Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

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

https://sort.veritas.com/documents

Documentation feedback

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

Contents

Chapter 1  Introduction ........................................................................................................... 10

About NetBackup commands ......................................................................................... 10
Navigating multiple menu levels .................................................................................... 11
NetBackup command conventions .................................................................................. 11
NetBackup Media Manager command notes .................................................................. 12
IPV6 updates .................................................................................................................. 12

Appendix A  NetBackup Commands ................................................................................ 14

acsd ................................................................................................................................. 23
add_media_server_on_clients ....................................................................................... 25
backupdbtrace ............................................................................................................... 26
backuptrace .................................................................................................................... 28
bmrc ............................................................................................................................... 30
bmrconfig ....................................................................................................................... 33
bmrepadm ....................................................................................................................... 39
bmrepadm ....................................................................................................................... 39
bmrprep ........................................................................................................................ 42
bmrs ................................................................................................................................. 45
bmrsrtadm ...................................................................................................................... 48
bp .................................................................................................................................. 49
bparchive ......................................................................................................................... 51
bpbackup ........................................................................................................................ 57
bpbackupdb .................................................................................................................... 66
bpcatarc ......................................................................................................................... 67
bpcatlist .......................................................................................................................... 68
bpctares .......................................................................................................................... 71
bpctrm ............................................................................................................................. 72
bp cd ................................................................................................................................ 73
bpchangeprimary ............................................................................................................. 75
bpclient ............................................................................................................................ 79
bpcimagelist .................................................................................................................... 86
bpcntcmd ........................................................................................................................ 90
bpclusterutil ................................................................................................................... 94
bpcompatd ....................................................................................................................... 97
bpconfig .......................................................................................................................... 99
bpdbjobs ........................................................................................................................ 108
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>bpdbm</td>
<td>115</td>
</tr>
<tr>
<td>bpdgclone</td>
<td>118</td>
</tr>
<tr>
<td>bpdown</td>
<td>120</td>
</tr>
<tr>
<td>bpduplicate</td>
<td>121</td>
</tr>
<tr>
<td>b perror</td>
<td>131</td>
</tr>
<tr>
<td>bpexpdate</td>
<td>140</td>
</tr>
<tr>
<td>bpfis</td>
<td>149</td>
</tr>
<tr>
<td>bpflist</td>
<td>151</td>
</tr>
<tr>
<td>bpgetconfig</td>
<td>158</td>
</tr>
<tr>
<td>bpgetdebuglog</td>
<td>164</td>
</tr>
<tr>
<td>bpimage</td>
<td>166</td>
</tr>
<tr>
<td>bpimagelist</td>
<td>171</td>
</tr>
<tr>
<td>bpimmedia</td>
<td>180</td>
</tr>
<tr>
<td>bpimport</td>
<td>192</td>
</tr>
<tr>
<td>bpinst</td>
<td>200</td>
</tr>
<tr>
<td>bpkeyfile</td>
<td>207</td>
</tr>
<tr>
<td>bpkeyutil</td>
<td>209</td>
</tr>
<tr>
<td>bplabel</td>
<td>211</td>
</tr>
<tr>
<td>bplist</td>
<td>215</td>
</tr>
<tr>
<td>bpmedia</td>
<td>223</td>
</tr>
<tr>
<td>bpmedialist</td>
<td>227</td>
</tr>
<tr>
<td>bpmlicense</td>
<td>239</td>
</tr>
<tr>
<td>bpnbat</td>
<td>242</td>
</tr>
<tr>
<td>bpnbaz</td>
<td>251</td>
</tr>
<tr>
<td>bppficorr</td>
<td>269</td>
</tr>
<tr>
<td>bpplcadtrinfo</td>
<td>272</td>
</tr>
<tr>
<td>bpplcients</td>
<td>276</td>
</tr>
<tr>
<td>bpldelete</td>
<td>287</td>
</tr>
<tr>
<td>bpplinclude</td>
<td>289</td>
</tr>
<tr>
<td>bppinfo</td>
<td>297</td>
</tr>
<tr>
<td>bpplist</td>
<td>324</td>
</tr>
<tr>
<td>bpplsched</td>
<td>332</td>
</tr>
<tr>
<td>bpplschedrep</td>
<td>350</td>
</tr>
<tr>
<td>bpplschedwin</td>
<td>360</td>
</tr>
<tr>
<td>bppolicynew</td>
<td>363</td>
</tr>
<tr>
<td>bpps</td>
<td>372</td>
</tr>
<tr>
<td>bprd</td>
<td>377</td>
</tr>
<tr>
<td>bprecover</td>
<td>379</td>
</tr>
<tr>
<td>bprestore</td>
<td>382</td>
</tr>
<tr>
<td>bpretlevel</td>
<td>398</td>
</tr>
<tr>
<td>bpschedule</td>
<td>401</td>
</tr>
<tr>
<td>bpschedulerep</td>
<td>409</td>
</tr>
<tr>
<td>bpsetconfig</td>
<td>416</td>
</tr>
</tbody>
</table>
Contents
nbdb_backup ................................................................. 616
nbdb_move ................................................................. 618
nbdb_ping ................................................................. 620
nbdb_restore ............................................................. 621
nbdb_unload ............................................................. 623
nbdb2adutil ............................................................... 626
nbdbms_start_server .................................................. 629
nbdbms_start_stop .................................................... 630
nbdc ................................................................. 631
nbdecommission ......................................................... 634
nbdelete ................................................................. 637
nbdeployutil .............................................................. 642
nbdevconfig .............................................................. 650
nbdevquery .............................................................. 663
nbdiscover ............................................................... 669
nbdna ................................................................. 673
nbemn ................................................................. 677
nbemmcmd ............................................................... 678
nbfindfile ............................................................... 697
nbfirescan ............................................................... 701
nbftadm ................................................................. 703
nbftconfig ............................................................... 704
nbgetconfig ............................................................. 714
nbhba ................................................................. 717
nbholdutil ............................................................... 720
nbhostidentity .......................................................... 723
nbhostmgmt ............................................................. 727
nbhypervtool ........................................................... 732
nbidpcmd ............................................................... 734
nbimageshare .......................................................... 736
nbinstallcmd ............................................................ 737
nbjm ................................................................. 746
nbkmioutil ............................................................... 747
nbkmcmd ............................................................... 751
nbkmsutil ............................................................... 758
nboraadm ............................................................... 762
nboraip ................................................................. 771
nbpem ................................................................. 774
npem ................................................................. 776
nbperfchk ............................................................... 781
nbplupgrade ............................................................. 785
nbrb ................................................................. 788
nbrbutil ..................................................................................... 789
nbregopsc ................................................................................. 795
nbreplicate ............................................................................... 797
nbrepo ..................................................................................... 800
nbrestorevm ............................................................................. 802
nbsecmd ................................................................................ 822
nbsetconfig ............................................................................... 831
nbsnapimport ........................................................................... 833
nbsnapreplicate ......................................................................... 835
nbsqladm ................................................................................. 837
nbstl ......................................................................................... 845
nbstlutil ..................................................................................... 854
nbstop ...................................................................................... 864
nbsu ....................................................................................... 867
nbsvrgrp .................................................................................. 871
resilient_clients .......................................................................... 874
restoretrace ............................................................................... 875
stopltid ..................................................................................... 877
tidd .......................................................................................... 878
tidcd ......................................................................................... 882
tpautoconf ................................................................................. 886
tpclean ..................................................................................... 889
tpconfig .................................................................................... 892
tpext ........................................................................................ 913
tpreq ........................................................................................ 914
tpunmount ................................................................................. 917
verifytrace ................................................................................. 919
vltdadm ................................................................................... 922
vltdcontainers ............................................................................. 924
vlteject ..................................................................................... 929
vltinject ..................................................................................... 933
vltoffsitemedia ............................................................................ 935
vltopmenu ................................................................................ 939
vltrun ...................................................................................... 941
vmadd ...................................................................................... 946
vmchange ................................................................................ 949
vmcheckxxx .............................................................................. 956
vmd ........................................................................................ 958
vmdelete ................................................................................... 960
vmoprcmd ................................................................................ 962
vmphyinv .................................................................................. 967
vmpool ..................................................................................... 971
vmquery ................................................................................... 974
Index

1021
Introduction

This chapter includes the following topics:

- About NetBackup commands
- Navigating multiple menu levels
- NetBackup command conventions
- NetBackup Media Manager command notes
- IPV6 updates

About NetBackup commands

This document contains all of the NetBackup man page commands. You can find a printable version of the command quickly and easily without searching through multiple books in the NetBackup Library.

This document contains detailed information on commands that run on UNIX systems as well as on Windows systems. Information that is pertinent only for UNIX systems versus Windows systems is noted accordingly.

Each command contains a brief description of the primary function of the command, a synopsis, and descriptions of each of the options listed in the synopsis. Some commands also contain notes, return values, examples, etc.

Included in this document are the NetBackup Server and NetBackup Enterprise Server commands. In most cases, a command pertains to both NetBackup products. However, there are instances where portions or options within a command apply specifically to one product such as NetBackup Enterprise Server. In these situations, a note has been inserted in the text to identify the information as information that only applies to one NetBackup product.
Navigating multiple menu levels

When navigating multiple menu levels, a greater-than sign (>) is used to indicate a continued action. The following example shows how the > is used to condense a series of menu selections into one step:

Start > Programs > Veritas NetBackup > NetBackup Administration Console.

The corresponding actions can be described in more steps as follows:

1. Click **Start** in the task bar.
2. Move your cursor to **Programs**.
3. Move your cursor to the right and highlight **Veritas NetBackup**.
4. Move your cursor to the right. First highlight and then click **NetBackup Administration Console**.

NetBackup command conventions

This document uses the following conventions when describing commands that are specific to NetBackup.

Run the following commands in the "Command Prompt" to see the results.

- The **-help (-h)** option prints a command line usage message when it is the only option on the command line. For example:

  `bpclient -help`

- Brackets [ ] indicate that the enclosed component of the command line is optional.

- Curly braces {} indicate an association between the enclosed options. For example, {opt1 [opt2 ... optn]} means that if the command contains opt1, then the command may optionally contain opt2 ... optn.

- A vertical bar (or the pipe symbol) | separates optional arguments from which the user can choose. For example, if a command has the following format, you can choose **arg1** or **arg2** (but not both):

  `command [ arg1 | arg2 ]`

- Italics indicate that the information is user supplied. For example, the user supplies policy, schedule, and filename in the following command:

  `bpbackup -p policy -s schedule filename`
An ellipsis (...) means that you can repeat the previous parameter. For example, consider the following command:

```
bpbackup [-S master_server [,master_server,...]] filename
```

Here, the -S option requires the first master server name. Additional names can be added, separated by commas and followed by a file name as in:

```
bpbackup -S mars,coyote,shark,minnow memofile.doc
```

**NetBackup Media Manager command notes**

In addition, Media Manager supports the following sets of commands that are used for device management; the NetBackup Device Manager service (ltid) starts or stops these commands as needed.

- `tpreq` and `tpunmount` are user commands for requesting tape mounts and unmounts for configured drives.
- `tpautoconf`, `tpclean`, `tpconfig`, and `vmoprcmd` are administrative commands for device management.
- `vmadd`, `vmchange`, `vmcheckxxx`, `vmdelete`, `vmpool`, `vmquery`, `vmrule`, and `vmupdate` are administrative commands for media management.

**IPV6 updates**

NetBackup does not support the use of IPv6 addresses where you can specify a host name (for example: `2001:db8:85a3:8d3:1319:8a2e:370:7348`). If a host name is required, NetBackup does not support the use of an IPv6 address. This rule remains true even though host names can resolve to IPv6 addresses through DNS, local hosts files, or other means.

Only the NetBackup commands and options that are shown let you enter an IPv6 address:

- `bpclntcmd -ip option`.
- `manageClientCerts -IP option`.
- `bpcluster VIRTUALADDRESS`
- `csconfig cldinstance` any references to host name or IP address.
- `nbhostmgmt -host option`.
- `bptestnetconn -H option`. 
Only the bp.conf parameters that are shown allow IPv6 addresses. All other parameters follow the same rules as command line options:

- PREFERRED_NETWORK
- RESILIENT_NETWORK
- VXSS_NETWORK
- THROTTLE_BANDWIDTH
NetBackup Commands

This appendix includes the following topics:

- acsd
- add_media_server_on_clients
- backupdbtrace
- backuptrace
- bmrc
- bmrcconfig
- bmrepadm
- bmrprep
- bmrs
- bmrsrtadm
- bp
- bparchive
- bpbackup
- bpbackupdb
- bpcatarc
- bpcatlist
- bpcatres
- bpcatrm
- bpcd
- bpchangeprimary
- bpclient
- bpclimagelist
- bpcintcmd
- bpclusterutil
- bpcompatd
- bpconfig
- bpdbjobs
- bpdbm
- bpdgclone
- bpdown
- bpduplicate
- bperror
- bpexpdate
- bpfs
- bpflist
- bpgetconfig
- bpgetdebuglog
- bpimage
- bpimagelist
- bpimmedia
- bpimport
- bpinst
- bpkeyfile
- bpkeyutil
- bplabel
- bplist
- bpmmedia
- bpmedialist
- bpmlicense
- bpnbat
- bpnbaz
- bppficorr
- bpplcatdrinfo
- bpplclients
- bppldelete
- bpplinclude
- bpplinfo
- bppllist
- bpplsched
- bpplschedrep
- bpplschedwin
- bppolicynew
- bpps
- bprd
- bprecover
- bprestore
- bpretlevel
- bpschedule
- bpschedulerep
- bpsetconfig
- bppstsinfo
- bpstuadd
- bpstudel
- bpstulist
- bpsturep
- bpstestbpcd
- bpstestnetconn
- bpstpcinfo
- bpup
- bpverify
- cat_convert
- cat_export
- cat_import
- configureCerts
- configureCertsForPlugins
- configureMQ
- configurePorts
- configureWebServerCerts
- create_nbdb
- csconfig cldinstance
- csconfig cldprovider
- csconfig meter
- csconfig throttle
- csconfig reinitialize
- duplicatetrace
- importtrace
- jbpSA
- jnbSA
- ltid
- manageClientCerts
- mklogdir
- nbauditreport
- nbcatsync
- NBCC
- NBCCR
- nbcertcmd
- nbcertupdater
- nbcldutil
- nbcloudrestore
- nbcomponentupdate
- nbcplogs
- nbcredkeyutil
- nbdb_admin
- nbdb_backup
- nbdb_move
- nbdb_ping
- nbdb_restore
- nbdb_unload
- nbdb2adutil
- nbdbms_start_server
- nbdbms_start_stop
- nbdc
- nbdecommission
- nbdelete
- nbdeployutil
- nbdevconfig
- nbdevquery
- nbdiscover
- nbdna
- nbemm
- nbemmcmd
- nbfindfile
- nbfirescan
- nbftadm
- nbftconfig
- nbgetconfig
- nbhba
- nbholdutil
- nbhostidentity
- nbhostmgmt
- nbhypervtool
- nbidpcmd
- nbimageshare
- nbinstallcmd
- nbjm
- nbkmiputil
- nbkmscmd
- nbkmsutil
- nboraadm
- nboradm
- nbpem
- nbpemreq
- nbmlb
- nbperfchk
- nbplupgrade
- nbrb
- nbrbutil
- nbregopsc
- nbreplicate
- nbrepo
- nbrestorevm
- nbseccmd
- nbsetconfig
- nbsnapimport
- nbsnapreplicate
- nbsqladm
- nbstl
- nbstlutil
- nbstop
- nbsu
- nbsvrgrp
- resilient_clients
- restoretrace
- stopltid
- tldd
- tldcd
- tpautoconf
- tpclen
- tpconfig
- tprext
- tpreq
- tpunmount
- verifytrace
- vltadm
- vltcontainers
- vlteject
- vltinject
- vltoffsitemedia
- vltopmenu
- vltrun
- vmadd
- vmchange
- vmcheckxxx
- vmd
- vmdelete
- vmoprcmd
- vmphyinv
- vmpool
- vmquery
- vmrule
- vmupdate
- vnetd
- vssat
- vwcp_manage
- vxlogcfg
- vxlogmgr
- vxlogview
- W2KOption
acsd

acsd – Automated Cartridge System (ACS) daemon (UNIX) or process (Windows)

SYNOPSIS

   acsd [-v]

On UNIX systems, the directory path to this command is
/usr/openv/volmgr/bin/

On Windows systems, the directory path to this command is
install_path\Volmgr\bin\n
DESCRIPTION

acsd interfaces with Media Manager to mount and unmount tapes automatically
that are under Automated Cartridge System (ACS) control. If the Media and Device
Management of the Administration Console shows drives in an ACS robot, the ltid
NetBackup Device Manager daemon or service (Windows) runs acsd. Stopping
ltid stops acsd.

On UNIX systems, start or stop acsd independently of ltid by using
/usr/openv/volmgr/bin/vmps or your server’s ps command to identify the acsd
process ID. Then enter the following commands:

   kill acsd_pid
   /usr/openv/volmgr/bin/acsd [-v] &

acsd performs its tasks by sending requests to the ACS storage server Interface
process (acsssi). It communicates with the server that controls the ACS.

On Windows systems, acsd performs its tasks by sending requests to the STK
LibAttach service, which communicates with the server that controls the ACS.

When the connection is established, acsd puts the ACS robot in the UP state and
can mount and unmount tapes. If the connection cannot be established or ACS
errors exist, acsd changes the robot to the DOWN state. In this state, acsd still runs
and returns the robot to the UP state when the problem no longer exists.

Use the following to address and define drives in the Media Manager: ACS number,
LSM number, Panel number, and Drive number.
Configure drive cleaning for ACS robots by using ACS library software. You cannot define the cleaning volumes by using Media Manager. In addition, you cannot use the `tpclean` command for cleaning operations on drives under ACS robotic control.

On UNIX systems, the Internet service port number for `acsd` must be in `/etc/services`. If you use NIS (Network Information Service), place the entry in this host's `/etc/services` file in the master NIS server database for services. The default service port number is 13702.

On Windows systems, the Internet service port number for `acsd` must be in `>%SystemRoot%\system32\drivers\etc\services`. The default service port number is 13702.

**Note:** This command applies only to the NetBackup Enterprise Server.

---

**OPTIONS**

`-v` This option is used on UNIX systems only. It logs debug information using `syslogd`. If you start `ltid` with `-v`, `acsd` also starts with `-v`.

---

**ERRORS**

On UNIX systems, `acsd` returns an error message if a copy of `acsd` is in operation. Media Manager logs ACS and network errors to `syslogd`. Log entries are also made when the state changes between UP and DOWN. `acsssi` logs to a log file in the `/usr/openv/volmgr/debug/acsssi` directory.

On Windows systems, Media Manager logs ACS and network errors to the Windows application event log. Log entries are also made when the state changes between UP and DOWN.

---

**SEE ALSO**

See `ltid` on page 549.

See `tpconfig` on page 892.
add_media_server_on_clients

add_media_server_on_clients – add media server on clients

SYNOPSIS

add_media_server_on_clients

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\

DESCRIPTION

Run the add_media_server_on_clients command from a NetBackup server to
synchronize the server list from the server’s configuration with the server lists on
the known clients.

The add_media_server_on_clients command tries to connect to all configured
clients (clients that are listed in backup policies).

For each client to which it can connect, add_media_server_on_clients updates
the client’s configuration (if necessary) to include all the servers from the server’s
configuration.
backupdbtrace

backupdbtrace – trace debug logs of backupdb (image catalog backup) jobs

SYNOPSIS

backupdbtrace [-server name] [-job_id number] [-start_time hh:mm:ss] [-end_time hh:mm:ss] mmddyy [mmddyy ...]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

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

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

- bpdbm on the master server
- bpcd on all servers

backupdbtrace uses the -job_id option as the sole criterion for selecting the backupdb job to trace. If -job_id is not used, then backupdbtrace selects all the backupdb jobs that started on the days that the day stamps (mmddyy) specified. Use the -start_time and -end_time options to examine the debug logs on the specified time interval.

The backupdbtrace utility writes error messages to standard error.

OPTIONS

-server

Name of the media server where the backupdb command is initiated. The default is the local host name.
-job_id
   Job ID number of the `backupdb` job to analyze. Default is any job ID.

-start_time
   Earliest timestamp to start analyzing the logs. Default is 00:00:00.

-end_time
   Latest timestamp to finish analyzing the logs. Default is 23:59:59.

mmddyy
   One or more day stamps. This option identifies the log file names (log.mmddyy
   for UNIX, mmddyy.log for Windows) to analyze.

OUTPUT FORMAT

The following is the format of an output line:

`daystamp.millisecs.program.sequence computer log_line`

`daystamp`
   The day that the log is generated in `yyyymmdd` format.

`millisecs`
   The number of milliseconds since midnight on the local computer.

`program`
   The name of the program (for example, BPBKAR) being logged.

`sequence`
   Line number within the debug log file.

`computer`
   The name of the NetBackup server or client.

`log_line`
   The line that appears in the debug log file.

EXAMPLES

Example 1 - Analyze the log of a `backupdb` job with job ID 5 that is run on May 6, 2013.

```
# backupdbtrace -job_id 5 050613
```

Example 2 - Analyze the log of all the `backupdb` jobs that were run on August 5, 2012 and August 17, 2013.

```
# backupdbtrace 080512 081713
```
**backuptrace**

**backuptrace** – consolidate the debug logs for a NetBackup job

**SYNOPSIS**

```bash
```

On UNIX systems, the directory path to this command is `/usr/openv/netbackup/bin/admincmd/`

On Windows systems, the directory path to this command is `install_path\NetBackup\bin\admincmd`

**DESCRIPTION**

The `backuptrace` utility consolidates the debug logs for specified NetBackup job or jobs. The debug log messages relevant to the specified backup jobs are written to standard output. Then the messages sort by time. The `backuptrace` utility tries to compensate for time zone changes and the clock drift between remote servers and clients. The output is formatted so that you can more easily sort or group by timestamp, program name, server name, or client name.

At a minimum, you must enable debug logging for the following:

- `nbjm` on the master server
- `bpbkr, bpbr, bpptm, and bpdm` on the media server
- `bpbkar` on the client

For best results, set the verbose logging level to 5 and enable debug logging for the following in addition to the processes already identified:

- `bpdbm` and `bprd` on the master server
- `bpcd` on all servers and clients

Use the `backuptrace` utility for regular file system, database extension, and alternate backup method backup jobs.
OPTIONS

-master_server name
   Name of the master server. Default is the local host name.

-job_id number
   Job ID number of the backup job to analyze.

-birth_time number
   Birth time (seconds since 1970) of the backup job to analyze.

-policy_name name
   Policy name of the jobs to analyze.

-client_name name
   Client name of the jobs to analyze.

-start_time hh:mm:ss
   Earliest timestamp to start analyzing the logs.

-end_time hh:mm:ss
   Latest timestamp to finish analyzing the logs.

mmddyy [mmddyy]
   One or more day stamps. This option identifies the log file names (log.mmddyy
   for UNIX, mmddyy.log for Windows) to analyze.

NOTES

Media Manager logs are not analyzed.

EXAMPLES

backuptrace -job_id 289 041105 > /tmp/job.log.289

backuptrace -policy_name weekly_bkups 051205 >/tmp/jobs.weekly_bkups

Use this utility to consolidate logs for all jobs that are started for the policy
weekly_bkups on the specified date. Use the -start_time/-end_time arguments
to limit the window for which the jobs are to be evaluated.
**bmrc**

*bmrc* — submit requests to the Bare Metal Restore server daemon

**SYNOPSIS**

```
bmrc -operation change -resource { restoretask | discovertask }
    [-client clientName] -state numericCode -progress numericCode

bmrc -operation complete -resource { restoretask | discovertask }
    [-client clientName] -state numericStateCode

bmrc -operation create -resource log [-client clientName]

bmrc -operation create -resource message [-client clientName] -msg messageText

bmrc -operation pull -resource { info | procedure }
    [-client clientName] -source sourceFileName -destination destinationFileName
```

On UNIX systems, the directory path to this command is

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

On Windows systems, the directory path to this command is

```
install_path\NetBackup\bin
```

**DESCRIPTION**

The *bmrc* client program runs on a Bare Metal Restore (BMR) client and submits requests to the BMR server daemon. The operation and resource are specified as arguments.

When you initiate *bmrc* from an external procedure in the repair environment on a restoring client, specify the path to the *bmrc* command as follows:

**On UNIX systems,**

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

**On Windows systems,**

```
%SystemDrive%\BMR\NBU\bin
```

On Windows systems, at the first boot external procedure point, *bmrc* is in

```
install_path\NetBackup\bin.
```
OPTIONS

-client clientName

Name of the Bare Metal Restore client.

On UNIX systems, -client is optional if CLIENT_NAME is defined in /
/usr/openv/netbackup/bp.conf on the client system.

-destination destinationFileName

On pull operation, the pathname of the file to be created on the local host.

-msg messageText

Text message to be added to the log on the server.

-operation operationName

An operation to perform:

change
complete
create
pull

-progress numericCode

A numeric progress code that is used internally by Bare Metal Restore.

-resource resourceName

A resource on which to perform the operation:

discovertask
info
log
message
procedure
restoretask

-source sourceFileName

On pull operation, name of file to retrieve from database.

-state numericCode

A numeric state code that is used internally by Bare Metal Restore.

EXAMPLES

Example 1 - Change the status of a discovery task:

# bmrc -operation change -resource discovertask -client clientName
   -state numericCode -progress numericCode
Example 2 - Change the status of a restore task:

```
# bmrc -operation change -resource restoretask -client clientName
   -state numericCode -progress numericCode
```

Example 3 - Complete a discovery task and set a final status code:

```
# bmrc -operation complete -resource discovertask -client clientName
   -status numericStatus
```

Example 4 - Complete a restore task and set a final status code:

```
# bmrc -operation complete -resource restoretask -client clientName
   -status numericStatus
```

Example 5 - Create a log on the server from standard input to this command:

```
# bmrc -operation create -resource log -client clientName
```

Example 6 - Create a message, which is added to a log on the server:

```
# bmrc -operation create -resource message -client clientName
   -msg message text
```

Example 7 - Pull a file from the server:

```
# bmrc -operation pull -resource info -client clientName
   -source sourceFileName -destination destinationFileName
```

Example 8 - Pull an external procedure from the server:

```
# bmrc -operation pull -resource procedure -client clientName
   -source sourceFileName -destination destinationFileName
```

NOTES

If you use NetBackup Access Management, and the user credentials and computer credentials expire, renew them before you perform prepare-to-restore operations. Use the `bpnbat -Login` command to renew your user credentials. Use the `bpnbat -LoginMachine` command to renew the computer credentials.

Specify `-?` to display the command’s usage statement when it is the only option on the command line.
bmrconfig

bmrconfig – change configuration settings

SYNOPSIS

bmrconfig -help [-resource resourceType [-platform win | hp | aix | solaris | linux] [-manager ldm | lvm | native | sfw | svm | vxvm | zfs] [-operation add | change | clearALL | delete | display | list | map]]

bmrconfig -operation verify -client clientName -configuration configName

bmrconfig -operation initialize -resource disk | network | device | all -client clientName -configuration configName -sourceconfiguration discovered_configName

bmrconfig -operation initialize -resource disk | network | device | all -client clientName -configuration configName -sourceclient source_clientName -sourceconfiguration source_configName

bmrconfig -operation initialize -resource driver -client clientName -configuration configName

bmrconfig -operation add | change | clearALL | delete | display | list | map -resource resourceType [-name resourceName] [-manager ldm | lvm | native | sfw | svm | vxvm] -client clientName -configuration configName [-attributes "key=value" ["key=value" ...]]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

The bmrconfig command changes the configuration of the system, network, volume, driver, and NetBackup settings. The read-only current configuration and discovered configuration cannot be changed. Use the bmrs command to create a copy of a configuration that you can change.
-attributes
Attributes of the resource are specified as name-value pairs. The name is always an alphanumeric string. The value is free form but must be double quoted if it contains white space or a shell-interpreted characters. To determine the specific set of attributes that apply to a resource, use `bmrconfig -operation list -resource resourceType`.

The following are some attributes specific to Solaris ZFS:

- `cache device` - Cache device if used.

- `copies number of copies` - applies only to the mirror layout

- `devtype` - The possible device types are the following:
  - `concat` - concatenation layout
  - `mirror` - mirror layout
  - `raidz1` - raidz1 layout
  - `raidz2` - raidz2 layout
  - `raidz3` - raidz3 layout

- `disk disk name` - Disk name to be used. Provide a disk name for every disk used.

- `log device` - Log device if used.

- `slice slice name` - Slice name to be used. Provide a slice name for every slice used.

- `spare` - spare device if used.

- `storagepool ZFS storage pool name` - Provides a ZFS storage pool name during ZFS and volume operations.

- `client clientName` - The NetBackup client name.

- `configuration configName` - The configuration to operate on.

- `force` - Forces the removal of a resource and all of its dependent resources.

- `initialize` - Initializes BMR configuration on a specified client.
-manager
The volume manager that controls the resource. Volume managers are as follows:

ldm - Windows Logical Disk Manager
lvm - AIX or HP-UX Logical Volume Manager
native - the volume manager native to the operating system
sfw - Veritas Storage Foundation for Windows
svm - Solaris Volume Manager
vxvm - Veritas Volume Manager
zfs - ZFS Volume Manager

-name resourceName
The name of the resource to act on. The various volume managers determine the valid characters in a resource name.

-operation operation_name
The operation to perform. Operations are as follows:

add - adds a resource to the configuration
change - changes specific attributes of a resource
clearALL - removes all resources except disks from a disk group
delete - removes a resource from the configuration
display - prints high-level information about the resource
help - prints the required resources and the optional attributes and values
initialize - initializes a configuration's hardware from a discovered configuration
list - prints all the instances of the specified resource type
map - maps a resource that includes dependent resources, from the original configuration to the working configuration
verify - checks that a config has sufficient data for a restore to succeed

-platform win | hp | aix | solars | linux
The platform of the specified resource. Used with -help only.

-resource resourceType
The type of the resource on which the operation is performed. Resource types are as follows:
all - all resources
accesspath - a Windows access path
disk - a physical storage device
diskgroup - a logical grouping of disks
diskset - a Solaris Volume Manager disk set
driveletter - a Windows drive letter
esm - backup client identity
filesystem - a file system for UNIX and Windows
gateway - a network gateway
host - a network server
hotfix - a Windows hotfix
hotsparepool - a set of the slices that are used for SVM failover
ip - network identity
license - a product license key
logicaldrive - a Windows extended partition; first one implicitly adds container
logicalvolume - an AIX or HP-UX logical volume
metadb - an SVM database replica slice
mountpoint - a path that serves as an access point to a volume
msd - a mass storage driver
multidevice - a Linux multidevice
nativedisk - Solaris Native disk resource
nativepart - Solaris Native partition resource
network - a sub network
nic - a network interface card
nicpkg - a network interface card driver
partition - Windows primary partition
physicalvolume - an AIX or HP-UX physical volume
slice - a Solaris slice; equivalent to volume
softpart - an SVM soft partition
volume - a logical division of a disk or a disk group
volumegroup - an AIX or HP-UX volume group
zfsfilesystem - ZFS file system
zfsstoragepool - ZFS storage pool
zfsvolume - ZFS volume

-sourceconfiguration source_configName
The configuration that is the source in an initialized configuration operation.

