `nbsetconfig` command to set the following configuration options on the primary 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 primary server.
4. Ensure whether a reverse connection between the primary server and the NAT media server is established using the `bptestbpcd` command.

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 primary server installation is new. A primary 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 primary server	To recover the NetBackup catalog from a clustered primary server to a single primary 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.

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.

The following is an example of a disaster recovery email after a successful catalog backup:

```
From:          NetBackup@example.com
Sent:          Tuesday, June 13, 2023 04:42
To:            NetBackup Administrator
Subject:       NetBackup Catalog Backup successful on host
```

```
               primary.example.com status 0
Attachments:   cat_1686692545_FULL.drpkg

Server
 primary.example.com

NetBackup Version
 10.3

Date
 6/13/2023 04:42:20 PM

Policy
 cat

Catalog Backup Status
 the requested operation was successfully completed (status 0).


DR image file: /usr/openv/cat_1686692545_FULL

To ensure that the NetBackup catalog data is protected through
Tue 13 Jun 2023 04:42:20 PM CDT, retain a copy of each attached file, and
the media or files listed below:

Catalog Recovery Media
 Media Server                Disk Image Path  Image File Required
 * media-server.example.com  @aaaab           cat_1686692540_FULL
 * media-server.example.com  @aaaab           cat_1686692545_FULL
 * media-server.example.com  @aaaab           cat_1686692545_FULL

DR file written to
 /usr/openv/cat_1686692545_FULL

DR Package file written to
 /usr/openv/cat_1686692545_FULL.drpkg

The CA configuration at the time of catalog backup is as follows:


The primary server primary.example.com is configured to use NetBackup certificates.

 ECA_CRL_PATH_SYNC_HOURS = 1
```

```
 ECA_CRL_REFRESH_HOURS = 24
 ECA_CRL_CHECK = LEAF



The primary server is configured to use service account: root

The primary server is configured to run with FIPS mode set to: DISABLE


* - 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 web UI or the nbseccmd command.
- If the catalog backup is encrypted using keys from an External KMS, configure
  the External KMS in NetBackup after the installation completes and before
  starting recovery. See the NetBackup Security and Encryption Guide for
  information on how to configure an external KMS.
  https://support.cohesity.com/s/article/article-100040135
- If this catalog backup is encrypted using a keys from the NetBackup KMS,
  configure the NetBackup KMS and restore the required keys after the installation
  completes and before starting recovery. See the NetBackup Security and
```

```
  Encryption Guide for information on how to backup and restore keys from the
  NetBackup KMS. https://support.cohesity.com/s/article/article-100040135

 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 "Are you currently
         performing a disaster recovery of a primary server? [y,n] (y)".
         Select "y"
      ii. On the Windows installer click the "Disaster Recovery Primary
         Server" button.
    b. The installation procedure prompts you for the primary server's DR
       Package
       (refer to the /usr/openv/cat_1686692545_FULL.drpkg mentioned earlier).
       Make sure that the primary server can access the attached DR package
       file.
    c. Type the passphrase associated with the DR Package,
       when prompted.
      i. The installer validates the DR package using the passphrase.
      ii. In case of errors in validation, the installer aborts the
          operation. To work around the issue, refer to the following
          article: https://support.cohesity.com/s/article/article-100033743
      iii. If the external CA-signed certificates could not be backed up,
           configure the certificates on the host.
           Refer to the following article:
           https://support.cohesity.com/s/article/article-100044249
 2. Configure the devices necessary to read the media listed above.
 3. Inventory the media.
 4. Make sure that the primary server can access the attached DR image file.
 5. Start the NetBackup Recovery Wizard from the NetBackup web UI.  Or, start
    the wizard from a command line by entering bprecover -wizard.

Disaster Recovery Procedure without the DR Image File
NOTE: ONLY ATTEMPT THIS AS A LAST RESORT
If you do not have the attachment included with this email, use the following
instructions to recover your catalog. (If using OpenStorage disk pools, refer
to the Shared Storage Guide to configure the disk pools instead of step 2 and
3 below ):

 1. Install NetBackup.
 2. Run:
    Configure certificates for the media server that is associated with this
    catalog recovery by running the below commands on that host:
```

```
      nbcertcmd -getCACertificate
      nbcertcmd -getCertificate -force
3.  Configure the devices necessary to read the media listed above.
4.  Inventory the media.
5.  Run
     To recover from copy 1:
     bpimport -create_db_info [-server name] -id /
6.  Run:
    cat_export -client client1.example.com
7.  Go to the following directory to find the DR image file
    cat_backup_1686692545_FULL:
    /usr/openv/netbackup/db.export/images/primary.example.com/1686000000
8.  Open cat_backup_1686692545_FULL file and find the BACKUP_ID
    (for example: primary.example.com_1686692545).
9.  Run:
    bpimport [-server name] -backupid primary.example.com_1686692545
10.  Run:
    bprestore -T -w [-L progress_log] -C primary.example.com -t 35
    -p cat_backup -X -s 1686692545 -e 1686692545 /
11. Run the NetBackup web UI to restore the remaining image database
    if the DR image is a result of an incremental backup.
12. To recover the NetBackup relational database, run:
    bprecover -r -nbdb
13. Stop and start NetBackup.
14. Run:
    Re-configure the certificates on the primary server and the media server,
    because the database is restored to a previous point in time.
        Run the following set of commands on the primary server:
            nbcertcmd -getCACertificate -force
            nbcertcmd -createToken -reissue -host <primary/media>
            name <>
            nbcertcmd -getCertificate -token <> -force
        Run the following set of commands on the media server that is
        associated with this catalog recovery:
            nbcertcmd -getCACertificate -force
            nbcertcmd -getCertificate -force
15. Configure the devices if any device has changed since the last
    backup.
16. To make sure the volume information is updated, inventory the
    media to update the NetBackup database.
```

About recovering the entire NetBackup catalog

Cohesity recommends that you recover the entire catalog. Doing so helps ensure consistency among the various parts of the catalog.