-sourceclient source_clientName
The client that serves as the source in an initialized configuration operation. If a source client is not specified, the configuration comes from the list of discovered configurations.

EXAMPLES

Example 1 - List the physical volumes in a configuration for client aixp31:

# bmrconfig -operation list -resource physical volume -configuration current -client aixp31

Example 2 - Map Native partitions on Solaris:

# bmrconfig -op map -re nativepart -name /dev/dsk/c1t0d0p1 -client client1 -config config1 -attributes disk=/dev/dsk/c1t0d0p0 percent=50 partid=191 active=true

Example 3 - List the volume groups in a configuration for client aixp31:

# bmrconfig -operation list -resource volume group -configuration current -client aixp31

Example 4 - Display the attributes of a volume group for client aixp31:

# bmrconfig -operation display -resource volume group -configuration current -client aixp31 -name rootvg

Example 5 - Initialize the new configuration with the discovered hardware for client aixp31:

# bmrconfig -operation initialize -resource config -configuration mynew -client aixp31 -sourceconfiguration discover

Example 6 - Add a volume group to a configuration for client aixp31:
# bmrconfig -operation add -configuration mynew -client aixp31
-resource volume group -name rootvg -attributes physical
volume=hdisk1

Example 7 - Add a disk to a volume group for client aixp31 (requires a full list of
physical volumes to be specified):

# bmrconfig -operation modify -configuration my new -client aixp31
-resource volume group -name rootvg -attributes physical
volume=hdisk1 physical volume=hdisk0

Example 8 - Remove a physical volume from a volume group for client aixp31:

# bmrconfig -operation modify -configuration my new -client aixp31
-resource volume group -name rootvg -attributes physical
volume=hdisk0

Example 9 - Map a volume group from the original configuration for client aixp31:

# bmrconfig -operation map -configuration my new -client aixp31
-resource volume group -name rootvg

Example 10 - On UNIX, map a ZFS storage pool set up in a mirrored layout that
provides three copies:

# bmrconfig -operation map -resource zfsstoragepool -client solbox
-config solconfig -namedatapool -attributes devtype=mirror copies=3
spare=/dev/dsk/clt1d0 cache=/dev/dsk/clt1d1 log=/dev/dsk/clt1d2
disk=/dev/dsk/clt1d3 disk=/dev/dsk/clt1d4

NOTES

If you use NetBackup Access Management, and the user credentials and computer
credentials expire, renew them before you perform prepare-to-restore operations.
Use the bpnbat -Login command to renew your user credentials. Use the bpnbat
-LoginMachine command to renew the computer credentials.

SEE ALSO

See bmrss on page 45.
bmrepadm

bmrepadm – manage external procedures

SYNOPSIS

bmrepadm [-data] -list [pattern]
bmrepadm [-data] -delete procedureName
bmrepadm [-data] -extract procedureName
bmrepadm [-data] -add fileName

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

The bmrepadm command lists, adds, extracts, or deletes external procedures from the database. The bmrepadm command is installed and runs on the NetBackup master server that is licensed for BMR.

A procedure name (procedureName) must be in the form procedureType.clientOs or clientName_procedureType.

procedureType is one of the following strings:

■ prediscover
■ preformat
■ prerestore
■ postrestore
■ firstboot

clientOs is one of following strings:

■ aix
■ hp
■ linux
■ sol
- win

name is the name of a Bare Metal Restore client.

OPTIONS

- **-add** *pathName*
  
  Adds the external procedure in *pathName* to the database. The last component of *pathName* must be a valid external *procedure Name*.

- **-data**
  
  Manipulates an arbitrary user-supplied data file instead of an external procedure. This option also relaxes all of the naming convention rules for procedure and file name argument values. The names of data files can be anything except a valid external procedure name.

- **-delete** *procedureName*
  
  Deletes the *procedureName* external procedure from the database. The *procedureName* must be a valid external procedure name.

- **-extract** *procedureName*
  
  Extracts an external procedure from the database and writes it to the current directory. The procedure name must be a valid external *procedureName*.

- **-list** [pattern]
  
  Lists the entries (external procedures or user-supplied data files) in the database. Only the entries that match the *pattern* are listed. If no *pattern* is specified, all entries in the database are listed. The "*" character may be used in the pattern to match a *procedureName*.

NOTES

*bmrepadm* does not validate client names. That is, you can add an external procedure for a nonexistent client.

If you use NetBackup Access Management and your user credentials and the computer credentials expire, renew them before you perform prepare-to-restore operations. Use the *bpnbat -Login* command to renew your user credentials and the *bpnbat -LoginMachine* command to renew the computer credentials.

Specify -? to display the command usage statement when it is the only option on the command line.

EXAMPLES

Example 1 - Add a data file:
# bmrepadm -data -add nameNotMatchingEPname

Example 2 - List the data files:

# bmrepadm -data -list

Example 3 - Add an external procedure that runs for all Solaris clients after the NetBackup restore phase of restoration:

bmrepadm -add pathname/postrestore.sol

Example 4 - Add an external procedure that runs before the disks are formatted on a client that is named zanzibar:

bmrepadm -add pathname/zanzibar_preformat
bmrprep

bmrprep – prepare a client for restore or discovery

SYNOPSIS

bmrprep -restore -client clientName -config configurationName -srt srtName [-policy policyName] [-logging] [-runep] [-systemonly] [-import] [-enddate enddate] [-quickformat]

bmrprep -discover -newconfig configurationName -srt srtName [-client clientName -config configurationName] -address clientAddress -default defaultGateway -netmask netmask -mac clientMacAddress -server nbuServerAddress -console consoleDeviceName -architecture architectureName [-gateway serverGateway] [-logging] [-runep]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

The bmrprep command prepares a Bare Metal Restore client for a restore or for a hardware discovery process. This command only runs on the Bare Metal Restore master server.

OPTIONS

-address clientAddress
(UNIX clients only.) IP address of the client, in dotted decimal notation. Required only for a -discover operation; optional if -client and -config options are specified.

-architecture architectureName
(UNIX clients only.) Architecture of the client to be discovered. Required only for a -discover operation; optional if -client and -config options are specified.

-client clientName
Name of the client to restore.
-config configurationName
  Name of the configuration to use.

-console consoleDeviceName
  (UNIX clients only.) Name of the console device to use during discovery.
  Required only for a -discover operation; optional if you specify the -client
  and -config options or use media boot.

-default defaultGateway
  (UNIX clients only.) Default gateway address, in dotted decimal notation.
  Required only for a -discover operation; optional if you specify the -client
  and -config options or use media boot.

-discover
  (UNIX clients only.) Perform a hardware discovery. Cannot be used with
  -restore.

-enddate enddate
  Date for point-in-time restores.
  The required date and time values format in NetBackup commands varies
  according to your locale. The /usr/openv/msg/.conf file (UNIX) and the
  install_path\VERITAS\msg\LC.CONF file (Windows) contain information such
  as the date-time formats for each supported locale. The files contain specific
  instructions on how to add or modify the list of supported locales and formats.
  For more information about the locale of your system, see the NetBackup
  Administrator’s Guide, Volume II.

-gateway serverGateway
  (UNIX clients only.) Gateway to a NetBackup server, in dotted decimal notation.
  Required only for a -discover operation.

-import
  Import non-system volume groups.
  For more information about how to use this flag, see the Bare Metal Restore
  Administrator’s Guide.

-logging
  Enable logging.

-mac clientMacAddress
  (UNIX clients only.) MAC address of the client. Required only for a -discover
  operation. (Exception: Optional if the IP address is configured during initial
  program load (IPL)); optional if you specify the -client and -config options
  or use media boot.
-netmask netmask
   (UNIX clients only.) Netmask of the client, in dotted decimal notation. Required only for a -discover operation; optional if -client and -config options are specified.

-newconfig configurationName
   (UNIX clients only.) Name to be given to the discovered configuration.

-policy policyName
   Name of the policy to be used.

-quickformat
   (Windows clients only.) Quickly formats Windows partitions.

-restore
   Performs a normal restore. Cannot be used with -discover.

-runep
   Runs external procedures.

-server nбуServerAddress
   (UNIX clients only.) A NetBackup server address, in dotted decimal notation. Required only for a -discover operation; optional if -client and -config options are specified.

-srt srtName
   Name of the shared resource tree to use.

-systemonly
   Restores system volume groups only.

   For more information about how to use this option, see "Prepare to Restore Client dialog box" in the Bare Metal Restore Administrator's Guide.

NOTES

If you use NetBackup Access Management and your user credentials and the computer credentials expire, renew them before you perform prepare-to-restore operations. Use the bpnbat -Login command to renew your user credentials and the bpnbat -LoginMachine command to renew the computer credentials.

You can specify -? to display the command usage statement when it is the only option on the command line.
**SYNOPSIS**

```
bmrs -operation delete -resource config -name configName -client clientName -resource client -name clientName -resource package -name packageName -resource srt -name srtName -resource discovertasklog -id idvalue -resource restoretasklog -id idvalue
```

```
bmrs -operation complete -resource discovertask -client clientName -status numericStatus -resource restoretask -client clientName -status numericStatus
```

```
bmrs -operation verify -resource srt -name srtName [-client clientName]
```

```
bmrs -operation copy -resource config -name configName -client clientName -destination newConfigName
```

```
bmrs -operation retrieve -resource config -client clientName -destination newConfigName [-enddate date] [-epochenddate eEnddate] [-policy policyName]
```

```
bmrs -operation import -resource config -path bundlePath [-client clientName] [-destination newConfigName]
```

```
bmrs -operation list -resource resourceName
```

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\

**DESCRIPTION**

The `bmrs` command manages resources in the Bare Metal Restore database. The `bmrs` command runs only on the master server.
OPTIONS

-client clientName
    Name of the Bare Metal Restore client.

-destination newConfigName
    Name of the destination configuration to create.

-enddate date
    The date for point-in-time restore configurations. If both -enddate and
    -epochenddate are specified, -epochenddate takes precedence.
    The required date and time values format in NetBackup commands varies
    according to your locale. The /usr/openv/msg/.conf file (UNIX) and the
    install_path\VERITAS\msg\LC.CONF file (Windows) contain information such
    as the date-time formats for each supported locale. The files contain specific
    instructions on how to add or modify the list of supported locales and formats.
    For more information about the locale of your system, see "About specifying
    the locale of the NetBackup installation" in the NetBackup Administrator's
    Guide, Volume II.

-epochenddate eEnddate
    The date for the point-in-time restore configurations. This date is specified in
    the number of seconds since January 1, 1970. If both -enddate and
    -epochenddate are specified, -epochenddate takes precedence.

-id idvalue
    Database record ID of the resource to use for this operation. It is either
    discoverTaskLogId or restoreTaskLogId.

-name value
    Name of the resource to use for this operation: clientName, configName,
    packageName, or srtName.

-operation operationName
    Possible operations are complete, copy, delete, import, list, retrieve, and verify.

-path bundlePath
    Pathname to a bundle file that the bmrsavecfg command creates.

-policy policyName
    Name of the policy to be used.

-resource resourceName
    A resource on which to perform the operation. The allowed resources vary with
    operation specified. For -operation list, the following resources are supported:
bootserver
client
config
discovertask
discovertasklog
package
restoretask
restoretasklog
srt

-status numericStatus
A numeric completion status code, used internally by Bare Metal Restore.

EXAMPLES

Example 1 - List the configurations in the BMR database:

bmrs -operation list -resource config

Example 2 - Copy the current configuration (read-only) and create a new configuration (mynew) that you can edit for client aixp31:

bmrs -operation copy -resource config -name current -client aixp31 -destination mynew

Example 3 - Delete configuration mynew for client aixp31:

bmrs -operation delete -resource config -name mynew -client aixp31

Example 4 - Verify the integrity of shared resource tree aixsrt:

bmrs -operation verify -resource srt -name aixsrt

NOTES

If you use NetBackup Access Management and your user credentials and the computer credentials expire, renew them before you perform prepare-to-restore operations. Use the bpnbat -Login command to renew your user credentials and the bpnbat -LoginMachine command to renew the computer credentials.

You can specify -? to display the command usage statement when it is the only option on the command line.

SEE ALSO

See bmrc on page 30.
**bmrsrtadm**

**bmrsrtadm** – create and manage SRTs and create bootable CD images

**SYNOPSIS**

`bmrsrtadm`

On UNIX systems, the directory path to this command is

`/usr/openv/netbackup/bin/`

On Windows systems, the directory path to this command is

`install_path\NetBackup\bin\`

**DESCRIPTION**

On UNIX systems, the **bmrsrtadm** command interactively manages shared resource trees.

On Windows systems, the **bmrsrtadm** command launches the Create Shared Resource Tree wizard.

Use **bmrsrtadm** on a BMR boot server (UNIX) or the Create Shared Resource Tree wizard on a BMR boot server (Windows) to do the following:

- Create a new shared resource tree.
- Create a bootable CD image that contains a copy of an existing shared resource tree.
- Install additional software into an existing shared resource tree.
- Copy an existing shared resource tree to a new location.
- Delete an existing shared resource tree.
- List available shared resource trees (UNIX).
- Enable and disable a shared resource tree for exclusive use (UNIX).

**NOTES**

UNIX: If you use NetBackup Access Management and your user credentials and the machine credentials expire, renew them before you perform prepare-to-restore operations. Use the **bnpbat -Login** command to renew your user credentials. Use the **bnpbat -LoginMachine** command to renew the machine credentials.
**bp**

bp – start NetBackup menu interface for users

**SYNOPSIS**

```
bp [-a | -ra | -b | -r | -rr | -o | -ro | -s | -rs | -i | -ri | -k
    | -rk | -rti | -p | -rp | -2 | -r2] [-verbose]
```

```
bp [ -b | -a | -r | -ra] [-verbose]
```

The directory path to this command is /usr/openv/netbackup/bin/

**DESCRIPTION**

This command operates only on UNIX systems.

The bp command starts a menu interface that lets users archive, back up, and restore files, directories, or raw partitions from their client workstations. You can run this interface from any character-based terminal (or terminal emulation window) where you have a termcap or a terminfo definition.

The bp online Help provides detailed operating instructions.

**OPTIONS**

The startup menu depends on the options that are used with the bp command. If you run the bp command without specifying an option, the utility starts at the main menu. To start the utility at a secondary menu, specify one of the following options:

- `-a` Starts bp in the Archive of Files and Directories menu.
- `-ra` Starts bp in the Restore Archives menu.
- `-b` Starts bp in the Backup of Files and Directories menu.
- `-r` Starts bp in the Restore Backups menu.
- `-rr` Starts bp in the Restore Raw Partitions Backups menu.
- `-o` Starts bp in the Backup Oracle DB menu.
- `-ro` Starts bp in the Restore Oracle DB menu.
-s  Starts bp in the Backup Sybase DB menu.
-rs  Starts bp in the Restore Sybase DB menu.
-i  Starts bp in the Backup Informix DB menu.
-ri  Starts bp in the Restore Informix DB menu.
-rti  Starts bp in the Restore True Image Backups menu.

Note that the following options apply only to the NetBackup Enterprise Server.

-p  Starts bp in the Backup SAP DB menu.
-rp  Starts bp in the Restore SAP DB menu.
-2  Starts bp in the Backup DB2 DB menu.
-r2  Starts bp in the Restore DB2 DB menu.
-k  Starts bp in the Backup SQL-BackTrack DB menu.
-rk  Starts bp in the Restore SQL-BackTrack DB menu.

-verbose  Provides a verbose response.

FILES

/usr/openv/netbackup/help/bp/*
/usr/openv/netbackup/logs/bp/*
/usr/openv/netbackup/bp.conf

SEE ALSO

See bparchive on page 51.
See bpbackup on page 57.
See bprestore on page 382.
bparchive

bparchive – archive files to the NetBackup server

SYNOPSIS

bparchive [-p policy] [-s schedule] [-L progress_log [-en]] [-S master_server [,master_server,...]] [-t policy_type] [-w [hh:mm:ss]] [-k "keyword_phrase"] [-utf8] -f listfile | filenames

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\

DESCRIPTION

bparchive processes the files that are listed on the command line or in the specified file, using the -f listfile option. Any file path that is entered can be a file name or a directory name. If the list of files includes a directory, it archives all files and subdirectories of that directory and starts at the directory itself.

By default, you return to the system prompt after bparchive is successfully submitted. The command works in the background and does not return completion status directly to you. Use the -w option to change bparchive to work in the foreground and to return completion status after a specified time period.

bparchive writes informative and error messages to a progress-log file if the file is created. Create the file before you run the bparchive command and specify it with the -L progress_log option. If bparchive cannot archive any of the requested files or directories, use the progress log to determine the reason for the failure.

If you create a directory with write access, bparchive creates a debug log file in this directory to use for troubleshooting.

On Windows systems, nbu_dir_path is install_path\NetBackup\logs\bparchive\

On UNIX systems, the directory is /usr/openv/netbackup/logs/bparchive/

NetBackup sends mail on the archive completion status to mail_address if USEMAIL = mail_address. It is entered as follows: non-administrator users specify it on the $HOME/bp.conf file; administrators specify it in the /usr/openv/netbackup/bp.conf file. This message is sent when the archive process is complete.
The following restrictions apply to this command:

- On UNIX systems: To archive a file with `bparchive`, you must be the root or the owner and a member of the primary group (as owner) to delete. Also, the file must not be read only. Otherwise, NetBackup saves the files but cannot reset their access time (`utime`) and does not delete them from the disk.

- On Windows systems, to archive a file with `bparchive`, you must have permission to delete the file and the file must not be read only. Otherwise, NetBackup saves the files but does not delete them from the disk.

- On UNIX systems: If you specify a UNIX file that is a link, `bparchive` archives only the link itself, not the file to which it links.

- `bparchive` does not archive the "." or "." directory entries, and does not archive disk-image backups.

**OPTIONS**

```bash
-f listfile
```

Specifies a file (`listfile`) that contains a list of files to be archived and can be used instead of the `filenames` option. In `listfile`, place each file path on a separate line.

The required file list format depends on whether the files have spaces, newlines, or returns in the names. To archive the files that do not have spaces or newlines or returns in the names, use the following format:

```
filepath
```

The path to the file you want to archive. Some examples on UNIX systems are: `~/home`, `~/etc`, and `~/var`. Some examples on Windows systems are: `c:\Programs` and `c:\documents\old_memos`

To archive the files that have spaces or newlines or returns in the names, use this format:

```
filepathlen filepath
```

`filepath` is the path to the file you want to archive and `filepathlen` is the number of characters in the file path.

Examples on UNIX systems are the following:
Examples on Windows systems are the following:

11 c:\Programs
8 c:\winnt
22 c:\documents\old memos

filenames
Names one or more files to be archived and can be used instead of the -f option. Any files that you specify must be listed at the end, after all other options.

-k keyword_phrase
Specifies a keyword phrase that NetBackup associates with the image created by this archive operation. You then can restore the image by specifying the keyword phrase with the -k option on the brestore command.

The keyword phrase is a textual description of the archive that is a maximum of 128 characters in length. All printable characters are permitted including space (" ") and period (".").

Enclose the phrase in double quotes ("...") or single quotes ('...').
The default keyword phrase is the null (empty) string.

-L progress_log [-en]
Specifies the name of an existing file in which to write progress information.
On UNIX systems, the file name must begin with /.
For example: netbackup/logs/user_ops/proglog
On Windows system, an example is NetBackup\logs\user_ops\proglog

The default is to not use a progress log.
Include the -en option to generate a progress log that is in English. The name of the log contains the string _en. This option is useful to support personnel in a distributed environment where different locales may create logs of various languages.

Only default paths are allowed for this option and Veritas recommends using the default paths. If you cannot use the NetBackup default path in your setup, you should add custom paths to the NetBackup configuration.
For more information on how to add a custom path, see the “BPCD_WHITELIST_PATH option for NetBackup servers and clients” topic in the NetBackup Administrator’s Guide, Volume I.

\textit{-p policy}

Names the policy to use for the user archive. If it is not specified, the NetBackup server uses the first policy it finds that includes the client and a user archive schedule.

\textit{-S master_server}

On UNIX systems, this option specifies the name of the NetBackup master server. The default is the first \texttt{SERVER} entry in the \texttt{/usr/openv/netbackup/bp.conf} file.

On Windows systems, this option specifies the name of the NetBackup master server. The default is the server designated as current on the Servers tab of the Specify NetBackup Machines dialog box. To display this dialog box, start the Backup, Archive, and Restore user interface on the client. Then click Specify NetBackup Machines on the File menu.

\textit{-s schedule}

Names the schedule to use for the user archive. If it is not specified, the NetBackup server uses the first user archive schedule it finds in the policy it currently uses. (See the \textit{-p} option.)

\textit{-t policy_type}

Specifies one of the following numbers that correspond to the policy type. The default for Windows clients is 13. The default for all others is 0:

\begin{itemize}
  \item 0 = Standard
  \item 4 = Oracle
  \item 6 = Informix-On-BAR
  \item 7 = Sybase
  \item 13 = MS-Windows
  \item 15 = MS-SQL-Server
  \item 16 = MS-Exchange-Server
  \item 19 = NDMP
  \item The following policy types apply only to NetBackup Enterprise Server:
  \item 11 = DataTools-SQL-BackTrack
  \item 17 = SAP
  \item 18 = DB2
\end{itemize}
20 = FlashBackup
21 = Split-Mirror
39 = Enterprise-Vault

-utf8

This option tells NetBackup that the file list that is provided is in UTF-8 format. With this option, NetBackup does not try to convert the path names. The option has no effect for non-Windows platforms or for other policy types.

For some policy types, NetBackup on Windows assumes that the input file list is formatted in the active code page (ACP). It converts each path specification from the ACP to UTF-8. The option applies to any backups that are initiated from the command line on Windows, for the following policy types:

DB2
MS-Exchange-Server
Lotus-Notes
Oracle
SAP
MS-SQL-Server
Sybase
MS-Windows

-w [hh:mm:ss]

Causes NetBackup to wait for a completion status from the server before it returns you to the system prompt.

The required date and time values format in NetBackup commands varies according to your locale. The /usr/openv/msg/.conf file (UNIX) and the install_path\VERITAS\msg\LC.CONF file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

See the "About specifying the locale of the NetBackup installation" topic in the NetBackup Administrator's Guide, Volume II.

You can optionally specify a wait time in hours, minutes, and seconds. The maximum wait time you can specify is 23:59:59. If the wait time expires before the archive is complete, the command exits with a timeout status. The archive, however, still completes on the server.

If you use -w without specifying the wait time or if you specify a value of 0, NetBackup waits indefinitely for the completion status.
EXAMPLES

Example 1 - Archive a single file:

**UNIX systems:** `bparchive /usr/user1/file1`

**Windows systems:** `bparchive c:\usr\user1\file1`

Example 2 - Archive the files that are listed in a file that is named `archive_list`:

`bparchive -f archive_list`

Example 3 - Associate keyword phrase "Archive My Home Directory 02/02/10" to the archive of a directory named `kwc` and use a progress log that is named `arch.log`:

**UNIX systems:**

```
bparchive -k "Archive My Home Directory 02/02/10" \
-L /usr/openv/netbackup/logs/user_ops/arch.log /home/kwc
```

**Windows systems:**

```
barchive -k "Archive My Home Directory 02/02/10" \
-L c:\Program Files\Veritas\NetBackup\logs\user_ops\arch.log \
c:\home\kwc
```
bpbackup

bpbackup – back up files to the NetBackup server

SYNOPSIS

bpbackup -f listfile | filenames [-p policy] [-s schedule] [-S master_server...] [-t policy_type] [-L progress_log [-en]] [-w [hh:mm:ss]] [-k "keyword_phrase"] [-utf8]

bpbackup -i [-p policy] [-h hostname {[-instance instance_name [-database database_name]] | [-database_unique_name name -database_id id]} [-s schedule] [-S master_server...] [-t policy_type] [-L progress_log [-en]] [-w [hh:mm:ss]] [-k "keyword_phrase"] [-utf8]

bpbackup -dssu DSSUname [-S master_server]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

The bpbackup command can start a backup process on clients and master servers. When you use an Oracle policy, bpbackup lets you back up an instance or a RAC database. When you use a SQL Server policy, bpbackup lets you back up an instance or a database in an instance.

On clients:

The -f option of bpbackup starts a user backup equivalent to what is performed by using the interface on the client. This type of backup can be started from any NetBackup client to back up files from that client.

bpbackup processes the files that you list on the command line or in the file that you specify with the -f listfile option. A file path can be a file name or a directory name. If the named files include a directory, bpbackup backs up all files and subdirectories of that directory; it starts at the directory itself.
Note: In addition to listing individual files or directories, bpbackup can also use directives to indicate the files to be backed up. For example: bpbackup "/Shadow Copy Components/" or bpbackup "/System State/". Clients can enter the directive in the listfile using the bpbackup -f listfile option.

On master servers:
The -i option of bpbackup starts an immediate manual backup of a client. The bpbackup option is available only to the administrator on the master server. It is equivalent to when you start a manual backup from the NetBackup Administration Console. Use the -h option to specify the host.

Because progress logs are written only on clients and this form of bpbackup is run from the master server only, the -L option is undefined.

The following restrictions apply to this command:

- You must be the owner of the file or an administrator to back up a file with bpbackup.
- You can back up files and the directories that other users own if you have the necessary permissions.
- On UNIX systems: If you specify a file that is a link, bpbackup backs up only the link itself, not the file to which it links.
- bpbackup does not back up the "." or ".." directory entries.

By default, you return to the system prompt after bpbackup is successfully submitted. The command works in the background and does not return completion status directly to you. The -w option lets you change this behavior so the command works in the foreground. It returns completion status after a specified time period.

If you create the file before you run the bpbackup command and then specify the file with the -L progress_log option, the following occurs: bpbackup writes informative and error messages to a progress-log file. If bpbackup cannot back up the requested files or directories, use the progress log to determine the reason for the failure.

Note: The -L option is not supported for NDMP clients.

If you create the following directory with public-write access, bpbackup creates a debug log file in the directory that you can use for troubleshooting:

On Windows systems: install_path\NetBackup\logs\bpbackup\n
On UNIX systems: usr/openv/netbackup/logs/bpbackup/
NetBackup sends mail on the backup completion status when the backup process is complete to *mail_address* when users specify the following:

- A nonroot user specifies `USEMAIL = mail_address` in the `$HOME/bp.conf` file
- A root user specifies `USEMAIL = mail_address` in the `/usr/openv/netbackup/bp.conf` file

**OPTIONS**

- `-database_id`
  The database id of the Oracle RAC database specified in the policy.

- `-database_unique_name`
  The unique name of the Oracle RAC database specified in the policy.

- `-dssu DSSUname`
  NetBackup immediately runs the schedule that is associated with the disk staging storage unit. The `-i` option is the implied behavior and is not necessary.

- `-f listfile`
  Specifies a file (*listfile*) that contains a list of files to back up. You can use this option instead of the `filenames` option, but you cannot use it with the `-i` option. List each file on a separate line.

  The format that is required for the file list depends on whether the files have spaces, newlines, or returns in the names.

  To back up the files that do not have spaces, newlines, or returns in the names, use the following format:

  `filepath`

  Where *filepath* is the path to the file you want to back up.

  On UNIX systems, examples are `/home`, `/etc`, and `/var`.

  On Windows systems, examples are `c:\Programs`, `c:\winnt`, and `c:\documents\old_memos`.

  To back up the files that have spaces, newlines, or returns in the names, use the following format:

  `filepathlen filepath`

  Where *filepath* is the path to the file you want to back up and *filepathlen* is the number of characters in the file path.
Examples on UNIX systems are the following:

5 /home
4 /etc
4 /var
19 /home/abc/test file

Examples on Windows systems are the following:

11 c:\Programs
8 c:\winnt
22 c:\documents\old memos

filenames
Names one or more files to back up. You can use this option instead of the -f option, but you cannot use it with the -i option. You must list any files that you specify at the end, following all other options.

-h hostname
Names the client host on which to run the backup. If it is not specified, NetBackup runs the backup on all clients in the policy.

-i
Starts an immediate manual backup. This operation is equivalent to starting a manual backup from the NetBackup administrator interface. You must be the administrator on the master server to use the -i option.

-instance instance_name [-database database_name]
 Specifies the name of an Oracle or SQL Server instance that you want to back up. The policy type (-t) must be set to 4 (Oracle) or 15 (SQL Server). You must use this option with the -h option, and you must be the administrator on the master server.

[-database database_name] specifies the name of a SQL Server database in an instance that you want to back up.

-k keyword_phrase
Specifies a keyword phrase that NetBackup associates with the image that this backup operation creates. You then can restore the image by specifying the keyword phrase with the -k option on the bprestore command.

If you use the -i option with -k, NetBackup establishes an association between the keyword phrase and the backup policy and image.

The keyword phrase is a textual description of the backup that is a maximum of 128 characters in length.
On UNIX systems, all printable characters are permitted including space (" ") and period ("."), Enclose the phrase in double quotes ("...") or single quotes ('...') to avoid conflict with the UNIX shell.

On Windows systems, all printable characters are permitted including space (" ") and period ("."), Enclose the phrase in double quotes ("...") or single quotes ('...').

The default keyword phrase is the null (empty) string.

-L progress_log [-en]
Specifies the name of a file in which to write progress information. NetBackup creates the file if it does not exist.

On Windows systems, for example: NetBackup\logs\user_ops\proglog

On UNIX systems, for example: netbackup/logs/user_ops/proglog

The default is not to use a progress log.

The -L option is not supported for NDMP clients.

Include the -en option to generate a progress log that is in English. The name of the log contains the string _en. This option is useful to support personnel in a distributed environment where different locales may create logs of various languages.

Only default paths are allowed for this option and Veritas recommends to use the default paths. If you cannot use the NetBackup default path in your setup, you should add custom paths to the NetBackup configuration.

For more information on how to add a custom path, see the “BPCD_WHITELIST_PATH option for NetBackup servers and clients” topic in the NetBackup Administrator’s Guide, Volume I.

-p policy
Names the policy to use for the backup.

If this option is not specified, NetBackup uses the first policy it finds that includes the client and a user backup schedule.

This option is required for an immediate-manual backup (-i option).

-s schedule
Names the schedule to use for the backup. If it is not specified, the NetBackup server uses the first user backup schedule it finds for the client in the policy currently in use.

See the -p option.
-S master_server [,master_server,...]

On UNIX systems, -S specifies the name(s) of the NetBackup master server(s). The default is the first SERVER entry that is found in the /usr/openv/netbackup/bp.conf file.

On Windows systems, -S specifies the name(s) of the NetBackup master server(s). The default is the server designated as current on the Servers tab of the Specify NetBackup Machines dialog box. To display this dialog box, start the Backup, Archive, and Restore user interface on the client. Then click Specify NetBackup Machines on the File menu.

-t policy_type

Specifies one of the following numbers that correspond to the policy type. The default for Windows clients is 13, and the default for all others is 0:

0 = Standard
4 = Oracle
6 = Informix-On-BAR
7 = Sybase
8 = MS-SharePoint
13 = MS-Windows
15 = MS-SQL-Server
16 = MS-Exchange-Server
19 = NDMP

Note that the following policy types apply only to the NetBackup Enterprise Server.

11 = DataTools-SQL-BackTrack
17 = SAP
18 = DB2
20 = FlashBackup
21 = Split-Mirror
39 = Enterprise-Vault
44 = BigData
-utf8

This option tells NetBackup that the file list that is provided is in UTF-8 format. With this option, NetBackup does not try to convert the path names. The option has no effect for non-Windows platforms or for other policy types.

For some policy types, NetBackup on Windows assumes that the input file list is formatted in the active code page (ACP). It converts each path specification from the ACP to UTF-8. The option applies to any backups that are initiated from the command line on Windows, for the following policy types:

DB2
MS-Exchange-Server
Lotus-Notes
Oracle
SAP
MS-SQL-Server
Sybase
MS-Windows

-w [hh:mm:ss]

Causes NetBackup to wait for a completion status from the server before it returns you to the system prompt.

You can optionally specify a wait time in hours, minutes, and seconds. The maximum wait time you can specify is 23:59:59. If the wait time expires before the backup is complete, the command exits with a timeout status. The backup, however, still completes on the server.

The `bpbackup -w` option causes the shell to wait for a return code. The operating system shell can only return one return code. Therefore, if you use `-w` without specifying a wait time or you specify a value of 0, NetBackup waits indefinitely for the completion status.

You can start a manual or an administrative backup using `bpbackup -i` along with the `-w` function. This type of backup has the potential to start multiple jobs because it is based on policy attributes. If the manual backup starts multiple jobs, the `-w` function still only returns one return code to the shell.

If you use `-i` with `-w` and more than one job begins, NetBackup waits until all jobs complete before it returns a completion status. However, because NetBackup only returns one status code to the shell, the job ID that the status code belongs to is unknown.

If multiple jobs are due to multiple clients and Allow Multiple Data Streams is not selected, use `-h` to restrict the operation to one client. However, if Allow Multiple Data Streams is selected in the policy and the selected client has multiple jobs, the returned status code is again unknown.
EXAMPLES

Example 1 - Perform a user backup of a single file.

On UNIX systems: # bpbackup /usr/user1/file1

On Windows systems: # bpbackup c:\users\user1\file1

Example 2 - Start a user backup of the files that are listed in a file that is named backup_list.

# bpbackup -f backup_list

Example 3 - Start an immediate-manual backup (all on one line) of the client host named diablo in the policy named cis_co. The policy type is Standard policy and is in the configuration on the master server named hoss.

UNIX: # bpbackup -p cis_co -i -h diablo -S hoss -t 0

Windows: # bpbackup -p cis_co -i -h diablo -S hoss -t 0

Example 4 - On Windows systems: Associate the keyword phrase "Backup My Home Directory 01/01/01" to the user backup of the directory C:\home\kwc. (Enter the command on one line.)

# bpbackup -k "Backup My Home Directory 01/01/01" -L c:\Program Files\Veritas\NetBackup\logs\user_ops\bkup.log \ C:\home\kwc

On UNIX systems: The following command associates the keyword phrase “Backup Home Dir 01/01/01” to the user backup of the directory /home/kwc. (Enter the command on one line or use the backslash continuation character.)

# bpbackup -k "Backup Home Dir 01/01/01" -L /usr/openv/netbackup/logs/user_ops/bkup.log \ /home/kwc

Example 5 - Associate the keyword phrase “Policy Win 01/01/01” to the immediate-manual backup of the client host named slater in the policy named win_nt_policy. (Enter the command all on one line.)

UNIX:

# bpbackup -k "Policy Win 01/01/01" -i -h slater \ -p win_nt_policy -t 13

Windows:

# bpbackup -k "Policy Win 01/01/01" -i -h slater -p win_nt_policy -t 13
Example 6 - Perform a manual backup of the Oracle instance `orac11g` on client host `hookvm2` by using the `ora` policy.

```bash
# bpbackup -i -p ora -h hookvm2 -t 4 -instance orac11g
```

Example 7 - Perform a manual backup of the SQL Server database `HRDB1` in instance `HR` on client host `winvm2` by using the `sql` policy.

```bash
# bpbackup -i -p sql -h winvm2 -t 15 -instance HR -database HRDB1
```

**FILES**

UNIX systems: `$HOME/bp.conf`

`/usr/openv/netbackup/logs/bpbackup/log.mmddyy`

Windows systems: `install_path\NetBackup\logs\bpbackup\*.log`

**SEE ALSO**

See `bp` on page 49.

See `bparchive` on page 51.

See `bplist` on page 215.

See `bprestore` on page 382.
bpbackupdb

bpbackupdb – initiate a hot catalog backup

SYNOPSIS

bpbackupdb -p policy_name -s sched_label

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

bpbackupdb initiates a hot catalog backup using the specified policy and schedule.

See the "About specifying the locale of the NetBackup installation" topic in the
NetBackup Administrator's Guide, Volume II.

See the NetBackup Administrator's Guide, Volume II for more information on how
to back up NetBackup catalogs. The NetBackup utility bprecover recovers the
catalogs that bpbackupdb has backed up.

See the NetBackup Troubleshooting Guide for more information on how to restore
the NetBackup catalogs if a disaster recovery is required.

OPTIONS

-p policy_name -s sched_label

The -p and -s options launch a policy-based, hot catalog backup.
bpcatarc

bpcatarc – back up the NetBackup catalog

SYNOPSIS

bpcatarc [-version] [-remove_dotf]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

bpcatarc processes the output of bpcatlist to back up the selected catalog image .f files and update their image file’s catarc field with this backup job ID.

OPTIONS

-version
   Displays the bpcatarc version and exit.

-remove_dotf
   Removes the .f files for an archived image immediately so that you do not need to run bpcatrm.

SEE ALSO

See bpcatlist on page 68.
See bpcatres on page 71.
See bpcatrm on page 72.
bpcatlist

bpcatlist – list selected parts of NetBackup catalog

SYNOPSIS

bpcatlist [-server server_name] [-client client_name] [-since [ctime |
[-since-days nnn | -since-weeks nnn | -since-months nnn | -before-days nnn | -before-weeks nnn | -before-months nnn]] [-before [ctime | [-since-days nnn | -since-weeks nnn | -since-months nnn | -before-days nnn | -before-weeks nnn | -before-months nnn]] [-date ctime] [-policy policy_name] [-sched sched_name] [-id backup_id] [-catarc catarc_id] [-version] [-online | -offline]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

bpcatlist is the starting point for all catalog archiving operations. Use bpcatlist to select the specific parts of the NetBackup catalog with which you want to work. All files-file (image .f files), the largest files in a NetBackup catalog, that are selected for bpcatarc, bpcatres, or bpcatrm, are first selected with bpcatlist. The output of bpcatlist is piped to the action you want to perform.

OPTIONS

-server server_name
   Indicates the name of the NetBackup server. Default: server_name is the first server name listed in the bp.conf file.

-client client_name
   Creates a list of backup images for client_name. Default: client_name is CLIENT_NAME in bp.conf or the current host name.

   To select all clients, use -client all.
-since [ctime | [-since-days nnn | -since-weeks nnn | -since-months nnn | -before-days nnn | -before-weeks nnn | -before-months nnn]]
Lists backup images since the specified time that is expressed in ctime (for example, Fri Oct 12 00:00:00 2012).
If no year is specified, bpcatlist uses the current year by default.
The following command lists all images after December 31, 2012:
bpcatlist -since 2012

Additional examples are found in the Examples section.

-before [ctime | [-since-days nnn | -since-weeks nnn | -since-months nnn | -before-days nnn | -before-weeks nnn | -before-months nnn]]
Lists backup images before the specified time that is expressed in ctime (for example, Fri Oct 12 00:00:00 2012). If no year is specified, bpcatlist uses the current year by default.

-date ctime
Lists of backup images for the specified date that is expressed in ctime (for example, Fri Oct 12 00:00:00 2012). If no date is specified, bpcatlist uses the current date by default.
Additional examples are found in the Examples section.

-catarc catarc_id
Lists the files-file that were archived with the specified catarc_id. For example:
-catarc 1022754972

-policy policy_name
Lists the backups that the indicated policy_name for the specified client creates.

-sched sched_name
Lists the backups that are created following schedule_name for the specified client.

-id backup_id
Creates a list for the specified backup_id.

-online
Lists only files-file that are online.

-offline
Lists only files-file that are offline.

-version
Displays the bpcatlist version and exit.
EXAMPLES

Displayed dates must be specified in ctime (for example, Fri Mar 16 00:00:00 2012) date format. Displayed dates may be cut and specified without modification.

Example 1 - List a backup for a specific date and time.

# bpcatlist -date Mon Aug 19 14:16:28 2013

Example 2 - List all backups between the two specified dates of the current year. When no year is specified, the current year is used by default.

# bpcatlist -since Fri Jul 5 00:00:00 -before Mon Aug 2 00:00:00

Example 3 - List the backups that are two to three months old.

# bpcatlist -before-months 2 -since-months 3

-since and -before use the following equivalent values:

-since-days nnn
-since-weeks nnn
-since-months nnn
-before-days nnn
-before-weeks nnn
-before-months nnn

For example, the setting -since-days 14 is equivalent to -since-weeks 2.

SEE ALSO

See bpcatarc on page 67.
See bpcatres on page 71.
See bpcatrm on page 72.
bpcatres

bpcatres  – restore NetBackup catalog

SYNOPSIS

bpcatres [-version]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

bpcatres processes the output of bpcatlist to restore the selected catalog image .f files.

OPTIONS

-version

Displays the bpcatres version and exits.

SEE ALSO

See bpcatarc on page 67.
See bpcatlist on page 68.
See bpcatrm on page 72.
bpcatrm

bpcatrm – delete NetBackup catalog

SYNOPSIS

bpcatrm [-version]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

bpcatrm processes the output of bpcatlist or bpcatarc to delete the selected
catalog image .f files that have a valid catarc ID in their image file.

OPTIONS

-version

  Displays the bpcatrm version and exits.

SEE ALSO

See bpcatarc on page 67.
See bpcatlist on page 68.
See bpcatres on page 71.
**bpcd**

*bpcd* – NetBackup client daemon. Enables the NetBackup clients and servers to accept requests from NetBackup servers.

**SYNOPSIS**

```
```

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is `install_path\NetBackup\bin`.

**DESCRIPTION**

On Windows systems, **`bpcd`** is a communications daemon that the NetBackup Client Service **`bpinetd`** activates. Normally, **`inetd`** activates **`bpcd`** on UNIX systems.

The **`bpcd`** daemon accepts requests from NetBackup servers. Requests include the following:

- Initiate backup and restore jobs
- Get NetBackup configuration parameters
- Set NetBackup configuration parameters

When you install NetBackup on a client, the installation process typically adds entries for **`bpcd`** to the following:

- **UNIX client:** /etc/services and /etc/inetd.conf
- **Windows client:** %SystemRoot%\system32\drivers\etc\services

The **`services`** entry looks like the following:

```
bpcd 13782/tcp bpcd
```

The **`inetd.conf`** entry on UNIX systems looks like the following:

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

The following options are available only on UNIX clients and imply that the
-standalone option is active.

-debug
Prevents bpcd from forking and does not disconnect it from standard input,
output, and error.

-keyfile
When -keyfile is specified, you are prompted for the NetBackup pass phrase
that lets bpcd access the NetBackup encryption key file.

For more information, see "Additional key file security" in the NetBackup Security
and Encryption Guide.

-portnum number
Specifies the port number where bpcd listens for requests. The default is the
bpcd entry in: /etc/services.

-standalone
Instructs bpcd to run continuously rather than requiring inetd to start
NetBackup. -standalone is the default condition for NetBackup startup.

-terminate
Stop the NetBackup Client Service (bpcd).

SEE ALSO

See bpclient on page 79.

See bpkeyfile on page 207.
**bpchangeprimary**

bpchangeprimary – promote a copy of a backup to be the primary copy

**SYNOPSIS**

```
bpchangeprimary -copy number | -pool volume_pool | -group volume_group
[-id backup_id] [-M master_server]
```

```
bpchangeprimary -copy number | -pool volume_pool | -group volume_group
```

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
**DESCRIPTION**

The `bpchangeprimary` command lets you change which copy is the primary copy for a set of backup images. You can choose the copy to be promoted to primary by specifying a copy number, volume pool, or volume group. You can apply several optional criteria to identify the backup images to be affected.

The primary copy of a backup is the copy used by a restore process. Ensure that the primary copy is accessible for restore. For instance, if one copy of a backup was sent off site, change the primary copy to be the copy that remains on site.

The `bpchangeprimary` command finds all backups that match the specified criteria and updates their copy number to primary. If you use the `-copy` option, the specified copy number becomes the primary copy. If you use the `-group` or `-pool` option, the process identifies all media IDs that belong to the specified volume group or volume pool. It then changes all copies that reside on those media to primary.

**OPTIONS**

One and only one of the following three options is required:

- `copy number`
  
  Specifies the number of the backup copy you want to promote to primary.
-pool volume_pool
  Specifies that the copy on the media that belongs to volume_pool is to be promoted to primary.

-group volume_group
  Specifies that the copy on the media that belongs to volume_group is to be promoted to primary.

You can apply combinations of one or more of the following optional criteria to specify which copies are made primary.

-cl client_name
  Specifies that backups of client_name are affected. This name must be as it appears in the NetBackup catalog. For those backup images, this option promotes the copy that corresponds to the specified -pool, -group, or -copy option to primary. The default is all clients.

-sd date time, -ed date time
  Specifies the start date (-sd) or end date (-ed) of the backup images for which the primary copy is changed.

  The required date and time values format in NetBackup commands varies according to your locale. The /usr/openv/msg/.conf file (UNIX) and the install_path\VERITAS\msg\LC.CONF file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

  For more information about the locale of your system, see "About specifying the locale of the NetBackup installation" in the NetBackup Administrator's Guide, Volume II.

  The default start date is January 1, 1970, which effectively causes a search for all images. If you run bpchangeprimary without using the -sd option, you are prompted to confirm that you want to change the primary copy for the backups that were created after January 1, 1970. The default end date is the current date. The valid range of dates is from 01/01/1970 to 01/19/2038.

-id backup_id
  Specifies the backup ID of the backup image for which the primary copy is changed. For that backup image, -id backup_id changes the copy that corresponds to the specified -pool, -group, or -copy option.

  If you specify -id, you can use the -M option to name an alternate master server. Specify -pool, -group, or -copy.

-kw keyword
  Specifies a keyword phrase for NetBackup to use when you identify backup images for which the primary copy is changed.
-M master_server
   Specifies that the backups that belong to master_server are affected. For those
   backup images, -M master_server promotes the copy that corresponds to
   the specified -pool, -group, or -copy option to primary.

   If you use this option, any other options you specify determine which backup
   images on the specified master server are affected. The server must allow
   access by the system that issues the bpchangeprimary command. The default
   is the master server for the system that runs the bpchangeprimary command.

-pn policy_name
   Specifies the name of the backup policy of the backups for which the primary
   copy is changed. The default is all policies.

-pt policy_type
   Specifies the type of the backup policies of the backups for which the primary
   copy is changed. The default is all policy types. The policy_type is one of the
   following character strings:

   Auspex-FastBackup
   BigData
   DataStore
   DataTools-SQL-BackTrack
   DB2
   Enterprise-Vault
   FlashBackup
   FlashBackup-Windows
   Hyper-V
   Informix-On-BAR
   LotusNotes
   MS-Exchange-Server
   MS-SharePoint
   MS-SQL-Server
   MS-Windows
   NDMP
   Oracle
   PureDisk-Export
   SAP
   Split-Mirror
   Standard
   Sybase
   Vault
   VMware
-sl schedule_name
   Specifies the schedule name (label) for the selection of the backup images for which the primary copy is changed. By default, the bpchangeprimary command uses all schedules.

-st schedule_type
   Specifies the schedule type for the selection of the backup images for which the primary copy is changed. By default, bpchangeprimary uses any schedule type. Valid values are as follows:
   
   FULL (full backup)
   INCR (differential-incremental backup)
   CINC (cumulative-incremental backup)
   UBAK (user backup)
   UARC (user archive)
   NOT_ARCHIVE (all backups except user archive)

EXAMPLES

Example 1 - Promote all copies on the media that belongs to the volume pool SUN that are created after 08/01/2012 to be the primary copy.

# bpchangeprimary -pool SUN -sd 08/01/2012

Example 2 - Promote copy 2 of all backups of client, oak, created after 01/01/2012 to be the primary copy:

# bpchangeprimary -copy 2 -cl oak -sd 01/01/2012

Example 3 - Promote copy 4 of all backups that the backup policy Offsite created after 08/01/2011 to be the primary copy:

# bpchangeprimary -copy 4 -pn Offsite -sd 08/01/2011
bpclient

bpclient – manage client entries on a master server

SYNOPSIS

bpclient -All [-M master_server] [-l | -L | -H]

bpclient -client client_name [-M master_server] [-l | -L | -H]

bpclient -client client_name [-M master_server] -add | -update
[ -dynamic_address 0|1] [-free_browse 0|1|2] [-list_restore 0|1|2|3]
[ -max_jobs 1-99] [-current_host host_name] [-online] [-offline
[ [-ut] -onlineat time]] | [-online_backup] | [-offline_backup
[ [-ut] -online_backup_at time]] | [-online_restore] | [-offline_restore
[ [ -ut] -online_restore_at time]] | [-WOFB_enabled 0|1] [-WOFB_FIM 0|1]
[ -WOFB_usage 0|1] [-WOFB_error 0|1] [-connect_options 0|1|2 0|1|2
0|1|2|3] [-granular_proxy granular_proxy_host] [-client_direct 0|1|2]
[ -client_direct_restore 0|1|2]

bpclient -client client_name [-M master_server] -delete

bpclient -client client_name -add_alias alias_name | -delete_alias
alias_name [-M master_server]

bpclient -client client_name -add_all_aliases | -delete_all_aliases
| -list_all_aliases [-M master_server]

bpclient -policy policy_name -validate -fi

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The bpclient command describes how a NetBackup server connects to NetBackup clients.
**OPTIONS**

- **add**
  Adds a new client entry.

- **add_alias | -delete_alias alias_name**
  Adds a new entry for a client alias or deletes an existing client alias entry.

- **add_all_aliases | -delete_all_aliases | -list_all_aliases**
  Does one of the following:
  - **-add_all_aliases** adds a new entry for every client alias.
  - **-delete_all_aliases** deletes all aliases.
  - **-list_all_aliases** outputs a list of all alias entries.

- **All**
  Lists all client entries. Only the client entries appear that are added explicitly by using the `bpclient` command.

- **-client client_name**
  Specifies the name of the client to list or update.

- **-client_direct 0 | 1 | 2**
  Client Direct improves backup performance by using the OpenStorage storage server instead of the media server to transfer data to the client. The `-client_direct` option setting determines if and when the client uses this feature. The following settings are possible:
  0 = Never use Client Direct as the data transfer method on the specified host. Always use the normal data transfer method. This setting is the default condition.
  1 = Prefer to use Client Direct. Probes for the Client Direct capabilities on the storage server that is identified during the backup. If the probe passes, NetBackup uses the Client Direct data transfer method on the specified client. If the probe fails, is uses the normal data transfer method.
  2 = Always use Client Direct. Tries to use only the Client Direct method with the specified client. If this method fails for any reason, the job fails. No other transfer method is tried.

- **-client_direct_restore 0 | 1 | 2**
  Client Direct Restore improves restore performance by using the OpenStorage storage server instead of the media server to restore data to the client. The `-client_direct` option setting determines if and when the client uses this feature. The following settings are possible:
0 = Never use Client Direct Restore as the data transfer method on the specified host. Always use the normal data transfer method. This setting is the default condition.

1 = Prefer to use Client Direct Restore. The command probes for Client Direct Restore capabilities on the storage server that is identified during the restore. If the probe passes, NetBackup uses the Client Direct Restore data transfer method on the specified client. If the probe fails, it uses the normal data transfer method.

2 = Always use Client Direct Restore. Tries to use only the Client Direct Restore method with the specified client. If this method fails for any reason, the job fails. No other transfer method is tried.

-connect_options 0|1|2 0|1|2 0|1|2|3

This option applies only to the client names that are local to the NetBackup server that makes the connection.

First set of arguments, Ports, represents the following:

0 = Reserved Port: Use a reserved port number.

1 = Non-reserved Port: Connect to the client’s bpcd by using a non-reserved port number. If you select this option, enable Allow Nonreserved Ports for the selected client.

2 = Use Default: Use Default is the default. Use the value that the DEFAULTCONNECT_OPTS configuration entry on the server defines.

The second set of arguments, BPCD Connect Back, represents the following:

0 = Random Port: NetBackup randomly chooses a free port in the allowed range to perform the traditional connect-back method.

1 = VNETD port: This method does not require a connect-back to a random port. The connect-back is to the Network Daemon (vnetd) instead. The Network Daemon was designed to enhance firewall efficiency with NetBackup during server-to-server and server-to-client communications.

2 = Use Default: The default option. Use the value that the DEFAULT_CONNECT_OPTIONS configuration entry on the server defines.

The third set of arguments (Daemon Connection Port) represents the following:

0 = Automatic: This option means that VNETD is used if possible; otherwise Legacy is used.

1 = Use the VNETD port.

2 = Use the Legacy port number.
3 = Use Default: The default option. Use the value that the DEFAULT_CONNECT_OPTIONS configuration entry on the server defines.

**Note:** If the vnetd Daemon Connection Port is used, the BPCD Connect Back setting is not applicable. If the vnetd Daemon Connection Port is used, non-reserved ports are always used regardless of the value of the Ports setting.

- **-current_hostname host_name**
  The current host name of the client. This option is meaningful only when the option -dynamic_address 1 is used. Usually, you do not have to enter a -current_hostname value. The client normally contacts the master server to set the host name and the IP address.

- **-delete**
  Deletes an existing client entry.

- **-dynamic_address 0 | 1**
  0 = The client name is assumed to be a valid host name for the client (default).
  1 = The client is assumed to have a dynamic host name (such as DHCP).

- **-fi**
  Validates the -snapshot_method_args options on the bpplinfo command. See -validate option.

- **-free_browse 0 | 1 | 2**
  A method that allows users to get around the checking that the server does when it browses images (owner or group). By default, normal users are not allowed to browse into scheduled backups on Windows.
  0 = Allow
  1 = Deny
  2 = Use
  By default, both the client and the server should be set up to 0 (allow). To browse freely, either the client or the server must be set up to 2 (use). Neither can be set up for 1 (deny).

- **-granular_proxy granular_proxy_host**
  Specifies the Windows granular proxy host for a source client. You can use this option when you duplicate backup images that are enabled by the Granular Recovery Technology (GRT).

- **-H**
  Lists host-specific client information.
-l

Lists the limited client information.

-L

Lists all client information in a VERBOSE format.

-list_restore 0 | 1 | 2 | 3

Sets up on the server to disallow list and restore requests from a particular client. The value in the client database overrides the bp.conf file setting.

0 = Not specified (default)
1 = Allow both list and restore requests
2 = Allow list requests only
3 = Deny both list and restore requests

-M master_server

Name of the master server that contains the client entries. The first server name in the local configuration is the default master server.

-max_jobs [1-99]

The maximum number of jobs up to 99 that are allowed to run concurrently on this client. You can configure this item in the NetBackup Administration Console. It is labeled "Maximum data streams." To perform this function by using this GUI, select the following: Host Properties > Master Servers > (double-click the master server name) > Client Attributes.

-online | -offline

Sets the client state to online or offline for both backups and restores.

-onlineat time

Sets the client state to online for both backups and restores at the time specified.

-online_backup | -offline_backup

Set the client state to online or offline for backup.

-online_backup_at time

Sets the client state to online for backup at the time specified.

-online_restore | -offline_restore

Set the client state to online or offline for restore.

-online_restore_at time

Sets the client state to online for restore at the time specified.
-policy policy_name
   Specifies the name of the backup policy to validate. This option is used with
   the -validate and -fi options.

-update
   Updates an existing client entry.

-ut
   Specifies the time in UNIX time.

-validate
   When using NetBackup commands to create a snapshot-based policy such
   as VMware or Hyper-V, this option validates the policy. To validate a policy
   that is created with the bpplinfo -snapshot_method_args command,
   -validate must be used with the -fi option.

   For more information on using NetBackup commands to create a VMware or
   Hyper-V policy, see the NetBackup for VMware Guide or the NetBackup for
   Hyper-V Guide.

-WOFB_enabled 0|1
   0 = disables Windows Open File Backup for the client that is specified in
   client_name.
   1 = enables Windows Open File Backup for the client that is specified in
   client_name.

-WOFB_error 0 | 1
   0 = Abort Backup on Error. Specifies that a backup aborts if it fails for a
   snapshot-related issue after the snapshot is created and while the backup uses
   the snapshot to back up open or active files on the file system.
   1 = Disable Snapshot and Continue. Specifies that if the snapshot becomes
   invalid during a backup, the volume snapshots for the backup are destroyed.
   The backup continues with Windows Open File Backups disabled.

-WOFB_FIM 0 | 1
   0 = Use Volume Snapshot Provider (VSP) as the snapshot provider for the
   Windows Open File Backups. VSP is supported only on the clients that use
   NetBackup Release 6.x. Clients that use NetBackup Release 7.x only use
   VSS. If you run a Release 7.x client and select VSP with this option, NetBackup
   automatically runs VSS instead.
   1 = Use Microsoft’s Volume Shadow Service (VSS) as the snapshot provider
   for Windows Open File Backups.
-WOFB_usage 0|1

0 = Individual Drive Snapshot. Specifies that the snapshot be of an individual drive. When this property is enabled, snapshot creation and file backup are done sequentially on a per volume basis.

1 = Global Drive Snapshot. Specifies that the snapshot is of a global drive. The snapshots are taken at one time for all the volumes that require snapshots for the backup job (or stream group for multistreamed backups).

EXAMPLES

Example 1 - Determine if the client hagar is in the client database on the master server:

```
# bpclient -client hagar -L
```

Example 2 - Add casper to the client database on the master server. It also allows a maximum of five concurrent jobs to be run on casper.

```
# bpclient -client casper -add -max_jobs 5
```

Example 3 - List all client information verbosely for client ollie.

```
# bpclient -client ollie -L
```

Client Name: ollie

Current Host:

  Hostname: ollie
  IP Address: 0.0.0.0

Dynamic Address: no

Free Browse: Allow

List Restore: Not Specified

Max Jobs This Client: Not Specified

WOFB Enabled: yes

WOFB FIM: VSP

WOFB Usage: Individual Drive Snapshot

WOFB Error Control: Abort on Error

Client Direct: Prefer to use client-side deduplication or Prefer to move data direct to storage

Client Direct Restore: Move data via media server

OST Proxy: Off

OST Proxy Server: Unspecified

Connect options: 2 2 3
bpclimagelist

bpclimagelist – produce status report on client NetBackup images or removable media

SYNOPSIS


On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

The bpclimagelist command generates status reports on client NetBackup images or removable media.

Note: For the NetBackup Accelerator feature, bpclimagelist can report the amount of data that was transferred over the network for each backup. You must configure the command to show the transferred data in the field that normally shows the Accelerator backup image size. For details, see the Accelerator topics in the NetBackup Administrator's Guide Volume I, the NetBackup for VMware Administrator's Guide, and the NetBackup for NDMP Administrator's Guide.

OPTIONS

-client client_name
   Specifies the client on which a status report is to be generated.

-ct client_type
   Displays only the images that are backed up for a specified client type. The client_type is specified as an integer. If -ct is not specified, the default value is standard (0). Valid values are as shown:

   0 - standard (typical for UNIX file system backups)
NetBackup Commands

bpclimagelist

4 - Oracle DB
6 - Informix DB
7 - Sybase DB
8 - Sharepoint
13 - Windows (typical for Windows file system backups)
15 - SQL Server
16 - Exchange
17 - SAP
18 - DB2
19 - NDMP
20 - Flash Backup
21 - Split Mirror
29 - FlashBackup-Windows
30 - Vault
34 - Disk Staging
35 - NetBackup Catalog
39 - Enterprise Vault

-e mm/dd/yyyy hh:mm:ss
Specifies an end date and time for the listing. See the description of the -s option that follows.

-keyword keyword_phrase
Specifies a keyword phrase for NetBackup to use when it searches. The phrase must match the phrase that was previously associated with the image.

-Likelydate
Searches for a useful timestamp that marks the start of backup images to use for a restore. Usually, this timestamp is the time of the last full backup image. With no other arguments, this option returns the decimal number of seconds since January 1, 1970.

-Listseconds
Specifies that the timestamp is shown in seconds granularity.

-policy policy_name
Reports on the backup images that use the specified policy. The default is any policy.
-oracle_copilot_ir
   Searches for and displays the images that may be used for Oracle Copilot Instant Recovery.

-s mm/dd/yyyy hh:mm:ss, -e mm/dd/yyyy hh:mm:ss
   Specifies the start date (-s) and end date (-e) for the listing.

   The -s option specifies a start date and time for the listing. The resulting list shows only files in backups or the archives that occurred at or after the specified date and time.

   The required date and time values format in NetBackup commands varies according to your locale. The /usr/openv/msg/.conf file (UNIX) and the install_path\VERITAS\msg\LC.CONF file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

   For more information about the locale of your system, see "About specifying the locale of the NetBackup installation" in the NetBackup Administrator’s Guide, Volume II.

   The valid range of dates is from 01/01/1970 00:00:00 to 01/19/2038 03:14:07. The default is the current date minus 6 months.

   The -e option specifies an end date and time for the listing. The resulting list shows only files from the backups or the archives that occurred at or before the specified date and time. Use the same format for start date and time. The default is the current date and time.

-server server_name
   Indicates the name of the NetBackup server. The default value is the first server name listed in the bp.conf file.

-t
   Specifies a schedule type for the image selection. The default is any schedule type. Valid values, in either uppercase or lowercase, are as follows:

   ■ FULL (full backup)
   ■ INCR (differential-incremental backup)
   ■ CINC (cumulative-incremental backup)
   ■ UBAK (user backup)
   ■ UARC (user archive)
   ■ ANY
   ■ NOT_ARCHIVE (all backups except user archive)
-U

User display format.
bpclntcmd

bpclntcmd – test functionality of a NetBackup system and enable Fibre Transport services on a NetBackup client

SYNOPSIS


On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\

DESCRIPTION

The bpclntcmd command tests the functionality of a NetBackup system and displays information about it. It also enables and disables the Fibre Transport services on a NetBackup client.

OPTIONS

-check_vxss

Checks if NBAC is configured correctly on the local system.

-check_vxss_with_host hostname

Checks if NBAC is configured correctly on the local system to connect to the remote host hostname.

-clear_host_cache

NetBackup caches host name to IP address mappings to minimize DNS lookups. Each NetBackup process typically has its own in-memory cache and
all the processes also share a cache that is stored on the file system. This option removes all the entries in the shared cache on the file system.

If host names/IP addresses have recently been updated on DNS or other host lookup services, the NetBackup caches may be out of sync for up to an hour. To ensure that NetBackup is in sync with host name changes, you can do the following: Stop NetBackup, run `bpclntcmd -clear_host_cache`, then restart NetBackup.

- `get_fqdn hostname`
  Returns the fully qualified domain name for the specified `hostname`.