Recovery includes the catalog image files and configuration files that are in the catalog backups that are identified by the disaster recovery file, as follows:

Full backup	The NetBackup database that is identified by the DR file is restored. The images and configuration files that are identified by the disaster recovery file are restored.
Incremental backup	The NetBackup database that is identified by the DR file is restored. All catalog backup image files back to the last full catalog backup are automatically included in an incremental catalog backup. You can then use the NetBackup web UI or the Backup, Archive, and Restore user interface to restore all backup images.

You can use either of the following methods to recover the entire catalog:

- The **NetBackup catalog recovery** wizard.
  See "Recovering the entire NetBackup catalog using the NetBackup catalog recovery wizard" on page 295.
- The text-based wizard launched by the `bprecover -wizard` command and option.
  See "Recovering the entire NetBackup catalog using bprecover -wizard" on page 300.

Recovering the entire NetBackup catalog using the NetBackup catalog recovery wizard

This procedure describes how to recover the entire catalog using the **NetBackup catalog recovery** wizard.

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, Cohesity recommends that you recover only the NetBackup image files.

See "About recovering the NetBackup catalog image files" on page 306.

Warning: Do not run any client backups before you recover the NetBackup catalog.

To recover the entire catalog by using the NetBackup catalog recovery wizard

1. Review the prerequisites before starting the catalog recovery.

   See "Prerequisites for recovering the NetBackup catalog or NetBackup catalog image files" on page 287.

2. If NetBackup is not running, start all of the NetBackup services by entering the following:

   - On UNIX and Linux:

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

   - On Windows:

     install_path\NetBackup\bin\bpup

3. Sign into the primary server on which you want to recovery the catalog. You must have the Administrator role or similar permissions.

4. Start the NetBackup web UI.

5. If the catalog backup and the recovery devices are not available, do the following:

   - 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:
     https://support.cohesity.com/s/article/article-100040135

   - If the catalog backup was written to an immutable (MSDP WORM) storage server, add the storage server back to the primary server's configuration with the `nbdevconfig` command.
     For more information on recovering the NetBackup catalog from an MSDP pool, see the article.

   - Make the media that contains the catalog backup available to NetBackup: 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.

6. At the top, click **Settings > NetBackup catalog recovery**.

7 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. The disaster recovery file must be available on the local computer from where you opened the web UI.

In most cases, you specify the most recent disaster recovery information file available. If the most recent catalog backup is an incremental backup, use the disaster recovery file from the incremental backup. (There is no need to first restore the full backup and then follow with the incremental backup.)

If some form of corruption has occurred, you may want to restore to an earlier state of the catalog.

Click **Next** to continue.

8 NetBackup searches for the media that are required to recover the catalog. It then informs you of the progress and locates the necessary backup ID of the disaster recovery image. If the media is not located, NetBackup indicates which media is needed to update the database.

If necessary, follow the instructions to insert the media that is indicated and run an inventory to update the NetBackup database. The information that displays depends on whether the recovery is from a full backup or an incremental backup.

When all the required media sources are found, click **Next**.

9 By default, the **Recover entire NetBackup catalog** option is selected.

Select a **Job priority** if wanted and then click **Next** to initiate the recovery. You can click **Cancel** to stop the NetBackup catalog recovery process.

10 NetBackup displays the progress of the recovery of the various catalog components:

- 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.

11 After the recovery completes, click **Finish**.

12 **Important:** After successful catalog recovery, you must set the disaster recovery package passphrase. The passphrase is not recovered during the catalog recovery.

Do one of the following to set the passphrase:

- At the top, click **Settings > Global security**. On **Disaster recovery** tab specify the passphrase.
- Use the `nbseccmd -drpkgpassphrase` command to specify the passphrase.

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 340.
- Before you restart NetBackup, 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, you must freeze the media that contains the backups more recent than the date of the catalog from which you recovered. Otherwise, NetBackup may overwrite that media.

14 Clean up the allowed list cache on all hosts.

15 Stop and restart NetBackup services on the primary 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 web UI is active on any of the hosts, the command that stops the NetBackup services shuts it down.

16 After the services are restarted, run one of the following commands:

- 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 340.
  Proceed with the next step.

17 If the catalog recovery is part of a server recovery procedure, complete the remaining steps in the appropriate recovery procedure.

Recovery can include the following:

- Importing the backups from the backup media into the catalog.
- Write protecting the media.
- Ejecting the media and setting it aside.
- Freezing the media.

Note: A catalog recovery changes the configuration of NetBackup back to the point in time of the catalog backup. Any change to the configuration after the point-in-time of the catalog backup (For example: changes to policies, clients, storage units) must be re-applied if those changes are desired. These changes should be re-applied before new backups are taken. If the changes are not applied, they can affect what is protected and how the protection is managed.

As an example, a storage unit might have been modified to require the use of WORM locking on new images. If WORM locking isn't re-applied, new backups do not have the desired WORM protections.

Recovering the entire NetBackup catalog using bprecover -wizard

The `bprecover -wizard` command is an alternative to using the NetBackup catalog recovery wizard.

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, Cohesity recommends that you recover only the NetBackup image files.

See "About recovering the NetBackup catalog image files" on page 306.

Warning: Do not run any client backups before you recover the NetBackup catalog.

To recover the entire catalog by using the bprecover -wizard

1. Review the prerequisites before starting the catalog recovery.

   See "Prerequisites for recovering the NetBackup catalog or NetBackup catalog image files" on page 287.