- `gethostname`
  Returns the host name that NetBackup uses on the local system.

- `get_local_client_patch_version`
  Returns the version of the local client patch software.

- `get_local_dn`
  Returns the domain name of the local host.

- `get_local_fqdn`
  Returns the fully qualified domain name of the local host.

- `get_local_server_patch_version`
  Returns the version of the local server patch software.

- `get_local_sn`
  Returns the short host name of the local host.

- `get_pbx_port hostname`
  Displays the number that `hostname` considers the PBX port number. If `hostname` is not specified, the option displays the number that the local host considers the PBX port number.

- `get_remote_host_version hostname`
  Returns the version of NetBackup that is running on the system that is identified in the `hostname` variable.

- `hn hostname`
  Returns the host name, alias, and IP address information about the host name that is identified in the `hostname` variable.

- `ip ip_address`
  Returns the host name, alias, and IP address information about IP address, `ip_address`.

- `is_emm_server hostname`
  Checks if `hostname` is operating as the EMM server on the local system.
-is_local_host hostname
  Checks if hostname is a network interface on the local system.

-is_master_server hostname
  Checks if hostname is the master server on the local system.

-is_media_server hostname
  Checks if hostname is a media server on the local system.

-is_server hostname
  Checks if hostname is a master server or a media server on the local system.

-is_trusted_master hostname
  Checks if hostname is a trusted master server on the local system.

-pn [-verbose]
  Returns what the master server considers your host name (or peer name) to be.
  Use the -verbose option to return how the master server sees the connecting host: Source IP address and port number, host name to which the IP resolves, and policy client for that host name. The -verbose option shows additional connection details including the host certificates that NetBackup uses to authenticate the hosts.

-refresh_use_at
  For a NetBackup media server, queries the master server for the NetBackup Enhanced Auditing authentication setting (USE_AUTHENTICATION) and updates the local cache with said setting. By default, NetBackup updates the authentication cache setting on media servers hourly.

-reverse_name_lookup [allowed | restricted | prohibited]
  Determines if NetBackup can use the reverse name lookup of the host name-IP. Use of this function can be allowed, prohibited, or restricted.

-sanclient [ 0 | 1 ]
  0 - Disables the client Fibre Transport (FT) service. The command returns a NetBackup SAN client to normal client functionality.
  1 - Enables the client FT service, which effectively turns a regular NetBackup client into a SAN client.

-self
  Returns the information about the local system.

-server NBU_master
  Returns the host name information of the NetBackup master server.
-sv

Returns the NetBackup version of the master server.

SEE ALSO

See `bpnbat` on page 242.
bpclusterutil

bpclusterutil – Modify and configure NetBackup in a cluster.

SYNOPSIS

bpclusterutil [-np] [-s [NBU|OC]] [-online] [-offline] [-freeze]
[-unfreeze] [-startagent] [-stopagent] [-addSvc "ServiceName"]
[-deleteSvc "ServiceName"] [-enableSvc "ServiceName"] [-disableSvc
"ServiceName"] [-iscluster] [-isactive] [-vname] [-sharedpath]
[-addIP -virtualIP "IPString" [-prefixLength "PrefixLength"| -subnet
"SubnetMask"]]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\

DESCRIPTION

This command modifies and configures NetBackup in a cluster. It is available on
NetBackup master and media servers.

On Windows, this command sets up the registry entries that are used for cluster
configuration and then to configure the cluster. This command only modifies registry
entries on the local node.

OPTIONS

-addIP

Adds a new virtual IP resource to the existing NetBackup cluster group. The
option uses the same network interface card (NIC) that was configured at initial
cluster configuration. In the case of WSFC cluster, ensure that the NetBackup
group is offline before you use the option. On a UNIX platform, this option is
only supported for VCS.

The parameters that are shown are required for the addIP option:

- virtualIP "IPString" Specifies the virtual IP address you want to add.
prefixLength "PrefixLength" When the virtualIP specified is an IPv6 address, you must use prefixLength to specify the prefix length. Please note that prefixLength and subnet are mutually exclusive.

subnet "SubnetMask" When the virtualIP specified is an IPv4 address, you must use subnet to the subnet mask for the IP address. Please note that prefixLength and subnet are mutually exclusive.

-addSvc "Service Name"
Add a NetBackup service to the NetBackup cluster group.

-deleteSvc "ServiceName"
Deletes an existing NetBackup service from the NetBackup cluster group. Ensure that ServiceName is provided within double quotes. For example, "NetBackup Key Management Service" for the key management service.

-disableSvc "ServiceName"
Disables monitoring of a NetBackup service by the cluster.

-enableSvc "ServiceName"
Enables the cluster to monitor a NetBackup service you added to the NetBackup cluster group.

-freeze
Freezes the NetBackup cluster group. This option is available on UNIX systems only.

-isactive
Displays the state of the NetBackup cluster group on the node. A return code of 1 indicates that the node is the active node. A return code of 0 indicates that the node is an inactive node.

-iscluster
Displays the cluster status of NetBackup.

-np
Places the operation in silent mode (no print).

-offline
Issues the offline command to the NetBackup group in the cluster.

-online
Issues the online command to the NetBackup group in the cluster.

-s [NBU | OC]
Selects the clustered server type. The possible values are NBU (NetBackup) and OC (Add-onProductShortName1);.
Displays the shared path of the clustered server.

Starts the NetBackup Cluster Server (VCS) agent.

Stops the NetBackup VCS agent.

Unfreezes the NetBackup cluster group. This option is available on UNIX systems only.

Displays the virtual name of the NetBackup cluster group. This option is available on UNIX systems only.

**EXAMPLES**

To add a virtual IPV4 resource to cluster group run the command shown:

```
bpclusterutil -addIP -virtualIP 10.210.91.56 -subnet 255.255.252.0
```

To add a virtual IPV6 resource to cluster group run the command shown:

```
bpclusterutil -addIP -virtualIP 2620:128:f0a1:9003::15d -prefixLength 64
```
bpcompatd

bpcompatd – run NetBackup compatibility service

SYNOPSIS

bpcompatd [-max_time seconds] [-console] [-debug]
bcompatd -alive [-debug]
bcompatd -terminate [-debug]
bcompatd -bpcd_connect clientname [-debug]
bcompatd -bpdbm_connect hostname [-debug]
bcompatd -bpjobd_connect hostname [-debug]
bcompatd -bprd_connect hostname [-debug]
bcompatd -robot_connect hostname robot_type [-debug]
bcompatd -vmd_connect hostname [-debug]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is \install_path\NetBackup\bin\n
DESCRIPTION

This command is used internally by new NetBackup services to communicate with legacy NetBackup services.

OPTIONS

-alive

Tests the local bpcompatd daemon or service to see if it is running.

-bpcd_connect clientname

Tests a bpcd connection to clientname by using the bpcompatd command.

-bpdbm_connect hostname

Tests a bpdbm connection to hostname by using the bpcompatd command.
-bpjobd_connect hostname
Tests a bpjobd connection to hostname by using the bpcompatd command.

-bprd_connect hostname
Tests a bprd connection to hostname by using the bpcompatd command.

If you specify -debug, the information that is normally logged in the debug log file of bpcompatd is written to standard error.

If you do not specify one of these options, bpcompatd runs as a daemon (for UNIX) or a service (for Windows). The following options are available when you run bpcompatd as a daemon or service:

-console
This option is applicable to Windows only. Normally, bpcompatd is run through the Service Manager. You can use the -console option to run the bpcompatd service from the command line.

-debug
If you specify -debug, the information that normally is logged on the debug log file of bpcompatd is written to standard error. For Windows, this option implies the -console option. On UNIX systems, this option prevents the bpcompatd service from running in the background.

-max_time seconds
The maximum time bpcompatd waits for a new connection before it performs routine tasks. The default is 60 seconds on UNIX systems. The default is one second on Windows systems.

-robot_connect hostname robot_type
Tests a robot daemon connection to hostname for robot_type by using the bpcompatd command.

Valid robot types include the following:

NONE - Not robotic
ACS - Automated Cartridge System
TLD - Tape Library DLT

-terminate
Terminates the local bpcompatd daemon or service if it is running.

-vmd_connect hostname
Tests a vmd connection to hostname by using the bpcompatd command.
bpconfig

bpconfig – modify or display global configuration attributes for NetBackup

SYNOPSIS

bpconfig [-cd seconds] [-ha hours] [-kl days] [-kt days] [-ma [address]] [-sto seconds] [-mj number] [-period hours] [-prep hours] [-to seconds] [cleanup_int hours] [cleanup_wait minutes] [-tries times] [-wi minutes] [-pui minutes] [-v] [-M master_server,...]

bpconfig [-L | -l | -U [-v] [-M master_server,...]]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The bpconfig command modifies or displays the NetBackup global configuration attributes. These attributes affect operations for all policies and clients. With the exception of the NetBackup administrator’s email address, the default values for these attributes are adequate for most installations.

See "About specifying the locale of the NetBackup installation" in the NetBackup Administrator’s Guide, Volume II.

For implications of setting the attribute values, see NetBackup Global Attributes in the NetBackup Administrator’s Guide, Volume I.

The following describes the two forms of bpconfig:

- The first form of bpconfig modifies one or more of the NetBackup global configuration attributes. At least one option that changes a NetBackup global configuration attribute must be on the command line.
- The second form of bpconfig displays the current settings of the NetBackup global configuration attributes. See DISPLAY FORMATS for more detail.

Errors are sent to stderr. A log of the command activity is sent to the NetBackup admin log file for the current day.
OPTIONS

-cd seconds
   Specifies the number of seconds that is the Compress Catalog Interval. When seconds is an integer, an image compresses after this number of seconds has elapsed since the creation of the image. The range of values is 86400 to 2147472000. The default is zero (0), which means no compression is done.

   Use the bimage command to decompress the images.

-cleanup_int hours
   Specifies the minimum period of time (in hours) that can elapse without a catalog cleanup. The default value is 12 (hours). Since cleanup cannot run during a catalog backup, large 24x7 environments that run long catalog backups may need a shorter cleanup interval (e.g., three hours). Regardless of the value of this option, the image database is automatically cleaned up at the end of a session of scheduled backups.

   This option appears in the output display as Image DB Cleanup Interval (see examples).

-cleanup_wait minutes
   Specifies the interval (in minutes) between image database catalog cleanup operations. The default value is 60 (minutes). If multiple backups occur during this cleanup wait interval, NetBackup only initiates one cleanup operation in this time period. The range of values is zero (0) to 720.

-ha hours
   Specifies the number of hours ago that is the beginning of the time range for selecting NetBackup report entries. The end of the time range is the current time. For example, if hours ago is 24 and if you request a Backup Status report at 10:00 a.m., the report includes the following: All backups that ran from 10:00 a.m. yesterday until 10:00 a.m. today.

   This value is used to calculate the time range for general reports and media reports. General reports include Backup Status, Client Backups, Problems, and All Log Entries. Media reports include Media List, Media Summary, Media Contents, Images on Media, and Media Log Entries.

   Hours Ago is a positive integer in the range of 1 to 32767. The default value is 24 (hours).

-kl days
   The number of days to keep logs. This number determines how long the NetBackup master server keeps its Error database and debug logs.

   NetBackup derives its Backup Status, Problems, All Log Entries, and Media Log Entries reports from the Error database.
This value limits the period that these reports can cover. The range of values is 1 to 24855. The default is 28 days. A value of zero (0) turns logs off.

**Note:** This attribute has no effect on remote media servers or clients (remote media servers apply only to NetBackup Enterprise Server).

```
-kt days
```

The number of days to Keep True-image-recovery (TIR) data. This value determines how long to keep TIR information for those policies that specify the collection of TIR information. The range of values is 1 to 24855. The default is one (1) day. A value of zero (0) turns off the TIR information.

```
-L
```

The list type is long. See the section DISPLAY FORMATS for more detail.

```
-l
```

The list type is short. This option is the default if the command line has no list-type option (for instance, if you enter `bpconfig` and a carriage return). See the section DISPLAY FORMATS for more detail.

```
-M master_server,...
```

The master server where the global configuration attributes reside.

```
-ma [address]
```

The mail address for the NetBackup administrator. NetBackup sends notification of failed automatic backups, the manual backup operations that the administrator directs, and automatic database backups to this email address. The default is NULL (no email address).

If no address is provided, the current setting of the Admin Mail Address is cleared. Notification is not sent by email to the NetBackup administrator.

```
-mj number
```

Specifies the maximum jobs per client. This number is the maximum number of jobs that a client can perform concurrently. It must be a positive integer. The range values are 1 to 32767. The default value is 1.

```
-period hours
```

The time interval that is associated with the configured number of tries for a backup (see `-tries`). This interval is the period in hours during which NetBackup tries a backup job for a client/policy/schedule combination for as many tries as configured. The hours must be a positive integer. The range values are 1 to 24. The default value is 12 hours.

**Note:** This attribute does not apply to user-directed backups and archives.
-prep hours

Specifies the preprocessing interval. This interval is the minimum time in hours between client queries to discover new paths when NetBackup uses auto-discover-streaming mode.

The default Preprocess Interval value is four (4) hours. If the preprocessing interval changes, change it back to the default by specifying -prep -1. The preprocessing interval can be set to preprocess immediately by specifying 0 as the preprocess interval for auto discovery on the bpconfig command line. The maximum Preprocessing Interval is 48 hours.

For more information, see the NetBackup Administrator's Guide, Volume I.

-pui minutes

Specifies the policy update interval, which is how often NetBackup policy updates are processed. The default value is 10 minutes. The range of values is 1 to 1440 (minutes).

-sto seconds

The multihosted-media-mount timeout. This timeout is the time in seconds that NetBackup waits for a shared medium to be mounted, positioned, and ready on backups and restores. Use this timeout to eliminate excessive waits if another server uses a shared medium. The default is 0, which means no timeout (unlimited wait time).

For more details about multihosted drives, see the NetBackup Administrator's Guide, Volume I.

-to seconds

Specifies the media-mount timeout. This timeout is the time in seconds that NetBackup waits for the requested media to be mounted, positioned, and ready on backups and restores. Use -to to eliminate excessive waits when you need to mount media manually (for example, when robotic media is out of the robot or off site).

The default is 0, which means no timeout (unlimited wait time). If seconds is not 0, its value range is 1 to 32,767 seconds.

-tries times

The number of retries for a backup during the configured time period (see -period). For a given combination of client, policy, and schedule, NetBackup tries to run a backup job the specified number of times. This option limits the number of backup tries if repeated failures occur.

Note: This attribute does not apply to user-directed backups and archives.
Values for `-tries` range from 1 to 32767. The default is two tries. If defaults are used for both `-tries` and `-period`, NetBackup tries the backup two times in 12 hours.

-`U`

The list type is user. See DISPLAY FORMATS for more detail.

-`v`

Selects verbose mode for logging. This option is meaningful only if it runs with the debug log function on. Therefore, the following directory must be defined:

On UNIX systems: `/usr/openv/netbackup/logs/admin`

On Windows systems: `install_path\NetBackup\logs\admin`

-`wi minutes`

Job Retry Delay. Specifies how often NetBackup retries a job. The default value is 10 minutes. The range of values is 1 to 1440 (minutes).

### DISPLAY FORMATS

`bpconfig` uses the following three different formats to display the current values of the NetBackup global configuration attributes:

- **User Display Format (U)**

  The NetBackup graphical user interface uses this display format. This option produces a list with one global attribute per line. Each line has the form `global attribute descriptor: value`. This list is similar to the `-L` format, except that the global attribute descriptors are more explicit.

  The following is an example of the user display format:

  ```
  # bpconfig -U
  Admin Mail Address:     
  Job Retry Delay:       1 minutes
  Max Simultaneous Jobs/Client: 1
  Backup Tries:          2 time(s) in 12 hour(s)
  Keep Error/Debug Logs: 28 days
  Max drives this master: 0
  Keep TrueImageRecovery Info: 1 days
  Compress DB Files:      (not enabled)
  Media Mount Timeout:   0 minutes (unlimited)
  Display Reports:       24 hours ago
  Preprocess Interval:   0 hours
  Image DB Cleanup Interval: 12 hours
  Image DB Cleanup Wait Time: 60 minutes
  Policy Update Interval: 10 minutes
  ```
Long Format (-L)

If the command line contains -L, the display format is long. This option produces a list with one global attribute per line, in the format global attribute descriptor: value. The fields are as follows:

The following example shows the long format:

```
# bpconfig -L
Mail Admin: *NULL*
Job Retry Delay: 1 minutes
Max Jobs/Client: 1
Backup Tries: 2 in 12 hours
Keep Logs: 28 days
Max drives/master: 0
Compress DB Files: (not enabled)
Media Mnt Timeout: 0 minutes (unlimited)
Shared Timeout: 0 minutes (unlimited)
Media Int Timeout: 0 minutes (unlimited)
Display Reports: 24 hours ago
Keep TIR Info: 1 days
Prep Interval: 0 hours
DB Clean Interval: 12 hours
DB Clean Wait Time: 60 minutes
Policy Update Interval: 10 minutes
```

Short Format (-l)

If the `bpconfig` command line contains -l or contains no list-format option, the display format is short, which produces a terse listing. This option is useful for the scripts or the programs that rework the list into a customized report format. The list layout is a single line that contains the values for all global attributes. The time units follow the attributes in parentheses for the attributes that are expressed in units of time. The attributes appear in the following order with blanks between them:

The following is an example of the short format:

```
# bpconfig -l
*NULL* 1 12 1 2 28 0 0 0 0 1 24 1 0 2 10 60
```

The display fields for the -l display are interpreted as follows:

- NetBackup administrator email address has not been set.
- Job Retry Delay is 1 minute.
- Time period is 12 hours.
- Maximum simultaneous jobs per client is 1.
- Tries per period is 2.
- Keep logs for 28 days.
- Maximum drives this master is 0.
- Compress Catalog Interval is 0 seconds; 0 denotes no compression.
- Media mount timeout is 0 seconds; 0 denotes unlimited.
- Multihosted-media-mount timeout is 0 seconds; 0 denotes unlimited.
- Postprocess images flag is 1 (immediate).
- Display reports from 24 hours ago.
- Keep TIR information for one (1) day.
- Preprocessing interval is zero (0) hours.
- Catalog database cleanup interval is two (2) hours.
- Catalog database cleanup wait time is 10 minutes.
- Policy update interval is 60 minutes.

**RETURN VALUES**

An exit status of zero (0) means that the command ran successfully. Any exit status other than zero (0) means that an error occurred.

If the administrative log function is enabled, the exit status is logged in the administrative daily log under the log directory:

Windows: `install_path\NetBackup\logs\admin`

UNIX: `/usr/openv/netbackup/logs/admin`

It has the following form:

`bpconfig: EXIT status = exit status`

If an error occurred, a diagnostic precedes this message.

**EXAMPLES**

Example 1 - While the master server `kiwi` runs, display the global attribute settings on the master server `plim`: 
# bpconfig -U -M plim
Admin Mail Address: ichabod@null.null.com
Job Retry Delay: 10 minutes
Max Simultaneous Jobs/Client: 1
Backup Tries: 1 time(s) in 8 hour(s)
Keep Error/Debug Logs: 6 days
Max drives this master: 0
Keep TrueImageRecovery Info: 1 days
Compress DB Files: (not enabled)
Media Mount Timeout: 30 minutes
Display Reports: 24 hours ago
Preprocess Interval: 0 hours
Image DB Cleanup Interval: 12 hours
Image DB Cleanup Wait Time: 60 minutes
Policy Update Interval: 10 minutes

Example 2 - Set the Compress Catalog Interval to 604800 seconds, so that NetBackup compresses images more than seven days old:

# bpconfig -cd 604800
# bpconfig -U
Admin Mail Address: *NULL*
Job Retry Delay: 10 minutes
Max Simultaneous Jobs/Client: 1
Backup Tries: 2 time(s) in 12 hour(s)
Keep Error/Debug Logs: 28 days
Max drives this master: 0
Keep TrueImageRecovery Info: 2 days
Compress DB Files: older than 7 day(s)
Media Mount Timeout: 0 minutes (unlimited)
Display Reports: 24 hours ago
Preprocess Interval: 0 hours
Image DB Cleanup Interval: 12 hours
Image DB Cleanup Wait Time: 60 minutes
Policy Update Interval: 10 minutes

Example 3 - Set the Media Mount Timeout to 1800 seconds.

# bpconfig -to 1800
# bpconfig -U
Admin Mail Address: sasquatch@wapati.edu
Job Retry Delay: 10 minutes
Max Simultaneous Jobs/Client: 1
Backup Tries: 1 time(s) in 12 hour(s)
Keep Error/Debug Logs: 3 days
Max drives this master: 0
Keep TrueImageRecovery Info: 24 days
Compress Image DB Files: (not enabled)
Media Mount Timeout: 30 minutes
Display Reports: 24 hours ago
Preprocess Interval: 0 hours
Image DB Cleanup Interval: 12 hours
Policy Update Interval: 10 minutes

FILES

UNIX systems:
/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/db/config/behavior

Windows systems:
install_path\NetBackup\db\config\behavior
install_path\NetBackup\logs\admin/*

SEE ALSO

See bpimage on page 166.
For more details about multihosted drives, see the NetBackup Administrator's Guide, Volume I.
bpdbjobs

bpdbjobs – interact with NetBackup jobs database

SYNOPSIS


bpdbjobs -summary [-M master_servers] [-ignore_parent_jobs] [ -U | -L | -all_columns ] [-file pathname] [-append] [verbose]

bpdbjobs -resume | -suspend | -delete | -cancel | -restart job1,job2,...jobn | type=jobtype | type=all [-M master_servers] [-quiet] [-reason "string"]

bpdbjobs -cancel_all [-M master_servers] [-reason "string"]

bpdbjobs -clean [-M master_servers] [ -keep_hours hours | -keep_days days ] [ -keep_successful_hours hours | -keep_successful_days days ] [verbose]

bpdbjobs -version

bpdbjobs -change_priority_by [-M master_servers] -priority number -jobid job1,job2,...jobn

bpdbjobs -set_priority [-M master_servers] -priority number -jobid job1,job2,...jobn

bpdbjobs -fast

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\

DESCRIPTION

bpdbjobs interacts with the jobs database and is useful in scripts or as a command-line administration tool. It prints the entire jobs database, prints a summary of the database, deletes done jobs, cancels incompleted jobs, and cleans old jobs.
To customize the output of `bpdbjobs`, add column definition entries (`BPDBJOBS_COLDEFS`) in the `bp.conf` file.

See the NetBackup Administrator’s Guide, Volume I for more information about the following: the `bp.conf` file, a complete list of the definitions, and the `BPDBJOBS_COLDEFS` entries.

The `-cancel`, `-delete`, `-jobid`, `-resume`, and `-suspend` options all use the `jobtype` as a suboption. Enter one of the following as `jobtype`. (Letters following the capitalized letters are ignored.)

```
ALL | *
   REStore
   BACkup
   ARCHive
   VERify
   DUPlicate
   IMPort
   LABel
   ERAse
   VAUlt
   TPReq
   CLEan
   FORmat
   INVentory
   QUAlification
   DBbackup | CATalogbackup
```

**Note:** For the NetBackup Accelerator feature, `bpdbjobs` reports the amount of data that was transferred over the network for each backup. You can also configure the command to show the transferred data in the field that normally shows the Accelerator backup image size. For details, see the Accelerator topics in the NetBackup Administrator's Guide Volume I, the NetBackup for VMware Administrator's Guide and the NetBackup for NDMP Administrator’s Guide.

### OPTIONS

- `-all_columns`
  Displays all columns of a report or summary. The output of this command consists of a single line per backup job. Each line of the output is a comma-delimited list. Information such as job ID, field 1, and client name, field 7, are included in the output.
Note: The field values in the -all_columns options are not stable. They can change from release to release. Any information about the fields is subject to change without notice.

-append

Appends the output to the file that the -file option specifies. If no -file option is provided, the output goes to stdout.

-cancel job1,job2,...jobn | type=jobtype | type=all

Causes bpdbjobs to cancel active jobs cleanly that appear with a status code of 150 in the Activity Monitor. For example:

bpdbjobs -cancel 11328
bpdbjobs -cancel 11328,11329,11330

Possible jobtype values are listed in the Description section.

-cancel_all

Causes bpdbjobs to cleanly cancel all incomplete jobs that appear with a Status 150 in the Activity Monitor. For example:

bpdbjobs -cancel_all

-change_priority_by [-M master_servers] -priority number -jobid job1,job2,...jobn

Changes the priority of the specified job or jobs.

-clean

Causes bpdbjobs to delete the completed jobs that are older than a specified time period. Use with the -keep_hours or -keep_days, or -keep_successful_hours or -keep_successful_days parameters to specify a retention period. For example:

bpdbjobs -clean -keep_hours 30

-delete job1,job2,...jobn | type=jobtype | type=all

Deletes the completed jobs that appear in the Activity Monitor. Multiple job IDs can be deleted in one command. For example:

bpdbjobs -delete 11328,11329,11330

This option deletes one of the following:

- The jobs that job1,job2,...jobn specify
- All the eligible jobs that jobtype indicates
- All eligible jobs if type=all is specified
  Possible jobtype values are listed in the Description section.

-fast
  Retrieves the job metadata from bpjobd, but the try file and files file is read directly from the file system. This option is ignored if bpdbjobs is started from a remote host (a host that is not the master).

-file pathname
  Names a file to which the output of bpdbjobs is written. If no -file option is provided, the output goes to stdout.

-gdm
  Displays less of the information in a report than -most_columns.

-ignore_parent_jobs
  Ignores the parent jobs for the -report and -summary options.

-jobid job1,job2,...jobn | type=jobtype | type=all
  Reports on multiple job IDs.
  Possible jobtype values are listed in the Description section.

-keep_days days
  Used with the -clean option to specify how many days bpdbjobs keeps completed jobs. Default is three (3) days.

-keep_hours hours
  Used with the -clean option to specify how many hours bpdbjobs keeps completed jobs. Default is 72 hours.

-keep_successful_days days
  Used with the -clean option to specify how many days bpdbjobs keeps successful completed jobs. Default is three (3) days.
  This value must be less than the -keep_days value.

-keep_successful_hours hours
  Used with the -clean option to specify how many hours bpdbjobs keeps successful completed jobs. Default is 72 hours.
  This value must be less than the -keep_hours value.

-L
  Reports in long format.

-lvault
  Displays the additional columns specific to Vault jobs.
-M master_servers
Applies to an environment with multiple master servers. Use the -M option to summarize jobs, delete jobid(s), cancel jobid(s), and cancel all active job IDs for a specific master server:

-mastertime
By default, bpdbjobs translates the start or the end times to be relative to the local clock. A job that starts 10 minutes ago looks like it starts 10 minutes ago regardless of time zone and clock differences with the master server. This option, however, circumvents that translation so that time values are consistent between admin clients. See the -utc option for normalizing to UTC instead of the local clock.

-most_columns
Behaves similarly to -all_columns but does not include the file list or any information on previous attempts. The -most_columns option is significantly faster than -all_columns.

Note: The field values in the -most_columns options are not stable. They can change from release to release. Any information about the fields is subject to change without notice.

-noheader
Prevents the header from being printed in the report.

-quiet
Cancels the reporting of the number of jobs resumed, suspended, deleted, and canceled.

-reason "string"
Indicates the reason why you are performing this command action. The reason text string that you enter is captured and appears in the audit report. The string must be enclosed by double quotes ("...") and cannot exceed 512 characters. It cannot begin with a dash character (-) nor contain a single quotation mark (').

-report
Provides a report of data that is stored in the Activity Monitor. If no option is specified with bpdbjobs, -report is the default option.

-restart job1,job2,...jobn | type=jobtype | type=all
Cleanly restarts a job that jobtype indicates. This option supports backups and enables you to restart a job by typing the word BACkup in the Activity Monitor.
-resume job1,job2,...jobn | type=jobtype | type=all
Resumes the jobs that job1,job2,...jobn specify, all eligible checkpoint backups or restore the jobs that jobtype indicates, or all eligible jobs if type=all is specified.

Possible jobtype values are listed in the Description section.

-set_priority [-M master_servers] -priority number -jobid job1,job2,...jobn
Sets the priority of the specified job or jobs to the specified priority number.

-summary [-U | -L | -all_columns]
Prints a summary line to stdout for all the jobs that are stored in NBU/jobs. Parameters -U and -L format the output of the command. Use the -file option to write the output to a given directory or file name. For example:

bpdbjobs -summary -U -file /tmp/summary.out

-suspend job1,job2,...jobn | type=jobtype | type=all
Suspends the jobs that job1,job2,...jobn specifies or all eligible checkpoint backups or restore the jobs that jobtype indicates, or all eligible jobs if type=all is specified.

Possible jobtype values are listed in the Description section.

-t timestamp
Fetches the job records which have modified after the specified timestamp. The timestamp is specified in the following format:

mm/dd/yyyy hh:mm:ss

The required date and time values format in NetBackup commands varies according to your locale. The /usr/openv/msg/.conf file (UNIX) and the install_path\VERITAS\msg\LC.CONF file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

For more information about the locale of your system, see "About specifying the locale of the NetBackup installation" in the NetBackup Administrator's Guide, Volume II.

-U
Reports in user format. NetBackup report-generating tools such as the NetBackup-Java Reports application uses this report format.

-utc
Print start and end times in Coordinated Universal Time (UTC) instead of relative to the local clock. Times that this switch translates have +0000 in the
time signature to represent UTC. A full example is: 01/01/19 12:00:00+0000.
Various reports pass through raw timestamps and they are not subject to translation.

-vault
Displays the additional columns specific to Vault jobs.

-verbose
Causes bpdbjobs to log additional information in the debug log in the following directory, if the directory exists:

On UNIX systems:
/usr/openv/netbackup/logs/bpdbjobs/*

On Windows systems:
install_path\NetBackup\logs\bpdbjobs/*

-version
Prints the version string, then halts. Any other switches are ignored.
bpdbm

bpdbm – run NetBackup database manager daemon

SYNOPSIS

bpdbm [-consistency [-move]] [-ctime timestamp] [-terminate] [-alive] [-verbose -logqueries -wakeup minutes]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\

DESCRIPTION

bpdbm responds to the queries that are related to the NetBackup internal databases (catalogs). bpdbm must be running for NetBackup commands and utilities to work properly. This daemon runs only on the master server and can be started only by the administrator. The NetBackup request daemon (bprd) or the following script starts bpdbm:

On UNIX: /usr/openv/netbackup/bin/initbpdbm

On Windows: install_path\NetBackup\bin\initbpdbm

When bpdbm starts, the following sequence occurs in the order listed:

- It logs a message that indicates that it has started and verifies that no other instances are running. If another process is found, the program terminates.

- bpdbm finds its port number by checking the services file for an entry with a service name of bpdbm and a protocol name of tcp. For example:

  bpdbm 13721/tcp

- bpdbm starts to respond to queries from bprd and the NetBackup administrative utilities. A child process is created to respond to each query.

OPTIONS

-alive

Sends a query to bpdbm to determine if the bpdbm service is up.
-consistency [0-2]
  Runs the consistency checks on the catalog. The following are the three consistency levels:
  0 - A quick check of the NetBackup image database (the default).
  1 - Performs more checks than the default check.
  2 - The most in-depth consistency check. In addition to the level 0 and 1 checks, this level checks that the media that is mentioned in the image exists. (That is, it cross-references the media servers databases.) On a large NetBackup installation, the process takes much longer to complete than the other checks.

-ctime timestamp
  Converts a UNIX timestamp to human-readable form.

-logqueries
  Causes bpdbm to log each bpdbm query to the file BPDBMqueries of the tmp directory. Each query has an entry at the start of the log of the form:
  
  date_stamp process_id query type
  
  And one at the end of the query of the form:
  
  date_stamp process_id query type status status
  
  Where date_stamp is a 10-digit integer, process_id is the identifier for the process that runs the query, type is an integer that identifies the type of query, and status is the status returned by the query.

-terminate
  Terminates bpdbm. Any currently running child process continues to run until its task is complete.

-verbose -logqueries
  Causes bpdbm to operate at verbose level 1 if it is configured to run in bp.conf at verbose level 0 and creates the bpdbm log directory and file.

-wakeup minutes
  Overrides the default timeout interval (in minutes) that bpdbm uses when it establishes the initial connection on the port. Used on UNIX systems only.

FILES

On UNIX systems:

/usr/openv/netbackup/db/*
/usr/openv/netbackup/bp.conf
/usr/openv/netbackup/logs/bpdbm/*
/usr/openv/netbackup/bin/initbpdbm

On Windows systems:

install_path\NetBackup\db\*
install_path\NetBackup\logs\bpdbm\*

SEE ALSO

See bprd on page 377.
bpdgclone

bpdgclone – create or remove clones of Volume Manager (VxVM) volumes

SYNOPSIS

bpdgclone [-c] -g disk_group -n volume [-d primary_disk,secondary_disk:primary_disk_2,secondary_disk_2: primary_disk_n,secondary_disk_n] [-f output_location] [-v] [-h]

The directory path to this command is /usr/openv/netbackup/bin/

DESCRIPTION

This command operates only on UNIX systems.

bpdgclone creates temporary disk groups or clones of disks that contain the mirror image of the volume for the backups that use array-specific snapshot methods. In array-specific snapshot methods (EMC TimeFinder, Hitachi ShadowImage, HP BusinessCopy) client data is configured over a Volume Manager volume. To avoid a name conflict in the Volume Manager, bpdgclone names the temporary disk group as client_name_diskgroup_name_clone. When the backup completes, NetBackup removes the disk group clone.

During normal operation, NetBackup calls the bpdgclone command as needed. No administrator use of this command is required. If a system failure prevents NetBackup from removing the clone, use the bpdgclone command with the -c option to remove it. Then synchronize the mirror disk again with the primary disk.

---

Note: If the backup completes, but the clone is not removed, subsequent backups of the client’s data fail. To remove a clone, see Examples.

OPTIONS

- -g 
  Specifies the name of the target disk group.

- -n 
  Specifies the name of the target volume.

- -d 
  Lists the primary disks and the secondary disks. The list consists of disk pairs (primary,secondary), where the primary is separated from the secondary by a comma. If there is more than one primary disk in the target volume, colons (:) separate the additional device pairs.
-c Deletes the cloned disk group and volume. Note that the primary disks and the secondary disks must be resynchronized after the clone is deleted.

-h Prints the command usage.

-v Sets the verbose mode.

-f Specifies an output file. This file contains a list of pathnames of the primary disks over which the target volume is configured. Use this option to discover the primary disks that make up the target volume.

NOTES

The following are considerations to note when you use the `bpdgclone` command:

- Do not remove a clone while the snapshot backup that uses that clone is still in progress. With no system failures, NetBackup removes the clone when the backup completes.

- If you use the `bpdgclone` command to remove a left over disk clone, you must synchronize the mirror disk again with the primary disk.

- Before NetBackup executes `bpdgclone` to create the clone, NetBackup splits the secondary disk from the primary disk.

EXAMPLES

The following example removes a clone.

```
/usr/openv/netbackup/bin/bpdgclone -g wil_test -n vol01 -c
```

where `wil_test` is the name of the disk group after which the clone was named. The actual clone is named `clone_wil_test_clone`.

For detailed assistance, see "Troubleshooting" in the NetBackup Snapshot Client Administrator's Guide.
bpdown

bpdown – shut down NetBackup services on Windows systems

SYNOPSIS


The directory path to this command is install_path\NetBackup\bin\.

DESCRIPTION

This command operates only on Windows systems.

bpdown shuts down the NetBackup services including many components of the product, such as the NetBackup databases, Media Manager, clients, and some robotic control daemons. This option does not shut down the processes.

The bpup command starts the NetBackup services.

OPTIONS

-S  Silent mode. No listing is generated and no confirmation is requested.
-v  The selected verbose mode generates a detailed listing.
-f  Forces a shutdown of the NetBackup services without prompting the user for a confirmation.
-c  Shuts down the client.
-d  Shuts down the NetBackup database.
-m  Shuts down Media Manager.
-n  Shuts down the NetBackup server and not the client.
-s  Shuts down the server (NetBackup and Media Manager).
-r  Shuts down the robotic control daemons.
**bpduplicate**

bpduplicate – create a copy of backups that NetBackup has created

**SYNOPSIS**

```
bpduplicate -npc new_primary_copy -backupid backup_id [-local]
            [-client client_name]

bpduplicate [-number_copies number] [-dstunit destination_storage_unit_label[,copy2,...]] [-dp destination_volume_pool_name[,copy2,...] [-p | -pd | -PD | -PM]
            [-Bidfile file_name] [-v] [-local] [-client client_name] [-st sched_type]
            [-sl sched_label] [-L output_file [-en]] [-host source_host] [-policy name] [-s date] [-e date] [-pt policy_type] [-hoursago hours] [[-cn copy_number] | [-primary]] [-dcn copy_number_1[copy_number_2,...,copy_number_n]] [-M master_server]
            [-altreadhost hostname] [-backupid backup_id] [-id media_id] [-rl retention_level[,rl-copy2,...]] [-fail_on_error 0|1[,...,0|1]] [-mpx]
            [-priority number] [-set_primary copy_index] [-bc_only]
            [-granular_proxy hostname] [-owner media_share_group[,copy2,...]]
```

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
**DESCRIPTION**

The **bpduplicate** command allows a copy of a backup to be created. The **bpduplicate** command can also change the primary copy to enable restoring from a duplicated backup. The primary copy is used to satisfy restore requests and is initially the original copy.

Multiplexed duplications can be created by using the **-mpx** option. Refer to the discussion of the **-mpx** option for more information.

The duplicated backup has a separate expiration date from the original. Initially, the expiration date of the copy is set to the expiration date of the original. You can change the expiration date of the copy or the original by using the **bpexpdate** command.
Use `bpduplicate` to create up to 10 copies of unexpired backups.

**OPTIONS**

- `-altreadhost hostname`
  Specify an alternate host from which to read the media. The default condition is that `bpduplicate` reads the source media from the host that performed the backup.

- `-backupid backup_id`
  Specifies the backup ID of a single backup to duplicate or for which to change the primary copy.

- `-bc_only`
  Catalogs the granular information (that is, it builds the catalog only). Running this option precludes the need to make another copy of the image, which can improve performance of future browse or restore operations.

- `-Bidfile file_name`
  `file_name` specifies a file that contains a list of backup IDs to be duplicated. List one backup ID per line in the file. If this parameter is specified, other selection criteria are ignored.

  Also, `file_name` is removed during the execution of that command line interface (CLI) because the NetBackup GUIs commonly use this parameter. They expect the command-line interface to remove the temporary file that was used for the `-Bidfile` option upon completion. Direct command-line interface users can also use the option; however, it removes the file.

- `-client name`
  Specifies the name of the client that produced the originals and is used as search criteria for backups to duplicate. The default is all clients.

  When you specify `-client` with the `-npc` option to change the primary copy, NetBackup first searches for the backup ID that belongs to the client. This search is useful if the client name has changed.

- `-cn copy_number | -primary`
  Determines the copy number to duplicate. Valid values are 1 through 10. The default is 1.

  `-primary` means to search or duplicate the primary copy.

- `-dcn copy_number_1[,copy_number_2,...,copy_number_n]`
  The destination copy number option specifies the copy number of the new copy that is made with the `bpduplicate` command. The option accepts multiple numbers that are separated with commas. If multiple copy numbers are
specified, you must use -number_copies. The -number_copies option must match the number of copies specified. For example, if -dcn 3,4 is specified, then you must specify -number_copies 2. If -dcn 3 is specified, then you can specify -number_copies 1 or you can omit it.

Please be aware if you cannot have multiple copies with the same copy number. If you specify a copy number that already exists, the command fails. If you omit this option, the bpduplicate command assigns the next available copy number.

```
-dp destination_volume_pool_name[,copy2,...]
```

Specifies the volume pool for the duplicates. NetBackup does not verify that the media ID that is selected for the duplicate copy is not the same media ID where the original resides. Therefore, to avoid the possibility of a deadlock, specify a different volume pool than where the original media ID resides. The default pool name is NB_duplicates.

Specify a pool for each copy that you specify.

```
-dstunit destination_storage_unit_label[,copy2,...]
```

Specifies the destination storage unit. This parameter is required to duplicate backups. Do not specify this option to preview backups to be duplicated (-p, -pb, -PM, or -PD options) or to change the primary copy (-npc option). This option does not have a default.

Specify a storage unit for each copy that you specify.

```
-e date, -s date
```

Specifies the end (-e) or start (-s) of the range of dates and times that include all backups to duplicate. The default end date is the current date and time. The default start time is 24 hours before the current date and time.

The required date and time values format in NetBackup commands varies according to your locale. The /usr/openv/msg/.conf file (UNIX) and the install_path\VERITAS\msg\LC.CONF file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

For more information about the locale of your system, see "About specifying the locale of the NetBackup installation" in the NetBackup Administrator’s Guide, Volume II.

```
-fail_on_error 0|1[,0|1,...,0|1]
```

Specifies whether to fail the other duplications if the copy fails, where:

0 - Do not fail the other copies
1 - Fail the other copies

Specify one for each copy that you specify.
-granular_proxy

Overrides the defined Exchange granular restore proxy host for a duplication operation. This host catalogs the granular information if duplicated to tape. By default, the defined Exchange granular restore proxy host is the original Exchange client for the backup. You can configure the proxy host in the client host Exchange properties of the backup client.

-hoursago hours

Specifies the number of hours before the current time to search for backups. Do not use with the -s option. The default is the previous midnight.

-id media_id

Search the image catalog for backups to duplicate that are on this media ID. If the original is fragmented between different media IDs, NetBackup duplicates only the backups that exist on the specified media ID. Backups that span media are duplicated, but not any other backups on the spanned media ID.

-L output_file [-en]

Specifies the name of a file in which to write progress information. The default is not to use a progress file.

Example for UNIX systems, /usr/openv/netbackup/logs/user_ops

Example for Windows systems, c:\Program Files\Veritas\NetBackup\logs\user_ops

Include the -en option to generate a log in English. The name of the log contains the string _en. This option is useful to support the personnel that assist in a distributed environment where different locales may create logs of various languages.

Only default paths are allowed for this option and It is recommended to use the default paths. If you cannot use the NetBackup default path in your setup, you should add custom paths to the NetBackup configuration.

For more information on how to add a custom path, see the “BPCD_WHITELIST_PATH option for NetBackup servers and clients” topic in the NetBackup Administrator’s Guide, Volume I.

-local

When bpduplicate runs from a host other than the master server and -local is not used (default), the following occurs: It starts a remote copy of the command on the master server. The remote copy allows the command to be terminated from the Activity Monitor.

Use this option to prevent the creation of a remote copy on the master server. You can also run bpduplicate only from the host where it was initiated.
If the `-local` option is used, `bpduplicate` cannot be canceled from the Activity Monitor.

`-M master_server`

Specifies the master server that manages the media catalog that has the media ID. If this option is not specified, the default is one of the following:

The NetBackup server supports only one server (the master) with no remote media servers. Therefore, the default in this case is always the NetBackup server master where you run the command.

On the NetBackup Enterprise Server, if the command is run on a master server, then that server is the default. If the command is run on a media server that is not the master, then the master for that media server is the default.

`-mpx`

Specifies that when you duplicate multiplexed backups, NetBackup creates multiplexed backups on the destination media, which reduces the time to duplicate multiplexed backups.

Multiplexed duplication is not supported for the following operations:

- Non-multiplexed backups
- Backups from disk type storage units
- Backups to disk type storage units
- FlashBackup or NDMP backups

If backups in the previous categories are encountered during duplication, NetBackup duplicates them first and uses non-multiplexed duplication. It then duplicates the multiplexed backups by using multiplexed duplication.

If all the backups in a multiplexed group are not duplicated, the duplicated multiplexed group has a different fragment layout. (A multiplexed group is a set of backups that are multiplexed together during a single multiplexing session.)

If this option is not specified, all backups are duplicated by using non-multiplexed duplication.

For more information about multiplex operations, see the NetBackup Administrator’s Guide, Volume I.

`-npc new_primary_copy`

Allows the primary copy to be changed. The value can be 1 through 10. The `-backupid` option must be specified with this option.
-number_copies number
   Specifies the number of copies to be created. Without the Inline Tape Copy
   option or NetBackup Vault extension that is installed, the value can be set to
   1 only. The default is 1.

   Use with -dstunit, -dp, -fail_on_error, and -r1:

   -number_copies 2 -dstunit stunit-copy1, stunit-copy2
   -number_copies 2 -dp pool1, pool2

-owner media_share_group [,share_group_copy2,...]
   Specifies the share group for the duplicate. Specify a share group for each
   copy that you specify.

-p
   Previews backups to be duplicated according the option settings, but does not
   perform the duplication. Displays the media IDs, server name, backups that
   are not candidates for duplication (and why), and information about the backups
   to be duplicated.

-pb
   Previews the duplication but does not perform the duplication. Similar to the
   -p option, but does not display information about the backups.

-PD
   Same as the -PM option, except that it sorts and displays the backups by date
   and time (newest to oldest).

-PM
   Displays the information on the backups to be duplicated according to the
   option settings, but does not perform the duplication. This format first displays
   the backup IDs that cannot be duplicated and the reason why (for example,
   the backup already has two copies). It displays the following information about
   the backup: Date and time of the backup, policy, schedule, backup ID, host,
   media ID or path, copy number, and whether the copy is the primary copy:

   1 = Primary copy
   0 = Not primary copy

-policy name
   Searches for backups to duplicate in the specified policy. The default is all
   policies.

-priority number
   Sets a backup policy to run at a lesser or a higher priority than disk staging
   duplication.
-pt policy_type

Search for the backups that the specified policy type created. The default is any policy type.

The policy_type is one of the following character strings:

Auspex-FastBackup
BigData
DataStore
DataTools-SQL-BackTrack
DB2
Enterprise-Vault
FlashBackup
FlashBackup-Windows
Hyper-V
Informix-On-BAR
LotusNotes
MS-Exchange-Server
MS-SharePoint
MS-SQL-Server
MS-Windows
NDMP
Oracle
PureDisk-Export
SAP
Split-Mirror
Standard
Sybase
Vault
VMware

-rl retention_level[,rl-copy2,...]

Provides a retention level for each copy that you specify.

If no retention levels are specified, the expiration date of the original copy is used for each copy. If a retention period is indicated, the expiration date for the copy is the backup date plus the retention period.

For example, if a backup was created on May 14, 2012, and its retention period is one week, the new copy’s expiration date is May 21, 2012.

A value of -1 indicates that the original expiration date is used for the copy.

-set_primary copy_index

Specify a new copy to become the primary copy.

copy_index is one of the following:
0 = Do not change the primary copy (default)
1 = First new copy is the primary copy
2 = Second new copy is the primary copy
3 = Third new copy is the primary copy, and so on.

`copy_index` cannot be greater than the `-number_copies` value.

If the copy specified to be the primary copy fails, but other copies are successful, the primary copy does not change from its current value.

`-shost source_host`
Specifies that only the backups that are created on the specified backup server are considered for duplication. The default is to consider all backups regardless of the backup server.

`-sl sched_label`
Search for backups to duplicate that the specified schedule created. The default is all schedules.

`-st sched_type`
Search for backups to duplicate that the specified schedule type created. The default is any schedule type.

Valid values are:

FULL (full backup)
INCR (differential-incremental backup)
CINC (cumulative-incremental backup)
UBAK (user backup)
UARC (user archive)
NOT_ARCHIVE (all backups except user archive)

`-v`
Selects the verbose mode. When you specify the debug logs or progress logs, it includes more information.

**EXAMPLES**

Example 1 - List backups with a copy number of 1. They were backed up by the policy that is named `stdpol`, and created between July 1, 2013, and August 1, 2013.

```
# bpduplicate -PM -cn 1 -policy stdpol -s 07/01/13 -e 08/01/13
```
Example 2 - Duplicate copy 1 of the backups that are listed in file `bidfile` in the `tmp` directory. The destination storage unit is `unit1` and the destination pool is `dup_pool`. Progress information is written to `bpdup.ls`. The command can be all on one line, or you can use a backslash continuation character.

**UNIX systems:**

```bash
# bpduplicate -dstunit unit1 -Bidfile /tmp/bidfile
-L /usr/openv/netbackup/logs/user_ops/bpdup.ls
-dp dup_pool -cn 1
```

**Windows systems:**

```bash
# bpduplicate -dstunit unit1 -Bidfile C:\tmp\bidfile
-L c:\Program Files\Veritas\NetBackup\logs\user_ops\bpdup.ls
-dp dup_pool -cn 1
```

Example 3 - This example is the same as Example 2, except that multiplexed backups are duplicated when you select multiplexed duplication. The command can be all on one line, or you can use a backslash continuation character.

**UNIX systems:**

```bash
# bpduplicate -dstunit unit1 -Bidfile -mpx
/L /usr/openv/netbackup/logs/user_ops/bpdup.ls
-dp dup_pool -cn 1
```

**Windows systems:**

```bash
# bpduplicate -dstunit unit1 -Bidfile -mpx
/L c:\Program Files\Veritas\NetBackup\logs\user_ops\bpdup.ls
-dp dup_pool -cn 1
```

**FILES**

**UNIX systems:**

```bash
/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/db/images/*
```

**Windows systems:**
install_path\NetBackup\db\images\*
install_path\NetBackup\logs\admin\*

SEE ALSO

See nbreplicate on page 797.
**bper**

**SYNOPSIS**

```
bper [-S | -statuscode status_code] [-r | -recommendation] [[-p
Unx | NTx] | [-platform Unx | NTx]] [-v]
```

```
bper [-all | -problems | -media | tape] [-backstat [-by_statcode]]
[-L | -l | -U] [-columns ncols] [-d date | -hoursago hours] [-e date]
[-client client_name] [-server server_name] [-jobid job_id] [-M
master_server,...] [-v]
```

```
bper [-s {severity[+]}|severity ... [-t type ...] [-dt disk_type]
[-L | -l | -U] [-columns ncols] [-d date | -hoursago hours] [-e date]
[-client client_name] [-server server_name] [-jobid job_id] [-M
master_server,...] [-v]
```

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
**DESCRIPTION**

*bper** displays information from either the same source as the online
troubleshooter (in the Activity Monitor or Reports applications) or from the NetBackup
error catalog. *bper* provides the following types of displays:

- A display of the message that corresponds to a status code and, optionally, a
  recommendation on how to troubleshoot the problem. In this case, the display
  results come from the same source as the online troubleshooter for the local
  system.

- A display of the error catalog entries that satisfy the command-line options. For
  instance, *bper* can display all the problem entries for the previous day.

- A display of the error catalog entries that correspond to a particular message
  severity and message type.

For information on details of the displays, see DISPLAY FORMATS later in this
command description.
bperror writes its debug log information to the following directory:

On Windows systems: `install_path\NetBackup\logs\admin`

On UNIX systems: `/usr/openv/netbackup/logs/admin`

You can use the information in this directory for troubleshooting.

The output of `bperror` goes to standard output.

**OPTIONS**

- `all, -backstat [-by_statcode], -media, -problems`
  These options specify the type and severity of log messages to display. The default type is ALL. The default severity is ALL.

  - `all`: The type is ALL, and severity is ALL. Run `bperror` with this option and with `-U` to produce an All Log Entries report.

  - `backstat`: The type is BACKSTAT, and severity is ALL. If `-by_statcode` is present, the display contains one entry for each unique status code. Line 1 of the entry contains the status code and the corresponding message text. Line 2 of the entry contains the list of clients for which this status code occurred. `-by_statcode` is only valid when the command line contains both `backstat` and `-U`. Run `bperror` with this option and with `-U` to produce a Backup Status report.

  - `media`: The type is MEDIACODE, and severity is ALL. Run `bperror` with this option and with `-U` produces a Media Logs report.

  - `problems`: The type is ALL, and severity is the union of WARNING, ERROR, and CRITICAL. Run `bperror` with this option and with `-U` to produce a Problems report.

- `client client_name`
  Specifies the name of a NetBackup client. This name must be as it appears in the NetBackup catalog. By default, `bperror` searches for all clients.

- `columns ncols`
  For the `-L` and `-U` reports, `columns` provides an approximate upper bound on the maximum line length. `bperror` does not try to produce lines exactly `ncols` characters in length.

  `columns` does not apply to the `-l` report.

  `ncols` must be at least 40. The default is 80.

- `d date, -e date`
  Specifies the start date and end date range for the listing.
-d specifies a start date and time (optional) for the listing. The resulting list shows only images in the backups or archives that occurred at or after the specified date-time. The valid range of dates is from 01/01/1970 00:00:00 to 01/19/2038 03:14:07. The default is 24 hours before the current date and time.

-e specifies an end date and time (optional) for the listing. The resulting list shows only files from backups or the archives that occurred at or before the specified date and time. Use the same format for the start date. The default is the current date and time. The end date must be greater than or equal to the start date.

The required date and time values format in NetBackup commands varies according to your locale. The /usr/openv/msg/.conf file (UNIX) and the install_path\VERITAS\msg\LC.CONF file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

For more about the locale of your system, see "About specifying the locale of the NetBackup installation" in the NetBackup Administrator's Guide, Volume II.

The following is a typical format for the -d and -e options:

[-d mm/dd/yyyy hh:mm:ss | -hoursago hours]
[-e mm/dd/yyyy hh:mm:ss]

-dt disk_type

Enables the user to specify a disk type. The following are the valid values for disk_type:

0 - All
1 - BasicDisk
3 - SnapVault
6 - DiskPool

-hoursago hours

Specifies a start time of many hours ago, which is equivalent to specifying a start time (-d) of the current time minus hours. Hours is an integer. The default is 24, which is a start time of 24 hours before the current time.

-jobid job_id

Specifies a NetBackup job ID. By default, bperror searches for all job IDs.

-L

Reports in long format.
-l
Reports in short format. This report produces a terse listing. This option is useful for scripts or the programs that rework the listing contents into a customized report format. This option is the default list type.

-M master_server,...
Specifies a comma-separated list of one or more hostnames. The command is run on each of the master servers in this list. The master servers must allow access by the system that issues the command. If an error occurs for any master server, the process stops at that point in the list. The default is the master server for the system where the command is entered.

-p Unx | NTx, -platform Unx | NTx
Displays the message that applies to the platform (UNIX or Windows) for the specified status code. The default is to display the message for the platform on which bperror is running. The -S or -statuscode option must be specified when you use this option.

-r | -recommendation
Displays the recommended action for the specified status code from the NetBackup Status Codes Reference Guide. The default is not to display the recommendation. The -S or -statuscode option must be specified when you use this option.

-S status_code, -statuscode status_code
Displays the message that corresponds to the status code. This option has no default condition.

-s severity, -s severity+
Specifies the severity of log messages to display. The defined values are ALL, DEBUG, INFO, WARNING, ERROR, and CRITICAL.

You can specify severity in two ways. The first way is a list of one or more severity values. For instance, "-s INFO ERROR" displays the messages with either severity INFO or severity ERROR. The delimiter must be a blank (" ") between the elements in the list. The second way is a single severity value with "+" appended, which is this severity or greater. For instance "-s WARNING+" displays the messages with severity values WARNING, ERROR, and CRITICAL.

The default is ALL. The severity value can be in uppercase or lowercase.

-server server_name
Specifies the name of a NetBackup server. This name must be as it appears in the NetBackup catalog. The display is limited to the messages that are logged for this server, which also satisfies the criteria for any other bperror options.
For example, if `-server plim` and `-hoursago 2` are `berror` options, the display contains the messages that were logged for `plim` in the past two hours.

The server name must match the server name that was recorded in the log messages. For example, if the logs record the server name as `plim.null.com`, `-server plim` does not display the logs, but `-server plim.null.com` does.

The query goes to the error catalog which resides on either the local master server or the master server that `-M` specifies. The master server must allow access by the system that runs `berror`.

The default is to display log messages for all media servers that are known to the master server(s).

```
-t type
```

Specifies the type of log messages to display. The defined values are `ALL`, `BACKSTAT`, `MEDIADEV`, `GENERAL`, `BACKUP`, `ARCHIVE`, `RETRIEVE`, and `SECURITY`. The default is `ALL`. The type value can be upper or lower case. It is entered as a list of one or more values. For instance, `-t BACKSTAT MEDIADEV` displays the messages with either type `BACKSTAT` or type `MEDIADEV`. The delimiter between the list elements must be a blank (" ").

```
-U
```

Reports in user format. NetBackup report-generating tools such as the NetBackup-Java Reports application uses this report.

```
-v
```

Verbose mode. This option causes `berror` to log additional information for the debugging purposes that go into the NetBackup administration daily debug log. `-v` is meaningful only when NetBackup has debug logs enabled. The default is to not be verbose.

### DISPLAY FORMATS

The following are display formats of the `berror` command:

- **Status code display** (for example, `berror -S status_code`):
  - `berror` queries the NetBackup online troubleshooter on the local system for the message that corresponds to the status code. `berror` displays the message text on one line and an explanation on a second line.
  - If `-r` is an option, `berror` also queries for the troubleshooting recommendation that corresponds to the status code. `berror` displays the recommendation following the status message, on one or more lines.

- **Error catalog display** (for example, `berror -all; berror -s severity`):
bperror queries the NetBackup error catalog on either the local master server or the master servers in the -M option list. The display consists of the results that are returned from querying the error catalog on the master server(s). The results are limited to catalog the entries that satisfy all the bperror options. For example, the bperror command line may contain options for client, start time, and end time. If so, then bperror reports only the jobs that are run for that client between the start time and end time.

The display variant that shows individual message entries from the error catalog can appear in long (-L), user (-U), or short (-l) format. The display variant that categorizes by status code can appear in user (-U) format only. The following is the display content for each of these formats:

- Error catalog display, individual message entries, long format (for example, bperror -media -L). This report produces several lines per log entry, with the following contents:
  - Field 1: Date and time - Number of seconds since 1/1/1970
  - Field 2: NetBackup version - The NetBackup version in use
  - Field 3: Error type - Media numeric identifiers of the error
  - Field 4: Log entry type - 2=Debug, 4=Info, 8=Warning, 16=Error, 32=Critical
  - Field 5: Server - Server name
  - Field 6: Job ID
  - Field 7: Group job ID
  - Field 8: Unused
  - Field 9: NetBackup process - Name of the NetBackup process that does the logging
  - Field 10: Client name
  - Field 11: Policy name
  - Field 12: Schedule type - The type of schedule being run for the backup
    0=FULL, 1=INCR, 2=CINC, 3=UBAK, 4=UARC
  - Field 13: Exit status - The status when the backup was completed

- Error catalog display, individual message entries, user format (for example, bperror -media -U). The user format produces a header line that shows column names, and one or more lines per log entry with these contents:
  - Line 1: Date and time
  - Server
  - Client
  - Text (at the start of the log message, continued on subsequent lines if needed)

- Error catalog display, individual message entries, short format (for example, bperror -media -l). The short format produces a single line per log entry, with the following contents:
  - Line 1: Time (internal system representation)
NetBackup version
Type code (decimal)
Severity code (decimal)
Server
Job ID
Job Group ID
An unused field
Client
Who
Text (the entire log message text, with no truncation of the line length)

- Error catalog display that the status code categorizes. This display reports only each unique status code, instead of listing every log entry for that status code (for example, `bperror -backstat -by_statcode -U`). This option produces two or more lines per status code, with the following contents:
  Line 1: Status code
  Text (the beginning of the log message text, continued on subsequent lines if necessary)
  Line 2: The list of clients for which this status occurred.

EXAMPLES

Example 1 - Display the error for a job that failed because the NetBackup encryption package was not installed. Status code 9 is the NetBackup status code for this failure. The second run of `bperror` displays the action that is recommended for NetBackup status code 9.

```bash
# bperror -d 12/23/2012 16:00:00 -e 12/23/2012 17:00:00 -t backstat -U
STATUS CLIENT POLICY SCHED SERVER TIME COMPLETED
9  plim dhcrypt user plim 12/23/2012 16:38:09
an extension package is needed, but was not installed
```

```bash
# bperror -S 9 -r
an extension package is needed, but was not installed
A NetBackup extension product is required in order to perform the requested operation.
Install the required extension product.
```

Example 2 - Report the problems in the User format that have occurred in the previous 24 hours.

```bash
# bperror -U -problems
TIME SERVER CLIENT TEXT
```
Example 3 - The following example displays status for type backstat for the jobs that are run in the previous 24 hours. The option -by_statcode produces a display that is organized by status code.

The display shows that one or more jobs for each of the clients chive, gava, and raisins have completed successfully (the status code is 0). In addition, one or more jobs for client nut have failed because nut did not allow access by the master server or media server. (The status code is 59.)

Example 4 - Identify and retrieve the results for a particular user job. It first lists the log entries with job IDs other than zero. It then runs a User-format report on the job of interest.

Example 5 - Show media entries in the error catalog for the past 2000 hours.
Example 6 - Report and add up the total number of bytes backed up in the past 24 hours.

`bperror -all -hoursago 24 | grep "successfully wrote backup id | awk '{bytes= bytes + $20} END {print "backed up",bytes," Kbytes of data"}')`

backed up 64 Kbytes of data
bpexpdate

bpexpdate – change expiration date of backups in image catalog and media in media catalog

SYNOPSIS

bpexpdate -m media_id -d date | 0 | infinity [-host name] [-force] [-nodelete] [-notimmediate] [-force_not_complete] [-M master_server,...]

bpexpdate -deassignempty [-m media_id] [-force] [-M master_server,...]  

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd

DESCRIPTION

NetBackup maintains catalogs, which are internal databases with backup image and media information. The image record in the image catalog contains an expiration date. The media ID in the media catalog also contains an expiration date. The expiration date is the date and time when NetBackup removes the record for a backup or a media ID from the corresponding catalog.

The bpexpdate command allows the expiration date and time of backups to be changed in the NetBackup image catalog. The command is also used to change the expiration of removable media in the NetBackup media catalog. If the date is set to zero, bpexpdate immediately expires backups from the image catalog or media from the media catalog. When a media ID is removed from the NetBackup media catalog, it is also removed from the Enterprise Media Manager database. It is removed regardless of the media’s previous state (FROZEN, SUSPENDED, and so on).