2. 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.

3 Start NetBackup using the following commands.

- UNIX and Linux:

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

- Windows:

  install_path`\NetBackup\bin\bpup.exe`

4 If the catalog backup and the recovery devices are not available, do the following:

a Configure the necessary recovery device in NetBackup.

b If the catalog backup was written to an immutable (MSDP WORM) storage server, add the storage server back to the primary server's configuration with the CLI `nbdevconfig` command. See the NetBackup Commands Reference Guide for more information about the command.

c 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:

https://support.cohesity.com/s/article/article-100040135

5 Start the `bprecover` wizard by entering the following command:

- UNIX and Linux:

  `/usr/openv/netBbckup/bin/admincmd/bprecover -wizard`

- Windows:

  install_path`\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)
```

6 Enter **Y** to continue. The following prompt appears:

```
Please specify the full pathname to the catalog disaster recovery
file:
```

7 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.

8 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 databases (NBDB, NBAZDB, and optionally BMRDB) are restored and recovered.

9 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
```

When the recovery job is finished, each image file is restored to the proper image directory, and the NetBackup databases (NBDB, NBAZDB, and optionally BMRDB) have been restored and recovered.

10 **Important:** After successful catalog recovery, you must set the disaster recovery package passphrase, because the passphrase is not recovered during the catalog recovery.

Do one of the following to set the passphrase:

- Open the web UI. At the top, click **Settings > Global security**. On **Disaster recovery** tab specify the passphrase.
- Use the `nbseccmd -drpkgpassphrase` command to specify the passphrase.

11 Before you continue, be aware of the following points:

- If you recovered the catalog from removable media, NetBackup freezes the catalog media.
  See "Unfreezing the NetBackup online catalog recovery media" on page 340.
- Before you restart NetBackup, Cohesity recommends that you freeze the media that contains the backups more recent than the date of the catalog from which you recovered.
- NetBackup does not run scheduled backup jobs until you stop and then restart NetBackup.
  You can submit backup jobs manually before you stop and restart NetBackup. However, if you do not freeze the media that contains the backups more recent than the date of the catalog from which you recovered, NetBackup may overwrite that media.

12 Clean up allowed list cache on all hosts.

13 Stop and restart NetBackup services on the primary 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
```

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 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 340.
  Proceed with the next step.

15 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

Note: A catalog recovery changes the configuration of NetBackup back to the point in time of the catalog backup. Any change to the configuration after the point-in-time of the catalog backup (For example: changes to policies, clients, storage units) must be re-applied if those changes are desired. These changes should be re-applied before new backups are taken. If the changes are not applied, they can affect what is protected and how the protection is managed.

As an example, a storage unit might have been modified to require the use of WORM locking on new images. If WORM locking isn't re-applied, new backups do not have the desired WORM protections.

Specifying the NetBackup job ID number after a catalog recovery

When the NetBackup catalog is recovered, NetBackup resets the job ID to 1. NetBackup starts assigning job numbers beginning with 1. You can specify the NetBackup job ID number after a catalog recovery.

To specify the NetBackup job ID number after a catalog recovery

1. Edit the NetBackup `jobid` file and set the value to one higher than the number from the last job ID number in the recovery catalog. The following is the pathname to the `jobid` file:
   - UNIX: `/usr/openv/netbackup/db/jobs/jobid`
   - Windows: *`install_path`*`\NetBackup\db\jobs\jobid`

   Because the recovery consumes job numbers, you must specify the number before the catalog recovery.
2. Recover the NetBackup catalog.

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.
- Restores the data and the metadata for the NetBackup databases (BMRDB, NBAZDB, NBDB) so that it is available for further recovery processing if required. See "About processing the NetBackup database in staging" on page 329.
- Optionally, recovers the policy and the licensing data.

Table 4-4 is a list of the files that are included in a partial recovery.

NetBackup supports recovery of the catalog image files and configuration files from a clustered environment to a non-clustered primary server at a disaster recovery.

Recovery recommendations

See "About NetBackup catalog recovery and symbolic links" on page 290.

Cohesity recommends that you recover the catalog images files in the following scenarios:

- The NetBackup database is valid, but NetBackup policy, backup image, or configuration files are lost or corrupt.
- 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 that are listed in the disaster recovery file, as follows:

Full backup	The image files and configuration files that are listed in the disaster recovery file are recovered.
Incremental backup	Two recover scenarios exist, as follows: ■ The catalog contains *no* information about the corresponding full backup and other incremental backups. NetBackup restores only the backup image `.f` files, configuration files, and NetBackup policy files that are backed up in that incremental backup. However, all of the catalog backup image `.f` files up to the last full catalog backup are restored. Therefore, you can restore the rest of the policy, image `.f` files, and configuration files with the NetBackup web UI with the **Regular recovery** option. Or you can use the Backup, Archive and Restore interface. ■ The catalog contains information about the corresponding full backup and other incremental backups. NetBackup restores all of the backup image `.f` files and the configuration files that were included in the related set of catalog backups.

Catalog image files

Table 4-4 lists the files that comprise a partial catalog recovery.

Table 4-4 Catalog image files

UNIX and Linux	Windows
`/usr/openv/netbackup/bp.conf`	Not applicable
`/usr/openv/netbackup/db/*`	*`install_path`*`\NetBackup\db\*`
`/usr/openv/netbackup/db/class/*` (optional)	*`install_path`*`\NetBackup\db\class\*` (optional)
`/usr/openv/netbackup/vault/sessions*`	*`install_path`*`\NetBackup\vault\sessions\*`

Table 4-4 Catalog image files *(continued)*

UNIX and Linux	Windows
`/usr/openv/var/*` (optional)	*`install_path`*`\NetBackup\var\*` (optional)
`/usr/openv/volmgr/database/*`	*`install_path`*`\Volmgr\database\*`
`/usr/openv/volmgr/vm.conf`	*`install_path`*`\Volmgr\vm.conf`

Recovering the NetBackup catalog image files using the NetBackup catalog recovery wizard

This procedure describes how to recover the NetBackup catalog image files by using the **NetBackup catalog recovery** wizard.

Warning: Do not run any client backups before you recover the NetBackup catalog.

To recover the catalog image files using the NetBackup catalog recovery wizard

1. Run the `nbgetconfig` command and save the output. This output can be used after the catalog recovery to recover the host-specific information that is overwritten during the catalog recovery.

   For example:

   ```
   ./nbgetconfig > sample.txt
   ```

2. Review the prerequisites before starting the catalog recovery.

   See "Prerequisites for recovering the NetBackup catalog or NetBackup catalog image files" on page 287.

3. If NetBackup is not running, start all of the NetBackup services by entering the following:

   - On UNIX and Linux:

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

   - On Windows:

     `install_path``\NetBackup\bin\bpup`

4. If the catalog backup and the recovery devices are not available, perform the following steps:

   - Configure the necessary recovery device in NetBackup.

- 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.
- Create symbolic links to match those in the original environment.
  See "About NetBackup catalog recovery and symbolic links" on page 290.

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:

5 Open the NetBackup web UI.

6 At the top, click **Settings > NetBackup catalog recovery**.

7 Specify where the disaster recovery file is stored. You can browse to select the file or enter the full pathname to the disaster recovery file.

In most cases, you specify the most recent disaster recovery information file available. If the most recent catalog backup is an incremental backup, use the disaster recovery file from the incremental backup. (There is no need to first restore the full backup and then follow with the incremental backup.)

If some form of corruption has occurred, you may want to restore to an earlier state of the catalog.

Click **Next** to continue.

8 NetBackup searches for the media that are required to recover the catalog. It then informs you of the progress and locates the necessary backup ID of the disaster recovery image. If the media is not located, NetBackup indicates 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**.

9 Select **Recover only NetBackup catalog image and configuration files**.

Select a **Job priority** if wanted and then click **Next** to initiate the recovery.

10 NetBackup 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.

11 After the recovery completes, click **Sign Out**.

Each image file is restored to the proper image directory and the configuration files are restored.

12 If you want to recover the image header information without recovering the entire NetBackup database, perform the following steps:

- Step a - Back up the target database. Run the following command.

  `nbdb_backup -online` *`directory`*

  Make sure that you do not specify the staging folder as the output directory. (The staging folder contains the schema data and configuration data for the NetBackup database from the catalog backup. Image `.f` and configuration files are recovered to their final destinations.)

- Step b - Recover the NetBackup database from the staging directory.

  ```
  nbdb_restore -recover -staging
  ```

- Step c - Export the image header data that you want to import from the backup.

  For example, the following command exports export all image header data. The data is exported to the `netbackup/db.export` directory.

  ```
  cat_export -all
  ```

- Step d- Recover the NetBackup database with the following command.

  `nbdb_restore -recover` *`directory`*

  Make sure that you specify the same directory as in step a.

- Step e- Run the `cat_import` command to import the image header data that you extracted in step c.

  ```
  cat_import -all -replace_destination -delete_source
  ```

  The command does the following:

  - Imports all of the image header data in the `netbackup/db.export` directory.
  - Replaces any image header data that was exported that already exists in the target database.
  - Removes the image header data that resides in the `netbackup/db.export` directory.

- Step f- If you recovered the catalog from a disk device, you may have to fix the disk media ID references. Run the following command:

  ```
  nbcatsync -sync_dr_file DR file path -dryrun
  ```

  Replace *DR file path* with the path to the catalog DR file.

- Step g - If the result of the dry run is satisfactory, run the following command:

  ```
  nbcatsync -sync_dr_file DR file path
  ```

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 340.
- Before you restart NetBackup, Cohesity 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 database portion of the catalog.
  See "About recovering the NetBackup databases" on page 320.

14 Recover the host settings that you backed up in step 1. Run the following command.

```
./nbsetconfig sample.txt
```

15 Stop and restart the NetBackup services on the primary server, as follows:

- On UNIX and Linux:

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

- On Windows:

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

16 After the services are restarted, run the following command:

On a non-clustered setup:

Windows:

```
install_path\netbackup\bin\nbcertcmd -renewcertificate
```

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 exist status 5988, refer to the following topic:
  See "Steps to carry out when you see exit status 5988 during catalog recovery" on page 340.
  Proceed with the next step.

17 If the catalog recovery is part of a server recovery procedure, complete the remaining steps in the appropriate recovery procedure.

Recovery can include the following:

- Importing the backups from the backup media into the catalog.
- Write protecting the media.
- Ejecting the media and setting it aside.
- Freezing the media.

Recovering the NetBackup catalog image files using bprecover -wizard

The `bprecover -wizard` command is an alternative to using the NetBackup catalog recovery wizard.

Warning: Do not run any client backups before you recover the NetBackup catalog.

See "About recovering the NetBackup catalog image files" on page 306.

To recover the catalog image files using bprecover -wizard

1. Run the `nbgetconfig` command and save the output. This output can be used after the catalog recovery to recover the host-specific information that is overwritten during the catalog recovery.

   For example:

   ```
   ./nbgetconfig > sample.txt
   ```

2. Review the prerequisites before starting the catalog recovery.

   See "Prerequisites for recovering the NetBackup catalog or NetBackup catalog image files" on page 287.

3. 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 symbolic links to match those in the original environment.
     See "About NetBackup catalog recovery and symbolic links" on page 290.

4. Start the NetBackup services on the primary server by entering the following command:

   - On Windows:
     install_path\NetBackup\bin\bpup
   - On UNIX and Linux:
     /usr/openv/netbackup/bin/bp.start_all

5. Start the `bprecover` wizard by entering the following command:

   ```
   bprecover -wizard
   ```

   The following is displayed:

   ```
   Welcome to the NetBackup Catalog Recovery Wizard!
   Please make sure the devices and media that contain catalog
   disaster recovery data are available
   Are you ready to continue?(Y/N)
   ```

6 Enter **Y** to continue. You are prompted to enter the full path name of the disaster recovery file, as follows:

```
Please specify the full pathname to the catalog disaster recovery
file:
```

7 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)
```

8 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)
```

9 Enter **Y** or **N** to continue. The following is displayed:

```
Do you also want to include licensing data?(Y/N)
```

10 Enter **Y** or **N** to continue. The following is displayed:

```
Catalog recovery is in progress. Please wait...

Gathering configuration information.
Waiting for the security services to start operation.
Generating identity for host 'vm2.example.com_1318309224'
Setting up security on target host: vm2.example.com_1318309224
nbatd is successfully configured on NetBackup Primary Server.
Operation completed successfully.

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 "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.

WRN - Local or global-level settings that you have configured on the
master server before catalog recovery are overwritten.
It is recommended that you re-configure the required settings after
the services are restarted.

For more information, please review the log file:
/usr/openv/netbackup/logs/user_ops/root/logs/Recover1318357550.log
```

11 When the recovery job is finished, each image file is restored to the proper image directory and the configuration files are restored. If you chose to recover the policy data and licensing data, it is restored also.

12 If you want to recover the image header information without recovering the entire NetBackup database, perform the following steps:

- Step a - Back up the target database. Run the following command.
  `nbdb_backup -online` *directory*

Make sure that you do not specify the staging folder as the output directory. (The staging folder contains the schema data and configuration data for the NetBackup database from the catalog backup. Image `.f` and configuration files are recovered to their final destinations.)

- Step b - Recover the NetBackup database from the staging directory.

  ```
  nbdb_restore -recover -staging
  ```

- Step c - Export the image header data that you want to import from the backup.
  For example, the following command exports export all image header data. The data is exported to the `netbackup/db.export` directory.

  ```
  cat_export -all
  ```

- Step d- Recover the NetBackup database with the following command.

  ```
  nbdb_restore -recover directory
  ```

  Make sure that you specify the same directory as in step a.

- Step e- Run the `cat_import` command to import the image header data that you extracted in step c.

  ```
  cat_import -all -replace_destination -delete_source
  ```

  The command does the following:

  - Imports all of the image header data in the `netbackup/db.export` directory.
  - Replaces any image header data that was exported that already exists in the target database.
  - Removes the image header data that resides in the `netbackup/db.export` directory.

- Step f- If you recovered the catalog from a disk device, you may have to fix the disk media ID references. Run the following command:

  ```
  nbcatsync -sync_dr_file DR file path -dryrun
  ```

  Replace *DR file path* with the path to the catalog DR file.

- Step g - If the result of the dry run is satisfactory, run the following command:

  ```
  nbcatsync -sync_dr_file DR file path
  ```

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 340.
- Before you restart NetBackup, Cohesity 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 database portion of the catalog.
  See "About recovering the NetBackup databases" on page 320.

14 Clean up allowed list cache for all hosts.

15 Recover the host settings that you backed up in step 1. Run the following command.

```
./nbsetconfig sample.txt
```

16 Stop and restart NetBackup services on the primary server and other hosts, as follows:

- On Windows:

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

- On UNIX:

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

17 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:

install_path\netbackup\bin\nbcertcmd -renewcertificate

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 external CA-signed certificates are used in your NetBackup domain, perform the following steps.
  Non-clustered setup:
  UNIX:

  /usr/openv/netbackup/bin/nbcertcmd -enrollCertificate

  Windows:

  install_path\netbackup\bin\nbcertcmd -enrollCertificate

  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 340.
  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 databases

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 database also contains the NetBackup catalog images files. The images files contain the metadata that describes the backups.

You can recover the NetBackup databases independently of an entire catalog backup.

Recover from a backup	See "Recovering the NetBackup database from a backup" on page 320.
Recover from the staging directory	See "Recovering the NetBackup database from staging" on page 325.

Recovering the NetBackup database from a backup

You can recover the NetBackup (NBDB), NetBackup Authorization (NBAZDB), or Bare Metal Restore (BMRDB) databases 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 database is available and the NetBackup Scale-Out Relational Database server is running, you do not need to create a database. Do only step 10 and step 12 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 database 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 NBDB, NBAZDB, or BMRDB from the database directories to a temporary directory.

The following are the default locations for the database files:

install_path`\NetBackupDB\data\nbdb`
install_path`\NetBackupDB\data\nbazdb`
install_path`\NetBackupDB\data\bmrdb`