You can change the expiration on a media ID basis or on an individual backup ID basis. When you change the expiration date of a media ID, the expiration date of all backups on the media are also changed. bpexpdate also provides the following options:

- Remove media from the media catalog if they no longer contain valid backups.
- Recalculate the expiration date to base it on the configured or a supplied retention level.
Once made WORM, copies can never become writable again. The copies, however, become deletable after the unlock time has elapsed.

Any authorized user can run this command.

For more about NetBackup authorization, see the *NetBackup Security and Encryption Guide*.

### OPERATIONS

The command operations are as follows:

- **-backupid backup_id**
  - Changes the expiration of a single backup. If the date is zero, the backup is removed from the image catalog. If the backup is on removable media and the -d expiration is greater than the current media ID expiration, the media catalog expiration also changes. The change affects all copies of a backup, unless the -copy option is used. The -copy option causes only the specified copy to be affected.

- **-Bidfile filename**
  - Specifies a file that contains a list of backup IDs whose expiration date you want to change. List one backup ID per line in the file.

- **-deassignempty**
  - Searches the catalog for the removable media that no longer contain valid backups. It removes the media from the media catalog and removes the media IDs in the Media Manager catalog. The media is then available to use again. You can use the NetBackup Images on Media report to determine if the assigned media no longer contain valid backups.

- **-recalculate**
  - Allows the expiration date of backups to be changed based on a retention level, or a new expiration date. You can change the expiration for a single backup, or for all backups for a particular client, policy, or schedule type. One of the -bybackuptime, -d, or -ret options may be used with this option.

  When the -bybackuptime option is used, the expiration date of the backup is set to the creation date plus the retention level value that was originally used for the backup. After a backup has been imported, this option can be used to reset its expiration date to the original value.

**Note:** Retention level 25 has a value of expire immediately. You cannot edit this value. If you set the retention level of a backup image to 25, the backup image expires immediately.
When the `-ret` option is used, the expiration date of the backup is set to the creation date plus the specified retention level value.

If `-bybackuptime`, `-d`, or `-ret` is not used with this option, the expiration date for any non-Storage Lifecycle Policy (SLP) backups are set to the creation date plus the current retention level of the schedule that wrote the backup, if it exists and the schedule's retention level has changed since the backup creation. A backup's expiration date is not recalculated under any of the circumstances shown:

- An SLP created it.
- If the policy and schedule that wrote the backup no longer exist.
- If the retention level of the schedule that wrote the backup has not changed since the backup was created.

If the backup is on removable media, the expiration date of the media is also changed if the new expiration date of the backup is later than the current media expiration date.

```
-sservername server_name
```

Specifies the name of a server that the expiration date change affects. The server name refers to a field of the image fragment record where the fragment resides. This server is the media server that performs the data movement. For snapshots, this server is the client where the snapshot resides.

```
-styype server_type
```

Specifies a string that identifies the storage server type. The `server_type` value can originate from one of the following sources:

- Veritas provided storage. Possible values are `AdvancedDisk` and `PureDisk`.
- Third-party disk appliances. The vendor supplies the `server_type` string.
- Cloud storage. The cloud `server_type` values reflect the cloud storage provider. Determine the possible values with the `csconfig` command, as shown. The information in bold (bold added for emphasis) is the required information for the `-styype` option. Please note the output of the `csconfig` command can change based on the currently supported providers.

```
root:~# csconfig cldprovider -l

amazon (Amazon - Simple Storage Service)
amazon.gov (Amazon GovCloud - Simple Storage Service)
azure (Microsoft Azure - Microsoft Azure Storage Service)
cloudian (Cloudian HyperStore - Cloudian HyperStore Object Storage)
```
google (Google Nearline - Google Cloud Storage Nearline)
hitachi (Hitachi Cloud Service (HCS) - Hitachi Off Premise Public Cloud)
hitachicp (Hitachi Content Platform (HCP) - Hitachi On Premise Private Cloud)
swiftstack (SwiftStack - SwiftStack Object Storage)
verizon (Verizon - Verizon Cloud Storage)

Cloud storage stype values must incorporate a suffix (for example, amazon_crypt). Possible suffixes are:

- _raw: The NetBackup backup image is sent to the cloud in raw format. Use this option if you do not want to compress or encrypt data before sending to cloud storage.
- _rawc: Compresses the raw data before it is written to the cloud storage.
- _crypt: Encrypt the data using AES-256 encryption before writing the data to cloud storage. You must have KMS configured in NetBackup to use this option.
- _cryptc: Compress and encrypt the data before writing to cloud storage.

The storage server type is case sensitive.

OPTIONS

-bybackupuptime

Specifies that the expiration date is set to the backup creation date plus the retention level value that was used for the backup.

-client name

Specifies the client name for the -backupid and -recalculate operations.

For the backupid operation, this option causes NetBackup to first search for the backup ID for the specified client. This option is useful if the client name has changed.

For recalculate, this option causes NetBackup to recalculate the expiration date to be based on the retention level for all the specified client backups.

-copy number

Expires or changes the expiration date of the specified copy number and is valid only with the -backupid and -recalculate options. Valid values are 1 through 10.

If the primary copy is expired, the other copy becomes the primary copy. If this option is not specified, the expiration affects both copies of the backup.
-d date
Specifies the expiration date and time. date can be any one of the following:

- mm/dd/yy hh:mm:ss
- 0 - the backup or media expires immediately
- infinity - the backup never expires

The required date and time values format in NetBackup commands varies according to your locale. The /usr/openv/msg/.conf file (UNIX) and the install_path\VERITAS\msg\LC.CONF file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

For more about the locale of your system, see "About specifying the locale of the NetBackup installation" in the NetBackup Administrator's Guide, Volume II.

-deassignempty
Searches the catalog for the removable media that no longer contain valid backups. It removes the media from the media catalog. The media is then available to use again. You can use the NetBackup Images on Media report to determine if the assigned media no longer contain valid backups.

-do_not_follow_dependee
By default, when a dependent image is expired, an eligible dependee image is also expired. The -do_not_follow_dependee option overwrites this behavior, so that the image expiration does not affect the dependee image.

-dp disk_pool_name -dv disk_volume
Specifies the disk pool and, optionally, the disk volume for the expiration date operation to be performed.

-extend_worm_locks
Use the -extend_worm_locks option to extend the expiration date of a WORM copy. WORM copy expiration time can never be shortened. By default, expiration for WORM copies cannot be extended. This option must be provided to allow the extension of expiration time for WORM copies. If no WORM copies are specified, this option has no effect.

-force
Before you run the specified operation, bpexpdate queries before it starts the operation. This option forces the bpexpdate command to carry out the operation without querying the user.
-force_not_complete

By default, an SLP-managed image or its copies cannot be expired if SLP processing is still in progress. The -force_not_complete option overrides this restriction and expires the image even if it is not SLP complete. Note that when you terminate further SLP processing of an image, other image copies may expire as well.

-host name

Note: For the NetBackup server, this option is not required because only one server (the master) exists. If you do use the option, specify the host name of that server.

Specifies the host name of the server to which the media is assigned. This option should be used only with the -m media_id option, and then only if the following is true: The master has remote media servers and the volume was not written on the server where you run bpexpdate.

For example, assume that you have a master server named whale and a media server named eel. You run the following command on whale to remove media ID BU0001 manually from the media catalog and all corresponding backups from the image catalog:

bpexpdate -m BU0001 -d 0 -host eel

You can use the NetBackup Media List report to determine which server’s media catalog has the volume.

-m media_id

Checks if valid backups exist on this particular media ID. This option is used only with the -deassignempty option. The media ID must be six or fewer characters and must be in the NetBackup media catalog.

-M master_server [, ...]

Specifies the master server that manages the media catalog that has the media ID. If this option is not specified, the default is one of the following:

For NetBackup Server:

NetBackup Server supports only one server (the master) with no remote media servers. Therefore, the default in this case is always the master server where you run the command.

For NetBackup Enterprise Server:
If the command is run on a master server, then that server is the default. If the command is run on a media server that is not the master, then the master for that media server is the default.

-`nodelete`

Deletes the backup from the image catalog but does not delete it from the disk storage. Use this option when you unimport a disk group from one master server and import the disk group to a different master server.

-`notimmediate`

Inhibits the call that `bpexpdate` makes to the `nbdelete` command after it expires an image on disk. If you intend to delete many images at the same time, use `-notimmediate` to avoid the overhead of multiple job creation for `nbdelete` to process. You can then run the `nbdelete` command later.

-`policy name`

Specifies the policy name and is valid with the `-recalculate` option. When the policy name is specified, the expiration is recalculated based on the retention level for all backups that are created in this policy.

-`recalculate`

Allows the expiration date of backups to be changed based on the specified retention level, or you can specify a new expiration date. You must specify either the `-d` or `-ret` option with this option. When the expiration changes according to retention level, the new date is based on the creation date of the backup plus the retention level value. You can change the expiration for a single backup, or for all backups for a particular client, policy, or schedule type.

If the backup is on removable media, the expiration in the media catalog changes if the command expiration is greater than the current expiration.

-`ret retention_level`

Specifies the retention level to use when you recalculate expiration dates and is valid with the `-recalculate` option. Levels range from 0 to 100. The new expiration date is the backup’s creation date plus this retention level. You must specify either `-backupid` or `-policy` with this option.

---

**Note:** If you run this command on a pre-NetBackup 8.0 media server, you can only specify a retention level between 0 and 24.

-`sched type`

Specifies the schedule type and is valid with the `-recalculate` option. When the type is specified, the expiration is recalculated based on the retention level for all backups that are created with this schedule type. Enter a numeric value for type as follows:
0 = Full
1 = Differential Incremental
2 = User Backup
3 = User Archive
4 = Cumulative Incremental

The `-policy` option must be specified with `-sched`.

**NOTES**

Some options in large environments can take a significant amount of time to complete. Changes that cause backups or media to expire are irrevocable. You may be required to import backups or recover previous versions of the catalogs if you make mistakes by using this command.

**EXAMPLES**

Example 1 - The following command runs on the master server and removes media ID BU0002 from the media catalog. It deassigns the media ID in the media manager catalog. It also expires associated image records in the image catalog.

```
# bpexpdate -m BU0002 -d 0
```

Example 2 - Change the expiration of copy 2 of `backupid eel_0904219764`. It does not affect the expiration of copy 1 of the backup.

```
# bpexpdate -backupid eel_0904219764 -d 12/20/2012 08:00:00 -copy 2
```

Example 3 - Remove the backup from the image catalog. Since the `-copy` option is not specified, all copies are removed.

```
# bpexpdate -backupid eel_0904219764 -d 0
```

Example 4 - Check for media in the media catalog of host `cat` that is still assigned, but no longer contain valid backups. The command removes any such media from the catalog and deassigns them in the media manager catalog.

```
# bpexpdate -deassignempty -host cat
```

Example 5 - Recalculate the expiration date of backup ID 1234 to the date 10/31/2012.

```
# bpexpdate -recalculate -backupid 1234 -d 10/31/12
```
Example 6 - Recalculate the expiration date of backup ID 1234 based on a retention level. The new retention level is 4 which is two months (default value). Backup ID 1234 is now scheduled to expire in 2 months.

```bash
# bpexpdate -recalculate -backupid 1234 -ret 4
```

**FILES**

**UNIX systems:**

```
/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/db/media/*
/usr/openv/netbackup/db/images/*
```

**Windows systems:**

```
install_path\NetBackup\logs\admin/*
install_path\NetBackup\db\media/*
install_path\NetBackup\db\images/*
```
bpfis

bpfis – create or delete a snapshot, or return information about existing snapshots

SYNOPSIS

bpfis delete [-force] -id id -copy copynum
bpfis query [-fq] [-id id -copy copynum]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/
On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

The bpfis command can delete or query (discover) snapshots of a client system (file system or volume).

Note: To store the image on tape or other media requires that you run a separate backup job.

For more information about the locale of your system, see "About specifying the locale of the NetBackup installation" in the NetBackup Administrator’s Guide, Volume II.

For detailed examples and procedures about using bpfis, see the NetBackup Snapshot Client Administrator’s Guide.

You must have administrator privileges to run this command.

OPTIONS

-copy copynum
   Identifies the copy number. When used with the query function, -copy lists detailed information for the specified copy number of the snapshot. With the delete function, -copy specifies the copy number of the snapshot to be deleted.

delete
   Deletes the snapshot that -id identifies.
-force
Forces the delete operation.

-fq
Generates a full query which includes a detailed description and information about a given snapshot.

-id
Returns the path of the original file system (snapshot source) and the path of the snapshot file system. The default ID is a timestamp that shows when the image was created.

For bpfis delete, this option designates the ID of the snapshot to be deleted.
For bpfis query, this option designates the ID of the snapshot for which to return information.

query
Retrieves detailed information on the specified snapshot of a client system.

EXAMPLES

Example 1 - Obtain information about a particular snapshot on the local host. The output shows the path of the snapshot source (UNIX: /mnt/ufscon) and the path of the snapshot file system (UNIX: /tmp/_vrts_frzn_img_26808/mnt/ufscon).

# bpfis query -id 1034037338
INF - BACKUP START 26838
INF - Frozen image host : ricochet
INF - Frozen image owner: GENERIC
INF - Time created : Mon Oct 7 19:35:38 2011
INF - REMAP FILE BACKUP /mnt/ufscon USING (UNIX systems)
INF - REMAP FILE BACKUP E: USING GUID (Windows systems)
/tmp/_vrts_frzn_img_26808/mnt/ufscon (UNIX systems)
OPTIONS:ALT_PATH_PREFIX=/tmp/_vrts_frzn_img_26808,FITYPE=MIRROR,
MNTPOINT=/mnt/ufscon,FSTYPE=ufs (UNIX systems)
MNTPOINT=E:\,FSTYPE=NTFS (Windows systems)
INF - EXIT STATUS 0: the requested operation was successfully completed

Example 2 - Delete a snapshot on the local host:

# bpfis delete -id 1034037338
INF - BACKUP START 26839
INF - EXIT STATUS 0: the requested operation was successfully completed
**bpflist**

bpflist – list the backed up and archived files on the NetBackup server

**SYNOPSIS**

```
```

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd

**DESCRIPTION**

The `bpflist` command shows a list of previously archived or backed up files according to the options that you specify. This command is available only on NetBackup servers and can be run only by authorized users. This command is similar to the `bplist` command that is available on all NetBackup hosts including clients.

The list can be reported in the following ways:

- `-l` Generates the report in short mode and is the default condition. This terse listing is useful for the scripts or programs that rework the listing contents into a customized report format. See Example 1.

- `-L` Generates the report in long mode.

- `-U` Generates the report in user mode with a text header for each result. The values are comma-separated. See Example 2.

**OPTIONS**

- `-backupid name`
  Specifies a backup ID to use for finding images to list.
-bt unixtime
   Sets the start date to the specified UNIX time. The -bt option is an alternative to the -d option.

-client client_name
   Specifies a client name to use for finding backups or archives to list. By default, bpflist uses the name of the host that runs the command.

-d mm/dd/yyyy hh:mm:ss  -e mm/dd/yyyy hh:mm:ss
   Specifies the start date and end date range for the listing as follows:
   ■ -d specifies a start date and time for the listing. The output list shows only files from backups or the archives that occurred at or after the specified date and time. The -d default is the previous midnight.
   ■ -e specifies an end date and time for the listing. The output list shows only files from backups or the archives that occurred at or before the specified date and time. The -e default is the current date and time.

   The start date and end date have the same format. The valid range of dates is from 01/01/1970 00:00:00 to 01/19/2038 03:14:07.

   The required date and time values format in NetBackup commands varies according to your locale. The /usr/openv/msg/.conf file (UNIX) and the install_path\VERITAS\msg\LC.CONF file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

   For more information about the locale of your system, see "About specifying the locale of the NetBackup installation" in the NetBackup Administrator's Guide, Volume II.

-group name
   Specifies the group that can access and list the files. Only the files accessible by the group can be listed. This option takes effect only if the -malgo option is set to 3.

-keyword "keyword_phrase"
   Specifies a keyword phrase for NetBackup to use when it searches for backups or archives from which to list files. The phrase must match the one that was previously associated with the backup or archive by the bpbackup -k command or the bparchive -k command. You can use this option in place of or in combination with the other options to make it easier to select backups and archives.

   Use the following meta-characters to help match keywords or parts of keywords in the phrase:
-M master_server,...

Specifies a comma-delimited list of host names that represent one or more alternative master servers. Each master server in the list runs the `bpflist` command. If an error occurs on any master server, the process stops at that point. The report is the composite of the information that all the master servers in this list return. The `bpflist` command queries each of these master servers. The master server returns image or media information from the image catalogs. Each master server must allow access by the system that issues the `bpflist` command. The default is the master server for the system running `bpflist`.

-malgo match_algorithm

Names the file or directory to list. Any files or directories that you specify must be listed at the end, following all other options. If you do not specify a path, the default is the current working directory. The valid values are as follows:

- 0 (MA_DEFAULT)
- 1 (MA_AWBUS)
- 2 (MA_USE_GMATCH)
- 3 (MA_WITH_SECURITY)

-option option ...

Specifies a list of space-separated options that affect the operation of the command. Possible values of `option` are the following:

NONE
FILESYSTEM_ONLY
GET_ALL_FILES
GET_PRIMARY_COPY_NUM_BLOCKS (Return the number of blocks in the primary copy)
IGNORE_CASE
INCLUDE_BITMAP
INCLUDE_EDI (Include EDI images)
INCLUDE_EFI (Include EFI system partition images)
INCLUDE_FSMAP
INCLUDE_HIDDEN_IMAGES (Include hidden images)
INCLUDE_RAW_INCR (Include raw incremental images)
INCLUDE_TIR (Include True Image Restore images)
NO_HSHAKE (Continue sending data even if the socket is not ready)
ONE_CONNECT (Run multiple queries on a single connection)
ONE_PASS (Return all files at once)
ONLY_DIRS (Return only directories)
ONLY_ENV_VARS (Return only NDMP environment variables)
ONLY_FIRST_FRAGMENT
ONLY_INPROGRESS_IMAGES (Return only in progress or unvalidated images)
ONLY_SC_CLIENT_TYPES
ONLY_TIR (Return only TIR images)
ONLY_VM_FILES (Return only virtual machine images)
STR2FILE_ENTRY_FORMAT

-patter fullpath
  Only files matching the specified pattern are listed.

-policy policy_name
  Names the policy to search to produce the list. If not specified, all policies are searched.

-psep path_separator_character
  Specifies the path separator character.

-pt policy_type
  Specifies a policy type. By default, bpflist searches for all policy types. The policy_type is one of the following character strings:

  Auspex-FastBackup
  BigData
  DataStore
  DataTools-SQL-BackTrack
  DB2
  Enterprise-Vault
  FlashBackup
  FlashBackup-Windows
  Hyper-V
  Informix-On-BAR
  LotusNotes
  MS-Exchange-Server
  MS-SharePoint
  MS-SQL-Server
-raw mode
   Specifies the raw partition mode.

-rl recursion_level
   Recursively lists the subdirectories that are encountered to the specified depth.

-st schedule_type
   Specifies the schedule type for the selection of the backup images for which the primary copy is changed. By default, `bpchangeprimary` uses any schedule type. Valid values are as follows:
   
   **FULL** (full backup)
   
   **INCR** (differential-incremental backup)
   
   **CINC** (cumulative-incremental backup)
   
   **UBAK** (user backup)
   
   **UARC** (user archive)
   
   **NOT_ARCHIVE** (all backups except user archive)
   
   **SCHED** (FULL, INCR, CINC, TLOG)
   
   **USER** (UBAK and UARC)
   
   **TLOG** (transaction logs)
   
   **ANY** (any of the previous types)

-user name
   Specifies the user that can access and list the files. Only the files accessible by the user can be listed. This option takes effect only if the `-malgo` option is set to 3.
-ut unixtime  
   Specifies an alternative to the -d and -e options and sets the start date and end date to the specified UNIX time. Use this option to specify a single backup or archive to list.

-v  
   Generates the report in verbose mode and displays log messages on the console.

EXAMPLES

Example 1 - On a UNIX system, search for the path /images in backups since unix time 1380000000. The list is in short mode (default condition).

# bpflist -client cl2 -bt 1380000000 -rl 0 -pt Standard -pattern /images

FILES 10 0 0 1383577314 0 cl2 test cl2_1383577314 - *NULL* 1 0 unknown 0 0 *NULL* 1 0 19 50 8 1 0 0 2051 /images/ 16877 root root 0 1383577314 1382366087 1383559354
FILES 10 0 0 1383334895 0 cl2 test cl2_1383334895 - *NULL* 1 0 unknown 0 0 *NULL* 1 0 19 50 8 1 0 0 2051 /images/ 16877 root root 0 1383334895 1382366087 1383296672
FILES 10 0 0 1383331752 0 cl2 test cl2_1383331752 - *NULL* 1 0 unknown 0 0 *NULL* 1 0 19 50 8 1 0 0 2051 /images/ 16877 root root 0 1383331752 1382366087 1383296672

Example 2 - Display the listing in user (-U) mode.

# bpflist -client cl2 -bt 1380000000 -rl 0 -pt Standard -pattern /images -U

Client: c12
Policy: test
Backup ID: cl2_1383577314
Backed up: Mon 04 Nov 2013 09:01:54 AM CS (1383577314)
Software Version: ?
Policy Type: Standard
Schedule Type: FULL
Version: 10
Keyword: ?
Num Files: 1
Files:
FN=1 L=0 PL=19 DL=50 BK=8 II=1 RS=0 GB=0 DN=2051 P=/images/ D=16877 root root 0 1383334897 1382366087 1383559354
Client: cl2
Policy: test
Backup ID: cl2_1383334895
Backed up: Fri 01 Nov 2013 02:41:35 PM CD (1383334895)
Software Version: ?
Policy Type: Standard
Schedule Type: FULL
Version: 10
Keyword: ?
Num Files: 1
Files:
FN=1 L=0 PL=19 DL=50 BK=8 II=1 RS=0 GB=0 DN=2051 P=/images/ D=16877 root
root 0 1383331790 1382366087 1383296672

SEE ALSO

See bparchive on page 51.
**bpgetconfig**

bpgetconfig – get configuration information

**SYNOPSIS**

```
bpgetconfig -M master [-x | -X | -d | -D] [config_item ...]
bpgetconfig [-u | -h] [-x | -X | -d | -D] [config_item ...]
bpgetconfig -g server [-L | -U | -l] [-c] [-A]
bpgetconfig -s server [-L | -U | -l] [-c] [-A]

bpgetconfig -i | -e filename client [policy [schedule]]
bpgetconfig -private_exld_list
```

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\

**DESCRIPTION**

bpgetconfig can be used as a stand-alone program or as a helper program for the backuptrace and the restoretrace commands to obtain configuration information. This command is available for all NetBackup server platforms. It displays the configuration information of a specified server in various formats.

bpgetconfig also retrieves general host information from a specified host server by using the -g or -s option.

You must have administrator privileges to run this command.

**OPTIONS**

- **-A**
  
  Displays all available system information. The -A option can be used only with the -g or -s option.
-c
Displays the ciphers, one per line, that are appended to the -g or -s option output. The -c option can be used only with the -g or -s option.

-D | -d
The -D option returns a listing of configuration entry names, the existing configuration values in brackets, and the default configuration values in parentheses. This operation can be performed locally or remotely. The remote machine with an identical version of NetBackup is installed. The -D and -d options may be combined with the -M, -h, and -u options.

The following is a portion of a full display of all configuration items:

```
REQUEST_DELIVERY_TIMEOUT [300] (300)
DISABLE_SCSI_RESERVE [NO] (NO)
Time_Overlap [60] (60)
Buffer_Size [16] (16)
Use_Archive_Bit [YES] (YES)
Perform_Default_Search [YES] (YES)
Accumulate_Files [NO] (NO)

...```

The -d option functions like the -D option, except -d displays only the entries that are changed from the configuration defaults. The following is an example display:

```

PEM_VERBOSE [-1] (0)
JM_VERBOSE [-1] (0)
RB_VERBOSE [-1] (0)
CONNECT_OPTIONS [**configured**] ()
Exclude [**configured**] ()
Browser [host1.min.vrts.com] ()
AUTHENTICATION_DOMAIN [**not configured**] ()
VXSS_NETWORK [**not configured**] ()
PREFERRED_NETWORK [**not configured**] ()

...```

-e filename server [class [schedule]]
Retrieves the exclude_list file from server and writes it to the location specified by filename. The policy and schedule qualifiers allow the exclude_list.policy file and the exclude_list.policy.schedule to be retrieved. The files in the exclude list are excluded from being backed up.
This option applies only to UNIX.

`-g server`
Selects the host server (server) for which the following general NetBackup information appears:
- Master or Client
- NetBackup Client Platform
- NetBackup Client Protocol Level
- Product Type
- Version Name
- Version number
- Installed Path for NetBackup Bin
- Installed OS for host server

`-h`
Displays the default local host configuration.

`-i filename server [class [schedule]]`
Retrieves the include_list file from server and writes it to the location specified by filename. The class (policy) and schedule qualifiers allow the include_list file and the include_list.class.schedule to be retrieved. The files in the include list are the exceptions to the exclude list. They are therefore included in a backup operation.

This option applies only to UNIX.

`-L`
Displays a long, user-readable list. The `-L` option can be used only with the `-g` or `-s` option.

`-l`
Displays a compact, machine-readable list. The `-l` option can be used only with the `-g` or `-s` option.

`-M master`
Specifies the master server (master) whose host configuration appears.

`-private_exld_list`
Lists all the directories and files that are excluded by default from a backup.

`-s server`
Selects the host server (server) for which `bpgetconfig` outputs the following field information:
■ Field 1 = Server type (master, media, or client)
■ Field 2 = OS type of the specified server
■ Field 3 = NetBackup client protocol level
■ Field 4 = NetBackup product type (e.g., NetBackup)
■ Field 5 = NetBackup version name (e.g., 8.0)
■ Field 6 = NetBackup version number (e.g., 800000)
■ Field 7 = Installation path to the NetBackup bin on the server
■ Field 8 = Installed OS for host server

-t
Displays the tier information, one item per line, that is appended to the -s option output. The -t option can be used only with the -g or -s option.

-U
Displays a brief, user-readable list (default). The -U option can be used only with the -g or -s option.

-u
Displays the current user configuration.

-X
Lists all configuration items by default. The -x and -X options may be combined with the -M, -h, and -u options. The -x and -X options have no effect if one or more configuration items are specified on the command line.

If config_item is specified, it appears on the specified configuration items.

-x
Excludes the items not explicitly listed in the configuration.

EXAMPLES

Example 1 - Retrieve the VERSIONINFO option setting from the bp.conf file.

# bpgetconfig VERSIONINFO
VERSIONINFO = "SunOS" 5.9" "Unknown" "NetBackup" 8.0" 800000

Example 2 - Retrieve all available system information and display a long, user-readable list.

# bpgetconfig -s hagar -A -L
Client/Master = Master
NetBackup Client Platform = Solaris9
NetBackup Client Protocol Level = 8.0
Product = NetBackup
Version Name = 8.0
Version Number = 800000
NetBackup Installation Path = /usr/openv/netbackup/bin
Client OS/Release = SunOS 5.9
Cipher =
Patch Level = 8.0

Example 3 - On a UNIX system, retrieve the file `exclude_list` from client `sun01` and write it to `sun01_exclude_list` in directory `/usr/openv/netbackup/lists`.

# bpgetconfig -e /usr/openv/netbackup/lists/sun01_exclude_list sun01

Example 4 - Retrieve the list of directories and files that are by default excluded from a backup.

#bpgetconfig -private_exld_list

Total Number of Entries in Exclude List : 23
/usr/openv/var/global/vxss/
/usr/openv/var/global/wsl/credentials/
/usr/openv/var/session/
/usr/openv/var/vxss/at/
/usr/openv/var/vxss/credentials/
/usr/openv/var/vxss/crl/
/usr/openv/var/websvcccreds/
/usr/openv/var/global/wmc/cloud/*.pem
/usr/openv/var/global/webrootcert.pem
/usr/openv/var/global/.yekcnedwssap
/usr/openv/var/global/jkskey
/usr/openv/var/keyfile.dat
/opt/VRTSnbu/var/global/vxss/
/opt/VRTSnbu/var/global/wsl/credentials/
/opt/VRTSnbu/var/session/
/opt/VRTSnbu/var/vxss/at/
/opt/VRTSnbu/var/vxss/credentials/
/opt/VRTSnbu/var/vxss/crl/
/opt/VRTSnbu/var/websvcccreds/
/opt/VRTSnbu/var/global/webrootcert.pem
/opt/VRTSnbu/var/global/.yekcnedwssap
/opt/VRTSnbu/var/global/jkskey
/opt/VRTSnbu/var/keyfile.dat
SEE ALSO

See `bpsetconfig` on page 416.

See `nbgetconfig` on page 714.

See `nbsetconfig` on page 831.
bpgetdebuglog

bpgetdebuglog – Run helper program for backuptrace and restoretrace. Prints out debug log file. Useful as a stand-alone program.

SYNOPSIS

bpgetdebuglog remote_machine [remote_program mmddyy
[user_name|user_name@domain_name]]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

If all arguments are specified, bpgetdebuglog prints the contents of the specified debug log file to standard output. If only remote_machine is specified, bpgetdebuglog prints to standard output the number of seconds of clock drift between the local computer and the remote machine. A positive number means that the local computer is ahead of the remote machine. A negative number means that the remote machine is ahead of the local computer.

If the user_name option is specified, the command fetches only those log files which are appended with the specified user name. On Windows platforms, the command input format requires username along with the machine or domain name (user_name@domain_name). For the log folders that do not have read-access granted, the command returns a Permission Denied error.

The bpgetdebuglog command must be in the specified directory (see SYNOPSIS) for backuptrace and restoretrace to use it.

You must have administrator privileges to run this command.

OPTIONS

remote_machine
    Name of the remote server.

remote_program
    Name of the debug log directory on the remote server.
The day stamp that is used to identify the log file (log.mmmddyy for UNIX, mmmddyy.log for Windows) to be read.

The name of the user for whom the debug log files are fetched.

The name of a non-administrator user along with the domain name or machine name from where the debug log files are fetched.

**EXAMPLES**

```
# bpgetdebuglog peony bpcd 071214
# bpgetdebuglog peony
# bpgetdebuglog peony bpcd 071214 Bob@example
```
bpimage

bpimage – perform functions on stored images in a database

SYNOPSIS

bpimage -[de]compress [-allclients | -client name] [-M master_server,...] [-update_compression]

bpimage -npc copy_number -backupid backupid [-client name] [-M master_server,...]

bpimage -newservice newservice_name [-oldserver oldserver_name] [-id id] [-M master_server,...]

bpimage -deletecopy copy_number -backupid backupid [-M master_server,...]

bpimage -testlock copy_number -backupid backupid [-M master_server,...]

bpimage -prunetir [-allclients | -client name] -cleanup [-notimmediate] [-M master_server,...]

bpimage -cleanup_image_change_log [-M master_server,...]

bpimage -gendrreport -backupid backupid [-M master_server,...]

bpimage -wff path bytes -backupid backupid [-client name] [-M master_server,...]

bpimage -update [-rfile 0|1 | -filesysonly 0|1 | -numfiles number | -keyword keyword_phrase | -objdesc string] [-client name -policy name -t type -d mm/dd/yyyy hh:mm:ss] [-id id] [-M master_server,...]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd

DESCRIPTION

This command can be used to perform many different functions to images that are stored in a database. Some of the functions are as follows:
- Compress and decompress the stored images.
- Remove existing images from the database.
- Test the locking capability on an image.