```
/usr/openv/db/data/nbdb
/usr/openv/db/data/nbazdb
/usr/openv/db/data/bmrdb
```

3 Start the NetBackup Scale-Out Relational Database server, as follows:

UNIX: `/usr/openv/netbackup/bin/nbdbms_start_stop start`

Windows: *install_path*`\NetBackup\bin\bpup -e vrtsdbsvc_psql`

4 Create the database. The command that you run depends on your scenario, as follows:

Run the command from the following directory:

UNIX: `/usr/openv/db/bin`

Windows: *`install_path`*`\NetBackup\bin`

Normal scenario	`create_nbdb -drop`
The database was relocated or the environment is clustered	`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	`create_nbdb -drop -data` *`VXDBMS_NB_DATA`* `-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.

5 Start the NetBackup services, as follows:

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

Windows: *`install_path`*`\NetBackup\bin\bpup`

6 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`

7 If you used the `nbdb_move` command to relocate the NetBackup databases, recreate the directories where databases were located when you backed up the catalog. The following are the default locations into which the `nbdb_move` command moves the databases:

install_path\NetBackupDB\data\nbdb
install_path\NetBackupDB\data\nbazdb
install_path\NetBackupDB\data\bmrdb

/usr/openv/db/data/nbdb
/usr/openv/db/data/nbazdb
/usr/openv/db/data/bmrdb

8 Start the NetBackup device manager on the NetBackup primary server, as follows:

UNIX: `/usr/openv/volmgr/bin/ltid -v`

Windows: Use Windows Computer Management to start the NetBackup Device Manager service (`ltid.exe`).

9 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:

https://support.cohesity.com/s/article/article-100040135

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:

https://support.cohesity.com/s/article/article-100040135

Import the catalog backup from the media on which it resides.

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

https://support.cohesity.com/s/article/article-100040135

10 Recover the catalog by running the following command on the primary server:

UNIX: `/usr/openv/netbackup/bin/admincmd/bprecover -r -nbdb`

Windows: *install_path*`\NetBackup\bin\admincmd\bprecover -r -nbdb`

11 Clean up allowedlist cache for all hosts.

12 Stop and restart NetBackup services on the primary 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
```

13 After the services are restarted, renew the certificates:

- 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 exist status 5988, refer to the following topic:

See "Steps to carry out when you see exit status 5988 during catalog recovery" on page 340.

Recovering the NetBackup database from staging

During a catalog backup, the data and the metadata of the NetBackup databases (BMRDB, NBAZDB, and NBDB) are copied to the staging directory. The recovery option that restores the image files and the configuration files also restores the data and metadata for the NetBackup databases to the staging directory.

See "About recovering the NetBackup catalog image files" on page 306.

You can recover the NetBackup databases (BMRDB, NBAZDB, and NBDB) from the staging directory.

See "About processing the NetBackup database in staging" on page 329.

Two recovery procedures from the staging directory exist, as follows:

The database is not corrupted	See "To recover the NetBackup database from staging if the database is not corrupted" on page 326.
The database is corrupted	See "To recover the NetBackup database from staging if the database is corrupted" on page 326.

To recover the NetBackup database from staging if the database is not corrupted

1. Run the following command on the primary 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\bpdown
   install_path\NetBackup\bin\bpup
   ```

To recover the NetBackup database from staging if the database is corrupted

1. If the NetBackup services are running, stop them as follows:

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

   Windows: *install_path*`\NetBackup\bin\bpdown`

2. Move the NBDB, NBAZDB, or BMRDB from the database directories to a temporary directory.

   The following are the default locations for the database files:

   ```
   install_path\NetBackupDB\data\nbdb
   install_path\NetBackupDB\data\nbazdb
   install_path\NetBackupDB\data\bmrdb

   /usr/openv/db/data/nbdb
   /usr/openv/db/data/nbazdb
   /usr/openv/db/data/bmrdb
   ```

3. Start the NetBackup Scale-Out Relational Database server, as follows:

   UNIX: `/usr/openv/netbackup/bin/nbdbms_start_stop start`

   Windows: *install_path*`\NetBackup\bin\bpup -e vrtsdbsvc_psql`

4. Create an empty database, as follows:

   UNIX: `/usr/openv/db/bin/create_nbdb -drop`

   Windows: *`install_path`*`\NetBackup\bin\create_nbdb -drop`

5. 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
   ```

6. 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`

7. If you used the `nbdb_move` command to relocate NetBackup database, recreate the directory where the database was located when you backed up the catalog.

8. Start the NetBackup Device Manager, as follows:

   UNIX: `/usr/openv/volmgr/bin/ltid -v`

   Windows: Start the device manager service.

9. Run the following command on the primary 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`

10. Clean up allowed list cache for all hosts.

11 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
```

12 After the services are restarted, renew the certificates:

- 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 exist status 5988, refer to the following topic:

See "Steps to carry out when you see exit status 5988 during catalog recovery" on page 340.

About processing the NetBackup database in staging

Warning: Cohesity recommends that you process the NetBackup NetBackup database *only* when directed to do so by Cohesity Technical Support. For help with NetBackup domain merges and splits, contact the Cohesity Information Management Consulting Services:

http://www.veritas.com/business/services/consulting_services.jsp

More information about the commands in the *NetBackup Commands Reference Guide*:

https://support.cohesity.com/s/article/article-100040135

A recovery of the NetBackup image files and configuration files also restores the data and metadata for the NetBackup databases (BMRDB, NBAZDB and NBDB) to the staging directory. You can use the following NetBackup command to further process the NBDB database if required:

`nbdb_restore -staging`	Use `nbdb_restore -staging` to recover the NetBackup database from the staging directory. See "Recovering the NetBackup database from staging" on page 325.

Terminating database connections

Before you run `nbdb_unload`, shut down NetBackup to terminate all active connections to the database. Shutting down NetBackup eliminates any possible concurrency problems.

To terminate database connections on Windows

1. Shut down all NetBackup services by typing the following command:

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

2. In the Windows **Services Manager**, restart the service called **NetBackup Scale-Out Relational Database Manager**.

3. Use one of the following methods to terminate database connections:
   - Use the NetBackup Database Administration utility.
   - Run `nbdb_unload` and indicate the outputs (database name, tables, or schema only) and the destination directory.
4. Stop the NetBackup Scale-Out Relational Database Manager service with the following command:

   install_path\NetBackup\bin\bpdown -e vrtsdbsvc_psql
5. Start all NetBackup services by typing the following command:

   install_path\NetBackup\bin\bpup

To terminate database connections on UNIX

1. Shut down all NetBackup daemons by typing the following command:

   /usr/openv/netbackup/bin/bp.kill_all
2. Start the NetBackup database daemon with the following command:

   /usr/openv/netbackup/bin/nbdbms_start_stop start
3. Start only the database server by using /usr/openv/netbackup/bin/nbdbms_start_stop start
4. Use one of the following methods to terminate database connections:
   - Use the NetBackup Database Administration utility.
   - Run `nbdb_unload` and indicate the outputs (database name, tables, or schema only) and the destination directory.
5. Shut down the database server by using `/usr/openv/netbackup/bin nbdbms_start_stop stop`.
6. Stop the NetBackup Scale-Out Relational Database Manager service with the following command:

   /usr/openv/netbackup/bin/nbdbms_start_stop stop
7. Start all NetBackup daemons by typing the following command:

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

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

Step	Task	Procedure
Step 1	If recovering to a primary server on which NBAC is configured and operational, disable NBAC (that is, set it to PROHIBITED mode).	See the *NetBackup Security and Encryption Guide*: https://support.cohesity.com/s/article/article-100040135
Step 2	Recover the NetBackup catalog from the online catalog backup using the Catalog Recovery Wizard or the `bprecover` command.	See "About recovering the entire NetBackup catalog" on page 295.
Step 3	Configure NetBackup to use NBAC by setting it to AUTOMATIC or REQUIRED as per the security level desired.	See the *NetBackup Security and Encryption Guide*: https://support.cohesity.com/s/article/article-100040135
Step 4	Restart NetBackup.	`/usr/openv/netbackup/bin/bp.kill_all` `/usr/openv/netbackup/bin/bp.start_all`

Table 4-6 To recover the NetBackup catalog on Windows when NetBackup Access Control is configured

Step	Task	Procedure
Step 1	If recovering to a primary server on which NBAC is configured and operational, disable NBAC (that is, set it to PROHIBITED mode).	See the *NetBackup Security and Encryption Guide*: https://support.cohesity.com/s/article/article-100040135
Step 2	Stop the NetBackup services.	*install_path*`\NetBackup\bin\bpdown.exe`

Table 4-6 To recover the NetBackup catalog on Windows when NetBackup Access Control is configured *(continued)*

Step	Task	Procedure
Step 3	In Windows, change the startup type of the NetBackup Authentication Service and NetBackup Authorization Service to Disabled.	Instructions for configuring Microsoft Windows are beyond the scope of the NetBackup documentation. Refer to the appropriate Microsoft documentation.
Step 4	Start the NetBackup services.	*install_path*\NetBackup\bin\bpup.exe
Step 5	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.	See "About recovering the entire NetBackup catalog" on page 295.
Step 6	In Windows, change the startup type of the NetBackup Authentication Service and NetBackup Authorization Service to Automatic.	Instructions for configuring Microsoft Windows are beyond the scope of the NetBackup documentation. Refer to the appropriate Microsoft documentation.
Step 7	Configure NetBackup to use NBAC.	The procedure depends on the environment, as follows: ■ For a NetBackup primary server in a Windows Server Failover Clustering environment, run the following command on the NetBackup primary server on the active node: `bpnbaz -setupmaster` This command provisions the Windows registry on all nodes with the required entries for NBAC. ■ For recovery to a new installation, run the following command on the NetBackup primary server: `bpnbaz -setupmaster` ■ For recovery in an existing environment, set NBAC to AUTOMATIC or REQUIRED as per the security level desired. See the *NetBackup Security and Encryption Guide*: https://support.cohesity.com/s/article/article-100040135
Step 8	Restart NetBackup.	*install_path*\NetBackup\bin\bpdown.exe *install_path*\NetBackup\bin\bpup.exe

See "Options to recover the NetBackup catalog" on page 286.

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.

To recover the catalog from a non-primary copy

1. Review the prerequisites before starting the catalog recovery.

   See "Prerequisites for recovering the NetBackup catalog or NetBackup catalog image files" on page 287.

2. If the copy of the catalog backup is on a medium other than tape, do the following:

   BasicDisk — Make sure that the disk that contains the backup is mounted against the correct mount path (as displayed in the disaster recovery file).

   Disk pool — For a catalog backup file in a disk pool, do the following:

   - Create the disk storage server for the storage by using the **Storage Server Configuration Wizard**.
   - Create the disk pool for the storage by using the **Disk Pool Configuration Wizard**.
   - Run the following command to synchronize the disaster recovery file to the new disk pool.

     ```
     nbcatsync -sync_dr_file disaster_recovery_file
     ```

3. Run the following NetBackup command to recover the catalog:

   ```
   bprecover -wizard -copy N
   ```

   N is the number of the copy from which you want to recover.

Recovering the NetBackup catalog without the disaster recovery file

If the disaster recovery file has been lost, consult the email that was sent to the administrator when the catalog was backed up. The disaster recovery file is written to the location you specify in the catalog backup policy and is appended to the backup stream itself.

If multiple streams are configured for the Catalog policy, DR package and DR file will have a suffix as `_DMS`.

In this case, the DR file is the consolidation of data from all streams and must be provided as it is during disaster recovery.

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 commands to retrieve all disaster recovery files from the catalog backup media:
   - (Conditional) - This is required only if multi-stream catalog backup was configured and the backup spans more than one piece of media.
     `bpimport-create_db_info -id` *`mediaid`* `-server` *`master_server_hostname`* `-L` *`progress_log`*
   - `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 290.

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 primary server and in email attachments to the NetBackup administrator.
2. Set up each primary server and media server in the same configuration as the configuration that is used during the last catalog backup. The primary 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 the NetBackup configuration for the primary 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 primary server.

UNIX:

```
/usr/openv/netbackup/db/images/primary_server/timestamp/tmp
```

Windows:

```
C:\Program Files\VERITAS\NetBackup\db\images\primary_server
\timestamp\tmp
```

Copy the DR file to the newly created directory.

5 Edit the DR file in `netbackup/db/images/primary_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 primary_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 in the disaster recovery file.