OPTIONS

The following options represent the criteria that determine which images or media are selected for the report. Where images are discussed in these options, media can be substituted if the context refers to a media report.

-allclients

Selects all NetBackup clients that are already backed up on the system.

-backupid backup_id

Specifies a backup ID to use for finding applicable images.

-cleanup

Deletes expired images, compresses the images that are scheduled to be compressed, and prunes the TIR information from the specified images.

Note: This option enables a user to accomplish the same tasks manually that the scheduler performs on a regular basis. It can be used when the user does not have enough time to wait for the scheduler to perform these tasks.

-cleanup_image_change_log

Cleans up the image change on the current master server and optionally, on other master servers that are specified by the -M option.

-client name

Specifies a client name to use for finding backups or archives on which to perform the specified function. The client name that bpimage searches for is case insensitive. For example, bpimage displays images from client, cLiEnT, and CLIENT. By default, bpimage searches for images on all clients.

-d date

Specifies the start date and end date range for the listing.

-d specifies a start date and time for the listing. The list shows only images in backups or the archives that occurred at or after the specified date and time.

The required date and time values format in NetBackup commands varies according to your locale. The /usr/openv/msg/.conf file (UNIX) and the install_path\VERITAS\msg\LC.CONF file (Windows) contain information such
as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

For more about the locale of your system, see "About specifying the locale of the NetBackup installation" in the NetBackup Administrator's Guide, Volume II.

The valid range of dates is from 01/01/1970 00:00:00 to 01/19/2038 03:14:07. The default is the previous midnight.

-decompress
  Initiates compression or decompression of a specified client or all clients.

-deletecopy copy_number
  Removes the images that the copy number and the backup_id specify.

-filesysonly 0|1
  Limits bpimage to query only the local file system if set to 1.

-gendrreport
  Generate a disaster recovery report for the specified backup_id.

-id id
  Specifies the media ID when used with the -newserver command or specifies the backup ID when used with the -update command.

-keyword "keyword_phrase"
  Specifies a keyword phrase for NetBackup to use when it searches. The phrase must match the phrase that was previously associated with the image.

-M master_server,...
  Specifies a list of alternative master servers. This list is a comma-delimited list of hostnames. Each master server in the list runs the bpimage command. If an error occurs for any master server, the process stops at that point.

  The report is the composite of the information that all the master servers in this list returns. bpimage queries each of these master servers. The master server returns image or media information from the image catalogs. Each master server must allow access by the system that issues the bpimage command.

  The default is the master server for the system running bpimage.

-newserver name | -oldserver name
  Specifies the new name or the old name of a NetBackup server.

-notimmediate
  Inhibits the call that bpexpdate makes to the nbdelete command after it expires an image on disk. If you intend to delete many images at the same time, use
-notimmediate to avoid the overhead of multiple job creation for nbdelete to process. You can run the nbdelete command later.

-npc copy_number
   Sets the specified image as the primary image, which is based on the copy number of the image.

-numfiles number
   Specifies the number of files when used with the -update command.

-objdesc string
   Specifies the object description string of the Informix client type when used with the -update command.

-policy name
   Searches for backups to import in the specified policy. The default is all policies.

-prunetir
   Prunes the true image restore (TIR) information from the specified clients. The default is all clients.

-rfile 0|1
   Use the Restore file when used with the -update command.

-t type
   Specifies a policy type. By default, bpimage searches for all policy types. type is one of the following character strings:

   Informix-On-BAR
   MS-Exchange-Server
   MS-SQL-Server
   MS-Windows
   Oracle
   Standard
   Sybase
   NDMP

The following policy types apply only to NetBackup Enterprise Server:

   BigData
   DataTools-SQL-BackTrack
   DB2
   FlashBackup
   SAP
   Split-Mirror
-testlock
Determines if the copy for the specified backup ID is locked.

-update
Updates an image that is based on the chosen parameter.

-update_compression
Tells NetBackup to uncompress the images that were compressed with the old compression algorithm and recompress them with the new algorithm. The -update_compression flag only applies used with the -compress option.

A new compression algorithm was deployed with NetBackup 7.6. With the old algorithm, the NetBackup .f files have a file name extension of .Z on Linux or UNIX. With the new algorithm, they have either a .zs or .zl extension. The .zs extension designates the files that are compressed with user-specified scripts and is only used on Linux and UNIX. The .zl extension is for the files that are compressed internally by NetBackup and is used on Windows, Linux, and UNIX platforms.

-wff path bytes
Writes the files file (image .f file) for the backup that is specified with -backupID.

EXAMPLES

Example: This example determines if the specified copy for the backup ID is locked.

# bpimage -testlock 1 -backupid abc123.server.domain.com_1416316372
Backupid abc123.server.domain.com_1416316372 copy 1 is not locked
bpimagelist

bpimagelist — produce status report on NetBackup images or removable media

SYNOPSIS


On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd

DESCRIPTION

bpimagelist uses a specified format to report on catalog images or the removable media that matches the attributes that are sent from the command options. bpimagelist reports on the removable media if the -media option is on the command line. If not, it reports on the catalog images.

The bpimagelist -changelog option reports on records in the image change log. You can filter the report to only new images, updated images, or deleted images. It writes its debug log information to the following directory:

On UNIX systems: /usr/openv/netbackup/logs/admin

On Windows systems: install_path\NetBackup\logs\admin

You can use the information in this directory for troubleshooting.
The output of `bpimagelist` goes to standard output.

Authorized users can run this command.

For more about NetBackup authorization, see the *NetBackup Security and Encryption Guide*.

**Note:** For the NetBackup Accelerator feature, `bpimagelist` reports the amount of data that was transferred over the network for each backup. You can also configure the command to show the transferred data in the field that normally shows the Accelerator backup image size. For details, see the Accelerator topics in the *NetBackup Administrator's Guide Volume I*, the *NetBackup for VMware Administrator's Guide*, and the *NetBackup for NDMP Administrator’s Guide*.

## OPTIONS

The following are the `bpimagelist` options:

- `-backupid backup_id`
  - Specifies a backup ID to use for finding applicable images (applies only to the image list).

- `-changelog`
  - Reports on the records from the image change log.

- `-class_id class_guid`
  - Specifies a class identifier to use to select images. The identifier represents a GUID (globally unique identifier). The `bpimagelist` command reports only those images with the specified class identifier.

- `-client client_name`
  - Specifies a client name to use for finding backups or archives to list. The client name that `bpimagelist` searches for is case insensitive. For example, `bpimagelist` displays images from `client`, cLiEnT, and CLIENT. By default, `bpimagelist` searches for all clients.

- `-d mm/dd/yy hh:mm:ss`, `-e mm/dd/yy hh:mm:ss`
  - Specifies the start date and end date range for the listing. If these values are not included on the command line, the default values are as follows:
    - The `-d` default is the previous midnight.
    - The `-e` default is the current date and time.

  The complete format of the start date and end date is as follows:
-d specifies a start date and time for the listing. The output list shows only images in backups or the archives (or data in the change log for the \texttt{-changelog} option) that occurred at or after the specified date and time.

-\texttt{e} specifies an end date and time for the listing. The output list shows only files from backups or the archives (or data in the change log for the \texttt{-changelog} option) that occurred at or before the specified date and time. Use the same format as for the start date.

The valid range of dates is from 01/01/1970 00:00:00 to 01/19/2038 03:14:07. The required date and time values format in NetBackup commands varies according to your locale. The \texttt{/usr/openv/msg/.conf} file (UNIX) and the \texttt{install_path\VERITAS\msg\LC.CONF} file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

For more about the locale of your system, see "About specifying the locale of the NetBackup installation" in the \textit{NetBackup Administrator's Guide, Volume II}.

-\texttt{hoursago hours}

Includes the images that were written up to this many hours ago. This option is equivalent to a specification of a start time (\texttt{-d}) of the current time minus \texttt{hours}. \texttt{hours} must be 1 or greater.

-\texttt{idonly}

Produces an abbreviated list. For an image list, the list contains the creation time, backup ID, and schedule type of each image. For instance, if the list criterion is a window of time, the image list contains the following: For each image that is created in this window, only the creation time, backup ID, and schedule type of the image.

For a media list, the list contains only the applicable media IDs. For instance, if the list criterion is a window of time, the list contains only the media IDs that are written in this window.

The following options represent the criteria that determine which images or media are selected for the report. Where images are discussed in these options, media can be substituted if the report is a media report.

-\texttt{inter-domain}

Displays placeholder copies of images that have been replicated from the source and replicated images that are pending import on the target.

-\texttt{json}

Prints the data in \texttt{json} format and spans multiple lines.
-\texttt{json\_compact}

Prints the data in \texttt{json} format on a single line.

-\texttt{keyword "keyword\_phrase"}

Specifies a keyword phrase for NetBackup to use when it searches. The phrase must match the one that was previously associated with the image. For instance, the -\texttt{k} option of the \texttt{bpbackup} or the \texttt{bparchive} command associates a keyword with the image when the image is created.

-\texttt{-L}

Generates the report in Long mode. For instance, for the Media List report, the report lists the information for each media ID as a series of \texttt{attribute = value} pairs. The density value is provided as both a descriptive term and a number. Long mode is the default condition.

-\texttt{-l}

Reports in Short mode, which produces a terse listing. This option is useful for the scripts or programs that rework the listing contents into a customized report format.

-\texttt{-M master\_server,...}

Specifies a list of one or more alternative master servers. This list is a comma-delimited list of hostnames. If this option is present, each master server in the list runs the \texttt{bpimagelist} command. If an error occurs for any master server, the process stops at that point.

The report is the composite of the information that all the master servers in this list return. \texttt{bpimagelist} queries each of these master servers. The master server returns image or media information from the image catalogs. Each master server must allow access by the system that issues the \texttt{bpimagelist} command.

The default is the master server for the system running \texttt{bpimagelist}.

-\texttt{-media}

Specifies that the listing reports on the removable media that are based on a set of criteria. If -\texttt{media} is not in the command line, the report is on images, not media.

-\texttt{-min\_changelog\_key key}

Prints records with the specified log key and newer. Newer change log entries have greater change log key values.

[-\texttt{new\_images}] [-\texttt{updated\_images}] [-\texttt{deleted\_images}]

Limits the change log report to new, updated, or deleted images. The default condition is to report all change log images.
-option option_name,...

Specifies one or more criteria for finding images to list. option_name is one of the following character strings in uppercase or lowercase:

- **INCLUDE_PRE_IMPORT** - Report the images that completed phase 1 of an import.
- **INCLUDE_TIR** - Report the images that true-image-recovery backups created.
- **LIST_COMPLETE_COPIES** - Do not report fragments of a duplicate copy that is still in process.
- **LIST_OLD_TO_NEW** - Report images by oldest to newest date.
- **ONLY_PRE_IMPORT** - Report only the images that completed phase 1 of an import.
- **ONLY_TIR** - Report only the images that true-image-recovery backups created.

The default is no restrictions on the selected images.

-**oracle_copilot_ir**

Searches for and displays the images that may be used for Oracle Copilot Instant Recovery.

-**policy name**

Searches for backups to import in the specified policy. The default is all policies.

-**pt policy_type**

Specifies a policy type. By default, bpimagelist searches for all policy types.

The **policy_type** is one of the following character strings:

BigData
DataStore
DataTools-SQL-BackTrack
DB2
Enterprise-Vault
FlashBackup
FlashBackup-Windows
Hyper-V
Informix-On-BAR
LotusNotes
MS-Exchange-Server
MS-SharePoint
MS-SQL-Server
MS-Windows
NDMP
Oracle
PureDisk-Export
SAP
Split-Mirror
Standard
Sybase
Vault
VMware

-rl retention_level
Specifies the *retention_level*. The *retention_level* is an integer between 0 and 100. By default, `bpimagelist` searches for all retention levels.

**Note:** If you run this command on a pre-NetBackup 8.0 media server, you can only specify a retention level between 0 and 24.

-server server_name
Specifies the name of a NetBackup server or ALL. If `-server` specifies a server name, then the images or media in the report are only those that reside on that server. The images also satisfy the other criteria that `bpimagelist` specifies. For instance, if `-hoursago 2` is specified, the media must contain an image that was created in the past two hours.

The query goes to the image catalog that resides on the local master server. The master server must allow access by the system running `bpimagelist`.

The default is to report all media in the image catalog on the local master server, which is equivalent to the specification of `-server ALL`.

-sl sched_label
Specifies a schedule label for the image selection. The default is all schedules.

-st sched_type
Specifies a schedule type for the image selection. The default is any schedule type. Valid values are as follows:

- **FULL** (full backup)
- **INCR** (differential-incremental backup)
- **CINC** (cumulative-incremental backup)
- **UBAK** (user backup)
- **UARC** (user archive)
- **NOT_ARCHIVE** (all backups except user archive)
-stl_complete
Reports only the images that the storage lifecycle completely processed. This option cannot be used with the stl_incomplete option.

-stl_incomplete
Reports only the images that the storage lifecycle has not completely processed. This option cannot be used with the stl_complete option.

-stl_name storage_lifecycle_name
Specifies a storage lifecycle name to be used when you select images. Only images with the specified storage lifecycle name are selected.

tape
Displays in the list only the images that have at least one fragment that resides on removable or tape-based media. Any disk-based fragments in these images are ignored. If an image has fragments on both tape and disk, this option displays only the tape-based fragments.

-U
Generates the report in User mode. The report is formatted. It includes a banner that lists the column titles. The status is a descriptive term instead of a number.

-v
Selects the verbose mode. This option causes bpimagelist to log additional information for debugging purposes. The information goes into the NetBackup administration daily debug log. This option is meaningful only when the debug log function is enabled; that is, when the following directory is defined:

UNIX systems: /usr/openv/netbackup/logs/admin
Windows systems: install_path\NetBackup\logs\admin

EXAMPLES

Example 1 - Show the last time the media IDs available to the server had a backup image that was written during the specified time:

```bash
# bpimagelist -media -d 01/05/2012 18:00:46 -e 01/06/2012 23:59:59 -U
```

<table>
<thead>
<tr>
<th>Media ID</th>
<th>Last Written</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM000</td>
<td>01/06/2012 01:06</td>
<td>hatt</td>
</tr>
<tr>
<td>AEK800</td>
<td>01/06/2012 03:01</td>
<td>hatt</td>
</tr>
<tr>
<td>C0015</td>
<td>01/06/2012 02:01</td>
<td>hatt</td>
</tr>
<tr>
<td>143191</td>
<td>01/05/2012 23:00</td>
<td>hatt</td>
</tr>
</tbody>
</table>

Example 2 - List all images that were written today:

```bash
# bpimagelist -tape
```
Example 3 - List all the images that the storage lifecycle has not completely processed that were written today:

```
# bpimagelist -U -stl_incomplete -idonly
```

```
Time: 12/6/2011 1:03:46 PM ID: escape_1323198226 FULL (0)
Time: 12/6/2011 1:02:42 PM ID: louisebl8vm1_1323198162 FULL (0)
Time: 12/6/2011 1:03:28 PM ID: monterrey_1323198208 FULL (0)
Time: 12/6/2011 1:03:10 PM ID: oprahl14vm3_1323198190 FULL (0)
Time: 12/6/2011 1:03:11 PM ID: oprahl14vm4_1323198191 FULL (0)
Time: 12/6/2011 1:03:12 PM ID: oprahl15vm3_1323198192 FULL (0)
Time: 12/6/2011 1:03:17 PM ID: oprahl15vm4_1323198197 FULL (0)
Time: 12/6/2011 1:02:22 PM ID: oprahl8vm5_1323198142 FULL (0)
Time: 12/6/2011 1:02:41 PM ID: thelmab11vm1_1323198161 FULL (0)
Time: 12/6/2011 1:02:54 PM ID: thelmab11vm2_1323198174 FULL (0)
Time: 12/6/2011 1:03:01 PM ID: thelmab12vm1_1323198181 FULL (0)
```

Example 4 - List all the incomplete images that were written today for the pem_tort policy:

```
# bpimagelist -U -stl_incomplete -policy pem_tort
```

```
Backed Up     Expires    Files   KB  C  Sched Type   ...  Policy
------------- ---------- ----- ------ - ------------ ---
12/06/2011 13:03 12/12/2011 86 1632 N Full Backup ... pem_tort
12/06/2011 13:02 12/12/2011 12 12512 N Full Backup ... pem_tort
12/06/2011 13:03 12/12/2011 5 32 N Full Backup ... pem_tort
12/06/2011 13:03 12/12/2011 3742 95936 N Full Backup ... pem_tort
12/06/2011 13:03 12/12/2011 3762 95936 N Full Backup ... pem_tort
12/06/2011 13:03 12/12/2011 8 64 N Full Backup ... pem_tort
12/06/2011 13:03 12/12/2011 9 32 N Full Backup ... pem_tort
12/06/2011 13:02 12/12/2011 5041 223104 N Full Backup ... pem_tort
12/06/2011 13:02 12/12/2011 6 32 N Full Backup ... pem_tort
```
Example 5 - List the new and updated change log entries entered since May 2, 2012:

```
# bpimagelist -changelog -new_images -updated_images -d 05/02/2012 10:18:00 -json
Image Change Log Key: 2
Backup ID: jumpmanvm2_133597123
Client Type: Standard (0)
Image Change Log Oper. Id: Updated (2)
```

FILES

UNIX systems:

```
/usr/openv/netbackup/logs/admin/log.mmddyy
/usr/openv/netbackup/db/images
```

Windows systems:

```
install_path\NetBackup\logs\admin\log.mmddyy
install_path\NetBackup\db\images
```

SEE ALSO

See bp on page 49.
See bparestore on page 382.
bpimmedia

bpimmedia – display information about NetBackup images on media

SYNOPSIS

```
```

```
bpimmedia -spanpools [-cn copy_number] [-mediald media_id] [-U]
```

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\

DESCRIPTION

bpimmedia queries the NetBackup image catalog and produces the following two types of reports on the images:

- An Images-on-Media report
- A Spanpools report

The first form of bpimmedia in the SYNOPSIS displays a set of NetBackup images in the Images-on-Media report. This report lists the contents of media as recorded in the NetBackup image catalog.

You can generate this report for any medium including disk. Filter the report contents according to client, media ID, path, and so on.

for more about the fields in the Images-on-Media report, see NetBackup Reports in the NetBackup Administrator’s Guide, Volume II.

The report does not show information for the media that is used in backups of the NetBackup catalogs.

Several options (-dt, -dp, -dv, -stype) report images present on SAN disk storage only, not on any other disk-resident images. Other options and output format continue to function as before.
The second SYNOPSIS form of `bpimmedia` uses `-spanpools` to list the disk ID pools that are related because images span from one volume to another. The output lists, for each media server in the cluster, the media IDs that have spanned images. The `-spanpools` form of `bpimmedia` must be run on the NetBackup master server that administers the volumes.

For more about spanned images, see "Spanning Media" in the NetBackup Administrator's Guide, Volume II.

Only removable media types are processed.

`bpimmedia` sends its error messages to stderr. `bpimmedia` sends a log of its activity to the NetBackup admin log file for the current day.

Authorized users can run this command.

For more about NetBackup authorization, see the NetBackup Security and Encryption Guide.

**OPTIONS**

`client client_name`

Client name. This name must be as it appears in the NetBackup catalog. By default, `bpimmedia` searches for all clients.

`-cn copy_number`

Copy number (1 or 2) of a backup ID. The default is copy 1. This option is used only in combination with `-spanpools`.

`-d date time, -e date time`

Specifies the start date and end date range for the listing.

`-d` specifies a start date and time for the listing. The output list shows only images in backups or the archives that occurred at or after the specified date and time.

`-e` specifies an end date and time for the listing. The output list shows only files from backups or the archives that occurred at or before the specified date and time. Use the same format as for the start date. The default is the current date and time.

The valid range of dates is from 01/01/1970 00:00:00 to 01/19/2038 03:14:07. The default is the previous midnight.

The required date and time values format in NetBackup commands varies according to your locale. The `/usr/openv/msg/.conf` file (UNIX) and the `install_path\VERITAS\msg\LC.CONF` file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.
For more about the locale of your system, see "About specifying the locale of the NetBackup installation" in the NetBackup Administrator's Guide, Volume II.

```
-dp disk_pool_name
Displays the images on the specified disk pool only.
```

```
-dt disk_type
Specifies the type of disk storage. The following are valid options:
1 - BasicDisk
3 - SnapVault
This option does not apply to the OpenStorage disk type.
```

```
-dv disk_volume
Displays the images that reside on the specified disk volume only. The input value is the path for BasicDisk.
```

```
-L
The list type is long.
See the DISPLAY FORMATS section that follows.
```

```
-l
The list type is short. This setting is the default if the command line has no list-type option (for example, if you enter bpimmedia and a carriage return).
See the DISPLAY FORMATS section that follows.
```

```
-legacy
Formats the new data in legacy format.
```

```
-M master_server,...
A list of alternative master servers. This list is a comma-separated list of hostnames. If this option is present, the command is run on each of the master servers in this list. The master servers must allow access by the system that issues the command. If an error occurs for any master server, the process stops at that point in the list. The default is the master server for the system where the command is entered.
```

```
-mediaid media_id | pathname
This ID is either a VSN or an absolute pathname. If the media ID is a VSN, it is a one- to six-character string. If the media ID is a pathname, it is the absolute pathname of the file system for a disk storage unit.

When -mediaid is specified, the Images-on-Media report displays only the images that are stored on this VSN or pathname. By default, the report displays the images that are stored on all media IDs and pathnames.
```
For the Spanpools report (-spanpools), only a VSN can follow -mediaid. If -mediaid is omitted when -spanpools is present, bpimmedia displays all media in all spanning pools.

-mtype image_type

Image type. The defined values and their interpretations are as follows:

- 0 = Regular backup (scheduled or user-directed backup)
- 1 = Pre-imported backup (phase 1 completed)
- 2 = Imported backup

-option option_name

Specifies a criterion for finding images to list. option_name is one of the following character strings, in either uppercase or lowercase:

- INCLUDE_PRE_IMPORT - Include images that completed phase 1 of an import.
- ONLY_PRE_IMPORT - Include only the images that completed phase 1 of an import.

The default is INCLUDE_PRE_IMPORT.

-policy policy_name

Searches for images with the specified policy name. By default, bpimmedia searches for images for all policies.

-rl retlevel

Specifies the retention_level. The retention_level is an integer between 0 and 100. By default, bpimmedia searches for all retention levels.

Note: If you run this command on a pre-NetBackup 8.0 media server, you can only specify a retention level between 0 and 24.

-sl sched_label

Searches for images with the specified schedule label. By default, bpimmedia searches for images for all schedule labels.

-spanpools

Specifies that bpimmedia should create a Spanpools report. The default (-spanpools not present on the command line) is to create an Images-on-Media report.

-stype server_type

Specifies a string that identifies the storage server type. The server_type value can originate from one of the following sources:
- Veritas provided storage. Possible values are AdvancedDisk and PureDisk.
- Third-party disk appliances. The vendor supplies the server_type string.
- Cloud storage. Use the csconfig clidprovider -l command to determine the possible stype values. The cloud stype values reflect the cloud storage provider. Cloud storage stype values can also incorporate a suffix (for example, amazon_crypt). Possible suffixes are:
  - _raw: The NetBackup backup image is sent to the cloud in raw format. Use this option if you do not want to compress or encrypt data before sending to cloud storage.
  - _rawc: Compresses the data before it is written to the cloud storage.
  - _crypt: Encrypt the data using AES-256 encryption before writing the data to cloud storage. You must have KMS configured in NetBackup to use this option.
  - _cryptc: Compress and encrypt the data before writing to cloud storage.

The storage server type is case sensitive.

-t sched_type
  Specifies a schedule type for the image selection. The default is any schedule type. Valid values, in either uppercase or lowercase, are as follows:
  - FULL (full backup)
  - INCR (differential-incremental backup)
  - CINC (cumulative-incremental backup)
  - UBAK (user backup)
  - UARC (user archive)

-tape
  Displays in the Images-on-Media report only the images that have at least one fragment that resides on removable or tape-based media. Disk-based fragments in these images are ignored. If an image has fragments on both tape and disk, this option displays only the tape-based fragments.

-U
  The list type is user. This option is used only in combination with -spanpools.
  See the DISPLAY FORMATS section that follows.

-verbose
  Select verbose mode for logging. This option is only meaningful when it runs with debug logging on; that is, when the following directory is defined:
DISPLAY FORMATS

IMAGES-ON-MEDIA REPORT

The Images-on-Media report consists of two formats, short (-l or default) and long (-L).

To process and use the output of `bpimmedia`, use the -l option. The output of `bpimmedia` that uses the -L or -U options may be truncated for the Backup-ID, Policy, and Host columns. The -L or -U options are useful when you want to obtain a quick, more readable view of the NetBackup images on media.

The following shows the long display format (-L) and the short display format (-l) of the Images-on-Media report:

- Long Display Format (-L)
  If the command line contains -L, the display format is long. It contains a multi-line entry for each backup image. The number of lines for an entry is n+1, where n is the number of fragments for the image. The fields for an entry are listed later. The first line of the entry contains the fields Backup_ID...Expires. Each fragment in the image has a line that contains the fields Copy_Media ID. The report has a two-line header. The first header line lists the field names for line 1 of each entry. The second header line lists the field names for the lines that contain fragment information.

  See the `bpduplicate` command page for more information on the copy number and primary copy.

  Fields and meanings for the -L format are as follows:
  
  Line 1
  Backup-ID - Unique identifier for the backup that produced this image
  Policy - Policy name (may be truncated if long)
  Type - Schedule type (FULL, etc.)
  RL - Retention level (0.100)

  **Note:** If you run this command on a pre-NetBackup 8.0 media server, the output only displays the retention levels between 0 and 24.

  Files - Number of files in the backup
  C - Compression (Y or N)
  E - Encryption (Y or N)
  T - Image type
**R** - Regular (scheduled or user-directed backup)

**P** - Pre-imported backup (phase 1 completed)

**I** - Imported backup

**PC** - Primary copy, 1 or 2. Designates which copy of the backup NetBackup chooses when it restores.

**Expires** - The expiration date of the first copy to expire, which appears in the Expires field of the fragment, which is described later.

**Line 2_{n+1}**

**Copy** - Copy number of this fragment

**Frag** - Fragment number or IDX for a true-image-restore (TIR) fragment

**KB** - Size of the fragment, in kilobytes. This value does not include the size of tape headers between backups. A fragment size of 0 is possible for a multiplexed backup.

**Type** - Media type (Rmed - removable media; Disk otherwise)

**Density** - Density of the removable media that produced the backup

**Fnum** - File number; the n-th backup on this removable media

**Host** - Server whose catalog contains this image

**DWO** - Device Written On; device where the backup was written. The DWO matches the drive index as configured in Media Manager (applies only to removable media).

**MPX** - Flag that indicates whether this copy is multiplexed: Y or N (applies only when fragment number is 1)

**Expires** - The expiration date of this copy (applies only when fragment number is 1)

**MediaID** - Media ID or absolute path where the image is stored

**Example of Long display format:**

```
bpimmedia -L -policy regrl_gava -t FULL
Backup-ID Policy Type RL Files C E T PC Expires
Copy Frag KB Type Density FNum Host DWO MPX Expires MediaID
----------------------------------------------------------------
gava_0949949902 r1_guav FULL 3 25 N N R 1 12:58 03/09/2012
1 1 256 RMed dlt 13 0 plim 0 Y 12:58 03/09/2012 A00002
```

**Short Display Format (-l)**

If the `bpconfig` command line contains `-l` or contains no list-format option, the display format is short, which produces a terse listing. This option can be useful for scripts or the programs that rework the listing into a customized report format. The `-l` display format contains a multi-line entry for each backup image. The number of lines per entry is n+1, where n is the number of fragments for the image. The layout of an entry is a first line that contains information about the image. A second line follows that contains information about each fragment of the image. The attributes appear in the following order (separated by blanks).
Fields for the `-l` format are as follows:
Field 1 = Client. The name of the image's client.
Field 2 = Version. The NetBackup version of the client.
Field 3 = Image keyword. The keyword for the backup image.
Field 4 = Policy name. The name of the policy that created the image.
Field 5 = Policy type. 0=Standard, 4=Oracle, 8=Sybase, 9=MS-SharePoint
Field 6 = Schedule - Schedule name that is run to create the backup.
Field 7 = Schedule type. 0=Full, 1=Differential incremental, 2=User-directed backup, 3=User-directed archive, 4=Cumulative incremental
Field 8 = Retention level (0-100).

**Note:** If you run this command on a pre-NetBackup 8.0 media server, the output only displays the retention levels between 0 and 24.

0 = 1 week, 4mm cartridge media
1 = 2 weeks, 8mm cartridge media
2 = 3 weeks, 8mm2 cartridge media
3 = 1 month, 8mm3 cartridge media
4 = 2 months, dlt cartridge media
5 = 3 months, dlt2 cartridge media
6 = 6 months, dlt3 cartridge media
7 = 9 months, dtf cartridge media
8 = 1 year, half-inch cartridge media
9-100 = infinite (except 25 which is expire immediately), half-inch cartridge 2 media

Field 9 = Number of files in the image.
Field 10 = Expiration time of the image in seconds since January 1, 1970. A value of zero (0) denotes an image in progress or failed.
Field 11 = Compression. 0=Use compression, 1=Do not use compression
Field 12 = Encryption.
Field 13 = Hold. 0=Image is not on hold, 1=Image is on hold

**Fragments**
Field 1 = Copy number
Field 2 = Fragment number
Field 3 = Fragment size in KBytes
Field 7 = File number
Field 8 = Media. The media where the image is stored.
Field 9 = The media server for the image.
Field 10 = Block size in KBytes
Field 11 = Offset
Field 12 = The time (in seconds since January 1, 1970) when the fragment was created
Field 13 = The device number where the image was written
Field 16 = Expiration time of the image in seconds since January 1, 1970. A value of zero (0) denotes an image in progress or failed.
Field 17 = Multiplexing. 0=multiplexing not used, 1=multiplexing used
Field 18 = Retention level.
  0 = 1 week, 4mm cartridge media
  1 = 2 weeks, 8mm cartridge media
  2 = 3 weeks, 8mm2 cartridge media
  3 = 1 month, 8mm3 cartridge media
  4 = 2 months, dlt cartridge media
  5 = 3 months, dlt2 cartridge media
  6 = 6 months, dlt3 cartridge media
  7 = 9 months, dlt cartridge media
  8 = 1 year, half-inch cartridge media
  9-100 = infinite (except 25 which is expire immediately), half-inch cartridge 2 media
Field 20 = Hold. 0=Fragment not on hold, 1=Fragment on hold

Example of the short display format:

```
# bpimmedia -l -policy regr1_gava -t FULL
IMAGE gava 3 gava_0949949902 regr1_gava 0 full 0 3 25 952628302 0 0
FRAG 1 1 10256 512 2 13 13 A00002 plim 65536 0 949616279 0 0 *NULL* 952628302 1
```

**SPANPOOLS REPORT**

The Spanpools report has two formats: user (-U option) and short (the default). Both formats list the server name and the pool data for each server. It lists the media IDs for each pool of media that share spanned backup images. When -mediaid appears on the command line, only the server pool and the disk pool that are related to that media ID appear.