```
bpimport -server primary_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 NetBackup web UI and click **Recovery**. Then on the **Regular recovery** card click **Start recovery**. Or, use the Backup, Archive, and Restore client interface.
- Select **NBU-Catalog** as the policy type.
- Set the source client and destination client to your primary server.
- Search the backups and restore all files that are located in the following directory:

```
install_path/netbackup/db/images/primary_server
```

- Verify that all files are restored successfully on the primary server.

9 Restore your critical data.

- Open the NetBackup web UI and click **Recovery**. Then on the **Regular recovery** card click **Start recovery**. Or, use the Backup, Archive, and Restore client interface.
- Select **NBU-Catalog** as the policy type.
- Set the source client and destination client to your primary server.
- (Backup, Archive, and Restore interface) Refresh the view.
- Restore the catalog backup images for each media server which requires data recovery.
- Browse for the following directory on the primary server.

  ```
  install_path/netbackup/db/images
  ```

- Restore the catalog backup images for each media server which requires data recovery. 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.

- Open the NetBackup web UI and click **Recovery**. Then on the **Regular recovery** card click **Start recovery**. Or, use the Backup, Archive, and Restore client interface.
- Select the policy type to match the data you want to restore.
- Set the source client and destination client to match the client that backed up the data.
- (Backup, Archive, and Restore interface) Refresh the view.

11 To recover the NetBackup database, run the following:

```
bprecover -r -nbdb
```

This command restores NetBackup media usage information, ensure that media containing backups are not overwritten, and restore the storage unit configuration.

You cannot recover the NetBackup database to a configuration that is not identical to the configuration on which the catalog was backed up. Instead, you must import each piece of backup media.

12 If your catalog recovery media is on tape, freeze the media that contains the catalog backup that is used for recovery. This action protects the media from being reused:

```
bpmedia -freeze -m media -h primary_server
```

Run `bpmedialist` to verify that the media is frozen.

13 Recover your policies and configuration data on each primary 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 NetBackup web UI and click **Recovery**. Then on the **Regular recovery** card click **Start recovery**. Or, use the Backup, Archive, and Restore client interface.
- Select **NBU-Catalog** as the policy type.
- Set the source client and destination client to your primary server.
- For each additional server that you want to restore, set the source client and destination client to that server.
- Restore all files that are backed up by the hot catalog backup on each server.

14 Clean up the allowed list cache for all hosts.

15 Stop and restart the NetBackup services on all hosts.

16 After the services are restarted, renew the certificates:

- 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 exist status 5988, refer to the following topic:

See "Steps to carry out when you see exit status 5988 during catalog recovery" on page 340.

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 web UI or the 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 "Options to recover the NetBackup catalog" on page 286.

To restore files from an online catalog backup

1. Open the NetBackup web UI. Or, use the Backup, Archive, and Restore client interface.
2. Click **Recovery**. Then on the **Regular recovery** card click **Start recovery**.
3. Select **NBU-Catalog** as the policy type.

4 Set the source client and destination client to your primary server.

5 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 "Options to recover the NetBackup catalog" on page 286.

To unfreeze the online catalog recovery media

1 On the primary 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 primary server, run the following command:

```
bpimport
```

3 On the primary 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: https://support.cohesity.com/s/article/article-100034092

Proceed to the next step.

2 Perform the user logon on the primary server. Use the following command:

```
install_path\netbackup\bin\bpnbat -login -loginType WEB
```

For example:

```
install_path\netbackup\bin\bpnbat -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 primary server. For a clustered primary 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 primary server. You can obtain its value by running the following command:

```
install_path\netbackup\bin\nbcertcmd -listCertDetails
```

For a clustered primary 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-xxxxxxxxx
Issued By : /CN=broker/OU=root@abc/O=vx
Serial Number : 0x62e108c90000000c
Expiry Date : Aug 21 08:42:54 2018 GMT
SHA1 Fingerprint : 50:89:AE:66:12:9A:29:4A:66:E9:DB:71:37:C7:
EA:94:8C:C6:0C:A0
Master Server : xyz
Host ID : 5a8dde7b-xxxx-4252-xxxx-d3bedee63e0a
Issued By : /CN=broker/OU=root@xyz.example.com/O=vx
Serial Number : 0x6ede87a70000000a
Expiry Date : Aug 21 09:52:13 2018 GMT
SHA1 Fingerprint : FE:08:C2:09:AC:5D:82:57:7A:96:5C:C1:4A:E6:
EC:CA:CC:99:09:D2
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 primary 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\admincmd\nbhostmgmt -a -i host ID -hm
hostname

install_path\netbackup\bin\admincmd\nbhostmgmt -a -i
78f9eed4-xxxx-4c6a-bb40-xxxxxxxxx -hm abc.example.com
abc.example.com is successfully mapped to
78f9eed4-xxxx-4c6a-bb40-xxxxxxxxx.
```

Alternately, you can also add this host-ID-to-host name mapping in the NetBackup web UI. Open **Security > Host mappings**.

6 Do the following to renew the certificates:

- To renew the NetBackup (or host ID-based) certificate of the primary server, use the following command:

  ```
  install_path\netbackup\bin\nbcertcmd -renewCertificate
  ```

  For a clustered primary server, run the following command:

```
install_path\netbackup\bin\nbcertcmd -renewCertificate -cluster
```