If you want to process and use the output of bpimmedia, we recommend that you use the -l option. The output of bpimmedia that uses the -U or -L options may be truncated for the Backup-ID, Policy, and Host columns. The -U or -L options are useful when you want to obtain a quick, more readable view of the NetBackup images on media.

The user (-U) display format looks like the following:

```
# bpimmedia -spanpools -U
Related media pools containing spanned backup images, server plim:
  Pool:
    A00002  A00003
```
Pool:
400032

The short display format looks like the following

```
# bpimmedia -spanpools
SERVER plim
POOL A00002 A00003
POOL 400032
```

**EXAMPLES**

Example 1 - List the images for policy c_NDMP. This request runs on a NetBackup media server. The report is based on the image catalog on the media server's master server, almond.

```
# bpimmedia -L -policy c_NDMP
```

<table>
<thead>
<tr>
<th>Backup-ID</th>
<th>Policy</th>
<th>Type</th>
<th>RL</th>
<th>Files</th>
<th>C</th>
<th>E</th>
<th>T</th>
<th>PC</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>c_NDMP</td>
<td>FULL</td>
<td>3</td>
<td>5909</td>
<td>N</td>
<td>N</td>
<td>R</td>
<td>1</td>
<td>15:58 07/18/2012</td>
</tr>
<tr>
<td>t_0929653085</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 IDX</td>
<td>844</td>
<td>RMed</td>
<td>dlt</td>
<td>2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 1</td>
<td>9136</td>
<td>RMed</td>
<td>dlt</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CB7514

Example 2 - Display the tapes that are required to restore a particular file. If the `bpimmedia` command line provides the criteria to identify an individual backup, the output shows the media that was used for the backup.

In this case, the command line provides the client, the date of the backup and the schedule type. The output shows that tape A00002 on the server `plim` contains the backup.

```
# bpimmedia -L -client gava -d 2/7/2012 -t UBAK
```

<table>
<thead>
<tr>
<th>Backup-ID</th>
<th>Policy</th>
<th>Type</th>
<th>RL</th>
<th>Files</th>
<th>C</th>
<th>E</th>
<th>T</th>
<th>PC</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>gava_0949949686</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 1</td>
<td>10256</td>
<td>RMed</td>
<td>dlt</td>
<td>11</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>plim</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example 3 - List in long format all the backups in the image catalog on master server `gava`.

```
# bpimmedia -L -policy c_NDMP
```
# bpimmedia -L -M gava

Backup-ID          Policy   Type   RL Files C E T PC Expires
Copy Frag  KB Type Density FNum Off Host   DWO MPX Expires MediaID
-------------------------------------------------------------------------------------
gava_0949599942   test-policy FULL  1 15 N N R 1 11:45 02/17/2011
                  1 1 224 Disk - - - gava - N 11:45 02/17/2011
/var/qatest/storage_unit//gava_0949599942_C1_F1

Example 4 - List in long format the backups on media ID CB7514.

# bpimmedia -L -mediaid CB7514

Backup-ID          Policy   Type   RL Files C E T PC Expires
Copy Frag  KB Type Density FNum Off Host   DWO MPX Expires MediaID
-------------------------------------------------------------------------------------
toaster1_0929679294 tort_policy FULL  3 5898 N N R 1 23:14 07/18/2012
                  1 IDX 839 RMed dlt 4 0 almond 6 CB7514
                  1 1 27154 RMed dlt 3 0 almond 6 23:14 07/18/2012 CB7514
toaster1_0929653085 NDMP_policy FULL  3 5909 N N R 1 15:58 07/18/2012
                  1 IDX 844 RMed dlt 2 0 almond 3 CB7514
                  1 1 9136 RMed dlt 1 0 almond 3 15:58 07/18/2012 CB7514

RETURN VALUES

An exit status of zero (0) means that the command ran successfully.
Any exit status other than zero (0) means that an error occurred.
If the administrative log function is enabled, the exit status is logged in the administrative daily log under the log directory:

UNIX systems: /usr/openv/netbackup/logs/admin
Windows systems: install_path\NetBackup\logs\admin

It has the following form:

bpimmedia: EXIT status = exit status

If an error occurred, a diagnostic precedes this message.

FILES

UNIX systems:
/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/db/images

Windows systems:

install_path\NetBackup\logs\admin/*
install_path\NetBackup\db\images

SEE ALSO

See bpbackupdb on page 66.
See bpduplicate on page 121.
See bpinport on page 192.
bpimport

bpimport – import NetBackup backups that are expired or are from another
NetBackup Server

SYNOPSIS

bpimport -create_db_info -id media_id or path | -stype server_type
[-dp disk_pool_name [-dv disk_volume]] [-server name] [-L output_file
[-en]] [-local] [-nh ndmp_host [-mst media_subtype]]

bpimport -drfile -id media_id or path | -stype server_type [-dp
disk_pool_name [-dv disk_volume]] -drfile_dest dir_name_on_master
[-client name] [-server name] [-L output_file [-en]] [-priority
number]

[-M master_server] [-Bdfile file_name] [-st sched_type] [-sl
sched_label] [-L output_file [-en]] [-policy name] [-s startdate]
[-e enddate] [-pt policy_type] [-hoursago hours] [-cn copy_number]
[-backupid backup_id] [[-id media_id | path | -stype server_type]]
[-dp disk_pool_name [-dv disk_volume]] [-priority number]
[-from_replica]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The bpimport command allows backups to be imported. This command is useful
for importing expired backups or the backups from another NetBackup server.

The import operation consists of the following two phases:

- Phase 1 is performed with the first form of the command that appears in the
  Synopsis (-create_db_info option). This step recreates catalog entries for the
  backups that are on the specified media.
- Phase 2 is performed with the second form of the command that appears in the
  Synopsis. This step imports the backups from the media.
The expiration date for imported backups is the current date plus the retention period. For example, if a backup is imported on 14 November 2012 and its retention level is one week, its new expiration date is 21 November 2012.

If imported data is WORM-locked, any changes to WORM retention lock times relative to the new expiration date are re-evaluated during an image cleanup job. The image cleanup job occurs every 12 hours by default. Run `bpimage -allclients -cleanup` to immediately start an image cleanup job.

You can import a backup only if all copies of it are expired.

For more about how to import backups, see the *NetBackup Administrator's Guide, Volume I*.

**OPTIONS**

- `-backupid backup_id`
  
  Specifies the backup ID of a single backup to import.

- `-Bidfile file_name`
  
  `file_name` specifies a file that contains a list of backup IDs to import. List one backup ID per line in the file. If this option is included, other selection criteria are ignored.

  In addition, NetBackup removes the file that is specified with the `-Bidfile` parameter during the activation of that command line interface (CLI). It is removed because the NetBackup GUIs commonly use this parameter. The GUIs expect the command-line interface to remove the temporary file that was used for the `-Bidfile` option upon completion. Direct command-line interface users can also use the option, however it removes the file.

- `-client name`
  
  The host name of the client for which the backups were performed. The default is all clients.

- `-cn copy_number`
  
  Specifies the source copy number of the backups to import. Valid values are 1 through 10. The default is all copies.

- `-create_db_info`
  
  This option recreates catalog entries for the backups that are on the specified media. It skips the backups that are already in the catalog. This option only creates information about the backups that are candidates for import, and does not perform the import operation. The `bpimport` command must be run with this option before you import any backups.
-dp disk_pool_name [-dv disk_volume]
   Imports images on the specified disk pool only. Optionally, the import can be
   restricted to the images that reside on the specified disk volume only. The
   disk_volume argument is the path for BasicDisk.
   
   Option -stype is required with this option.

-e enddate, -s startdate
   Specifies the start date and end date range for all backups to import.
   
   -s specifies a start date and time for the listing. The output list shows only
   images in backups or the archives that occurred at or after the specified date
   and time.
   
   -e specifies an end date and time for the listing. The output list shows only
   files from backups or the archives that occurred at or before the specified date
   and time. Use the same format as for the start date. The default is the current
   date and time.
   
   The valid range of dates is from 01/01/1970 00:00:00 to 01/19/2038 03:14:07.
   The default is the previous midnight.
   
   The required date and time values format in NetBackup commands varies
   according to your locale. The /usr/openv/msg/.conf file (UNIX) and the
   install_path\VERITAS\msg\LC.CONF file (Windows) contain information such
   as the date-time formats for each supported locale. The files contain specific
   instructions on how to add or modify the list of supported locales and formats.
   
   For more about the locale of your system, see "About specifying the locale of
   the NetBackup installation" in the NetBackup Administrator's Guide, Volume
   II.
   
   The following is part of the -help USAGE statement for -bpimport that shows
   the -s and -e options:
   -s mm/dd/yy [hh:[mm]:[ss]]] -e mm/dd/yy [hh:[mm]:[ss]]]

-from replica
   Scans for images only that are capable of automatic import and places them
   in the Storage Lifecycle Policy automatic import worklist. This option is part of
   Phase 1 of the import.

-hoursago hours
   Specifies the number of hours to search before the current time for backups.
   Do not use with the -s option. The default is the previous midnight.

-id media_id | path
   Disk media: Specifies the path to the storage directory that contains the backup
   to be imported.
Tape media: For step 1 (`-create_db_info`), this option specifies the media ID that has the backups you plan to import. This option is required with `-create_db_info`.

For step 2, this option designates a specific media ID from which to import backups. The default is all media IDs that were processed in step 1 of the import operation.

A backup ID that begins on a media ID that step 1 does not process, does not import (the backup is incomplete).

```
-L output_file [-en]
```

Specifies the name of a file in which to write progress information. The default is not to use a progress file.

Example for UNIX systems, `/usr/openv/netbackup/logs/user_ops`

Example for Windows systems, `c:\Program Files\Veritas\NetBackup\logs\user_ops`

Include the `-en` option to generate a log that is in English. The name of the log contains the string `_en`. This option is useful to support the personnel that assist in a distributed environment where different locales may create logs of various languages.

Only default paths are allowed for this option and it is recommended to use the default paths. If you cannot use the NetBackup default path in your setup, you should add custom paths to the NetBackup configuration.

For more information on how to add a custom path, see the “BPCD_WHITELIST_PATH option for NetBackup servers and clients” topic in the NetBackup Administrator’s Guide, Volume I.

```
-l
```

Produces the output in the progress log that lists each imported file.

```
-local
```

When a host other than master server initiates `bpimport` and `-local` is not used (default), the following occurs: `bpimport` starts a remote copy of the command on the master server. The remote copy allows the command to be terminated from the Activity Monitor.

Use `-local` to prevent the creation of a remote copy on the master server. You also can use it to run the `bpimport` only from the host where it was initiated. If the `-local` option is used, `bpimport` cannot be canceled from the Activity Monitor.
-M master_server

**Note:** This option is not required for NetBackup server because it has only one server, the master. If you do use this option in this case, specify the NetBackup master where you run the command.

Specifies the master server that manages the media catalog that has the media ID. If this option is not specified, the default is one of the following:

If the command is run on a master server, then that server is the default.

If the command is run on a media server that is not the master, then the master for that media server is the default.

-p

Previews backups to import according to the option settings, but does not perform the import. Displays the media IDs, server name, and information about the backups to import.

-pb

Previews the backups to import but does not perform the import. Similar to the -p option, but does not display the backups.

-PD

Same as the -PM option, except the backups sort by date and time (newest to oldest).

-PM

Displays the information on the backups to be imported according to the option settings, but does not perform the import. It displays the date and time of the backup, and the policy, schedule, backup ID, host, and media ID.

-policy name

Searches for backups to import in the specified policy. The default is all policies.

-priority number

Specifies a new priority for the import job that overrides the default job priority.

-pt policy_type

Searches for the backups that the specified policy type created. The default is any policy type.

The *policy_type* is one of the following character strings:

Auspex-FastBackup
DataStore
DataTools-SQL-BackTrack
Specifies the name of the media server. The volume database for this server must have a record of the media ID that contains the backups to import. The default is the media server where the command is run.

**Note:** The NetBackup server has only one server (the master). When you use NetBackup server, specify the name of that server.

- **sl** *sched_label*
  Search for backups to import that the specified schedule created. The default is all schedules.

- **st** *sched_type*
  Search for backups to import that the specified schedule type created. The default is any schedule type.

Valid values are as follows:

- **FULL** (full backup)
- **INCR** (differential-incremental backup)
- **CINC** (cumulative-incremental backup)
- **UBAK** (user backup)
UARC (user archive)

NOT_ARCHIVE (all backups except user archive)

-stype server_type

Specifies a string that identifies the storage server type. The server_type value can originate from one of the following sources:

- Veritas provided storage. Possible values are AdvancedDisk and PureDisk.
- Third-party disk appliances. The vendor supplies the server_type string.
- Cloud storage. Use the csconfig cldprovider -1 command to determine the possible stype values. The cloud stype values reflect the cloud storage provider. Cloud storage stype values can also incorporate a suffix (for example, amazon_crypt). Possible suffixes are:
  - _raw: The NetBackup backup image is sent to the cloud in raw format. Use this option if you do not want to compress or encrypt data before sending to cloud storage.
  - _rawc: Compresses the data before it is written to the cloud storage.
  - _crypt: Encrypt the data using AES-256 encryption before writing the data to cloud storage. You must have KMS configured in NetBackup to use this option.
  - _cryptc: Compress and encrypt the data before writing to cloud storage.

The storage server type is case sensitive.

-v

Displays more information in the debug logs and progress logs.

EXAMPLES

Example 1 - Create all on one line catalog information for backups on media ID A0000. The media host hostname is cat. The progress file is bpimport.ls, which is located in the tmp directory.

UNIX systems: # bpimport -create_db_info -id A0000 -server cat -L /usr/openv/netbackup/logs/user_ops/bpimport.ls

Windows systems: # bpimport -create_db_info -id A0000 -server cat -L c:\Program Files\Veritas\NetBackup\logs\user_ops\bpimport.ls

Example 2 - Display all on one line information about the backups that are candidates for import. The backups that appear were created between 11/01/2012 and 11/10/2012. The bpimport command with the -create_db_info option must be run before this command.
Example 3 - Import the backups that were specified in the images file. The progress is entered in the bpimport.ls file.

**UNIX systems:**
```
# bpimport -PM -s 11/01/2012 -e 11/10/2012
```
```
# bpimport -Bidfile /tmp/import/image -L
/usr/openv/netbackup/logs/user_ops/bpimport.ls
```

**Windows systems:**
```
# bpimport -Bidfile \tmp\import\image -L c:\Program Files\Veritas\NetBackup\logs\user_ops\bpimport.ls
```

**FILES**

**UNIX systems:**
```
/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/db/images/*
```

**Windows systems:**
```
install_path\NetBackup\logs\admin/*
install_path\NetBackup\db\images/*
```
bpinst

bpinst – configure legacy NetBackup Encryption

SYNOPSIS

```
bpinst -LEGACY_CRYPT [-crypt_option option] [-crypt_strength strength]
   [-passphrase_prompt | -passphrase_stdin] [-verbose] [ [-policy_encrypt
   0 | 1] -policy_names] name1 [name2 ... nameN]
```

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\n
DESCRIPTION

NetBackup Encryption provides file-level encryption of backups and archives.

-LEGACY_CRYPT is the Legacy Encryption method. It provides the user with the
  encryption strength choices previously available (40-bit DES and 56-bit DES).

The bpinst command that is used with the -LEGACY_CRYPT option configures the
legacy NetBackup Encryption product on the NetBackup clients that can support
encryption. You can also configure encryption for a client that is installed on the
master server host.

Activate bpinst -LEGACY_CRYPT on the master server to configure NetBackup
Encryption on the clients. A single activation makes the necessary configuration
changes on both the clients and the master server.

**Note:** Ensure that the DISALLOW_SERVER_FILE_WRITES NetBackup configuration
option is not set on the client. If this option is set, the server cannot configure the
software on the client.

OPTIONS

-LEGACY_CRYPT

Required if you use 40-bit DES or 56-bit DES encryption. To configure DES
encryption, specify this option first to use the bpinst command. The order is
important; do not omit this option.
-crypt_option option

Configures the CRYPT_OPTION configuration entry on the NetBackup clients. If you do not specify -crypt_option, the client allows either encrypted or unencrypted backups (see ALLOWED).

The possible values for option are:

DENIED | denied | -1

Specifies that the client does not permit encrypted backups. If the server requests an encrypted backup, it is considered an error. This option is the default for a client that has not been configured for encryption.

ALLOWED | allowed | 0

Specifies that the client allows either encrypted or unencrypted backups. ALLOWED is the default condition.

REQUIRED | required | 1

Specifies that the client requires encrypted backups. If the server requests an unencrypted backup, it is considered an error.

-crypt_strength strength

Configures the CRYPT_STRENGTH configuration entry on the NetBackup clients. If you do not specify this option, the CRYPT_STRENGTH configuration entries on the clients remain unchanged.

The possible values for strength are:

DES_40 | des_40 | 40

Specifies the 40-bit DES encryption. This value is the default value for a client that has not been configured for encryption.

DES_56 | des_56 | 56

Specifies the 56-bit DES encryption.

-passphrase_prompt | -passphrase_stdin

Note: Do not forget the pass phrase. If the key file is damaged or lost, you may need the pass phrase to regenerate the key file. Without the proper key file, you cannot restore encrypted backups.

NetBackup uses a pass phrase to create the data that it places in a key file on each client. NetBackup then uses the data in the key file to create the encryption
keys that are required to encrypt and decrypt the backup data. This option applies to the -LEGACY_CRYPT option only.

The -passphrase_prompt option prompts you to enter a pass phrase. The actual pass phrase is hidden while you type.

The -passphrase_stdin option reads the pass phrase through standard input. You must enter the pass phrase twice. This option is less secure than the -passphrase_prompt option because the pass phrase is not hidden. However, it may be more convenient if you use bpinst -LEGACY_CRYPT in a shell script.

NetBackup uses the pass phrase for all the clients that you specify on the bpinst -LEGACY_CRYPT command. If you want separate pass phrases for each client, enter a separate bpinst -LEGACY_CRYPT command for each client.

When you specify a pass phrase, bpinst -LEGACY_CRYPT creates or updates the key files on the clients. The encryption keys (generated from the pass phrase) are used for subsequent backups. Old encryption keys are retained in the key file to allow restores of previous backups.

If you do not specify either the -passphrase_prompt or -passphrase_stdin option, the key files on the clients remain unchanged.

-verbose
Prints the current encryption configuration of each client and what gets installed and reconfigured on each client.

-policy_encrypt 0 | 1
Sets the Encryption policy attribute for the NetBackup policies. You can include -policy_encrypt only with the -policy_names option. The possible values are:

0 - clears the Encryption attribute (or leaves it clear) so the server does not request encryption for clients in this policy. This setting is the default for the policies that are not configured for encryption.

1 - sets the Encryption attribute so the server requests encryption for clients in this policy.

If you do not specify this option, the Encryption attributes for the policies remain unchanged.

-policy_names
Specifies that the names you specify (with the names option) are NetBackup policy names.

If you include the -policy_names option, bpinst -LEGACY_CRYPT configures all the clients in each specified policy. If you omit the -policy_names option, the names are assumed to be NetBackup client names.
name1 [name2 ... nameN]

Specifies one or more NetBackup client or policy names, depending on whether you have included the \-policy_names option. If you omit the \-policy_names option, the names are assumed to be NetBackup client names.

NOTES

The following notes apply to the \-LEGACY_CRYPT option:

- If you are running NetBackup in a clustered environment, you can push configuration data to the client only from the active node.
- If you push the configuration to clients that are located in a cluster, do the following: Specify the hostnames of the individual nodes (not virtual names) in the clients list.
- When you finish the restore of encrypted files from a client, rename or delete the key file created. Move or rename your own key file to its original location or name. If you do not re-establish your key file to its original location or name, you may not be able to restore your own encrypted backups.
- Existing 40-bit encryption license keys or 56-bit encryption license keys are valid for upgrades.
- A privately defined NetBackup 40-bit DES key encrypts the pass phrase that \bpinst \-LEGACY_CRYPT sends over the network.
- The key file on each NetBackup client is encrypted with a privately defined NetBackup DES key. The key can be 40 bits or 56 bits depending on how the client is configured. Restrict access to the key file to the administrator of the client computer. On a UNIX client, the owner of the key file should be root and the mode bits should be 600. The key file should not be exportable through NFS.
- The key file must be the same on all nodes in a cluster.
- Remember pass phrases. In a disaster recovery situation, you may have to recreate a key file on a client by using \bpinst \-LEGACY_CRYPT. For example, suppose a NetBackup client that is named orca performs encrypted backups and an accident occurs that causes orca to lose its files. In this case you must reinstall and configure encryption on the client to restore your backups.

For more about how to restore the operating system and NetBackup, see the NetBackup Troubleshooting Guide.
To provide disaster recovery when you use encryption (client named orbit)

1. Reinstall the operating system on orbit.
2. Reinstall and configure the NetBackup client software on orbit.
3. Reinstall and configure encryption on orbit by using the following command:
   
   ```
   # bpinst -LEGACY_CRYPT -crypt_option allowed
   ```

4. Activate `bpinst -LEGACY_CRYPT` to create a pass phrase by using the following command:
   
   ```
   # bpinst -LEGACY_CRYPT -passphrase_prompt orbit
   Enter new NetBackup pass phrase: *********************
   Re-enter new NetBackup pass phrase: *********************
   Enter the pass phrase that is used on orca.
   ```

5. Activate `bpinst -LEGACY_CRYPT` for each subsequent pass phrase that is used on orbit by entering the following:
   
   ```
   # bpinst -LEGACY_CRYPT -passphrase_prompt orbit
   Enter new NetBackup pass phrase: *********************
   Re-enter new NetBackup pass phrase: *********************
   ```

6. Restore the backed up files to orbit.

**EXAMPLES**

**Example 1** - Configure all on one line 40-bit DES encryption on UNIX clients in a policy named `policy40`:

```
# bpinst -LEGACY_CRYPT -crypt_option allowed -crypt_strength des_40 -policy_encrypt 1 -policy_names policy40
```

Use the `-policy_encrypt` option to set the Encryption attribute for the policy. You can also use the NetBackup administrator utility to set the Encryption attribute.

**Example 2** - Use the `-passphrase_prompt` option to create a passphrase on all clients in a policy named `policy40`:

```
# bpinst -LEGACY_CRYPT -passphrase_prompt -policy_names policy40
Enter new NetBackup pass phrase: *********************
Re-enter new NetBackup pass phrase: *********************
```

**Example 3** - Specify all on one line the NetBackup client named strong must use 56-bit DES encryption:
# bpinst -LEGACY_CRYPT -crypt_option required -crypt_strength des_56 strong

**Example 4 - Display a verbose listing of the configuration for the client named strong:**

```shell
# bpinst -LEGACY_CRYPT -verbose strong
```

BPCD protocol version 8.0.0 on client strong
40-bit library version is 3.1.0.40 on client strong
56-bit library version is 3.1.0.56 on client strong
BPCD platform is redhat for client strong
Current configuration entries are:
- CRYPT_KEYFILE = /usr/openv/netbackup/keyfile
- CRYPT_LIBPATH = /usr/openv/lib
- CRYPT_OPTION = required
- CRYPT_STRENGTH = des-56
- V_PATH_SHARE = /usr/openv/share

No update of NetBackup configuration required for client strong
No update of NetBackup pass phrase required for client strong

## FILES

The following are the files that are used on UNIX systems:

- **UNIX server command**
  
  `/usr/openv/netbackup/bin/bpinst`

- **UNIX client encryption libraries for 40-bit DES and 56-bit DES**
  
  `/usr/openv/lib/libvdes*.`

- **UNIX client encryption key file for 40-bit DES and 56-bit DES**
  
  `/usr/openv/netbackup/keyfile`

- **UNIX client encryption key file utility for 40-bit DES and 56-bit DES**
  
  `/usr/openv/netbackup/bin/bpkeyfile`

- **UNIX client encryption key file utility for 128-bit OpenSSL cipher and 256-bit OpenSSL cipher**
  
  `/usr/openv/netbackup/bin/bpkeyutil`
  `/usr/openv/share/ciphers.txt`
The following are the files that are used on Windows systems:

- Windows server command
  
  \texttt{install\_path\NetBackup\bin\bpinst.exe}

- Windows client encryption key file
  
  \texttt{install\_path\NetBackup\var\keyfile.dat}

- Windows client encryption libraries
  
  \texttt{install\_path\bin\libvdes*.dll}

- Windows client encryption key file utility
  
  \texttt{install\_path\bin\bpkeyfile.exe}
  \texttt{install\_path\share\ciphers.txt}
bpkeyfile

bpkeyfile – run the legacy key file utility that is used for NetBackup standard encryption

SYNOPSIS

bpkeyfile [-stdin] [-change_key_file_pass_phrase]
[-change_netbackup_pass_phrase] [-display] key_file_path

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/
On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd

DESCRIPTION

bpkeyfile creates or updates a file that contains the information that is used to generate DES encryption keys. The information is generated based on a NetBackup phrase that you supply. You supply a key-file pass phrase to encrypt the key file. NetBackup client software uses an encryption key that is calculated from the key file information to encrypt files during backups or decrypt files during restores.

If the file exists, you are prompted to enter the current key-file pass phrase.

If you specify -change_key_file_pass_phrase, you are prompted for a new key-file pass phrase. If you enter an empty pass phrase, a standard key-file pass phrase is used.

If you use the standard key-file pass phrase, bpcd runs automatically. If you use your own key-file pass phrase, start bpcd with the -keyfile argument.

For more about how to start bpcd with the -keyfile argument, see the NetBackup Security and Encryption Guide.

OPTIONS

-stdin
   Reads pass phrases from standard input. By default, bpkeyfile reads the pass phrases that you are prompted to input from your terminal window.

-change_key_file_pass_phrase (or -ckfpp)
   Changes the pass phrase that is used to encrypt the key file.
-change_netbackup_pass_phrase (or -cnpp)
   Changes the pass phrase that is used to encrypt NetBackup backups and archives on this client.

-display
   Displays information about the key file.

key_file_path
   The path of the key file that bpkeyfile creates or updates.

NOTES

The pass phrases that NetBackup uses can be from 0 to 63 characters long. To avoid compatibility problems between systems, restrict the characters in a pass phrase to printable ASCII characters: from the Space character (code 32) to the tilde character (code 126).

The bpkeyfile command is used for legacy encryption.

FILES

Client encryption key file:
UNIX systems: /usr/openv/netbackup/keyfile

Windows systems: install_path\NetBackup\bin\keyfile.dat
bpkeyutil

bpkeyutil – run the key file utility that is used for NetBackup standard encryption

SYNOPSIS

bpkeyutil [-stdin | -insert | -delete] [-display] [-clients client_name1[,client_name2,...]] [-M server]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\

DESCRIPTION

The bpkeyutil command updates a key file that contains the keys that are used for encryption and decryption. The keys are generated based on the private NetBackup pass phrases that you supply. The key file is encrypted by using a key. The NetBackup client software uses an encryption key from the key file to encrypt files during a backup or decrypt files during a restore.

OPTIONS

-stdin
   Reads pass phrases from standard input. By default, bpkeyutil reads the pass phrases that you are prompted to input from your terminal window.

-insert
   Inserts a new NetBackup pass phrase to the key file to encrypt NetBackup backups and archives on this client.

-delete
   Deletes an existing pass phrase from the key file.

-display
   Displays information about the key file.

-clients client_name1[,client_name2,...,client_namen]
   Name of the client where the key file resides. The default is the local client. You may specify multiple client names that are separated by commas. You can only use this argument if you are a NetBackup administrator.
-M server

Name of the master server of the client. The default is the master server defined in the local client's configuration. You can only use this argument if you are a NetBackup administrator on the specified master server.

NOTES

Note the following items when you use the `bpkeyutil` command:

- The `bpkeyutil` command is used for standard encryption.
- The key file must be the same on all nodes in a cluster.

FILES

Client encryption key file:

UNIX systems: `/usr/openv/var/keyfile.dat`

Windows systems: `install_path\NetBackup\var\keyfile.dat`
bplabel

bplabel – write NetBackup label on tape media

SYNOPSIS

```
bplabel -m media_id -d density [-o] [-p volume_pool_name] [-n drive_name | -u device_number] [-host media_server] [-erase [-l]] [-priority number]
```

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The bplabel command writes a NetBackup label on the specified media. Labels are required only for the media that were last used for NetBackup catalog backups or by a non-NetBackup application. You can use this command to erase and label the media that is unassigned in a volume database. In addition, you can use this command to assign specific media IDs. The NetBackup Device Manager daemon or service (ltid) must be active for bplabel to succeed. You also must manually assign the drive by using the NetBackup Device Monitor unless you include the -u option on the bplabel command.

**Caution:** Ensure that the media does not contain required backups. After the media is relabeled, any backups that were on it cannot be restored.

Any authorized user can run this command.

For more about NetBackup authorization, see the *NetBackup Security and Encryption Guide*.

The following are some items about how to use this command:

- The -m and -d options are required.

- The -p option is required if the media ID is not in the NetBackup volume pool.

- If the data on the media is in a recognized format and the -o option is not specified, bplabel prompts you to confirm the overwrite. Data format recognition
works only if the first block on a variable length media is less than or equal to 32 kilobytes.

■ Use the bplabel command only for tapes.

You must have administrator privileges to run this command.

OPTIONS

-d density
A required option that specifies the density of the tape drive on which the media is mounted. The tape mount request must be performed on a drive type that satisfies the -d option.

Note: Do not use capital letters when you enter the density. Incorrect density syntax causes the command to fail and an "Invalid Density Drive Type" message to appear.

The valid densities are as follows:

4mm (4-mm Cartridge)
8mm (8-mm Cartridge)
dlt (DLT Cartridge)
hcart (1/2 Inch Cartridge)
qscsi (1/4 Inch Cartridge)

-erase [-l]
This option is used to erase the media. Short erase is the default erase. If -l option is specified, the media is long erased. A long erase operation can take a long time depending on the type of drive.

-host media_server
The media_server variable is the host where the drive is attached. This drive is the drive that is used to mount the media. By default, if this option is not used, the command runs on the local system.

-m media_ID
A required option that specifies the external media ID that is written to the tape label as a media ID. You can enter the media ID in either uppercase or lowercase. Internally, it always converts to uppercase. The media ID must be six or fewer alphanumeric characters.
-n drive_name
Unconditionally assigns the stand-alone drive that drive_name specifies. The drive must contain media and be ready. By using this option, manual operator assignment is not required. The name for the drive can be obtained from the Media Manager configuration.

-o
Unconditionally overwrites the selected media ID. If this option is not specified, bplabel prompts for permission to overwrite the media that meets any of the following conditions:

Contains a NetBackup media header.
Is a NetBackup catalog backup media.
Is in TAR, CPIO, DBR, AOS/VS, or ANSI format.

-p volume_pool_name
This option is required if the media ID is defined in the Enterprise Media Manager Database but is not in the NetBackup volume pool.

volume_pool_name must specify the correct pool.

-priority number
Specifies a new priority (number) for the label job that overrides the default job priority.

-u device_number
Unconditionally assigns the stand-alone drive that device_number specifies. The drive must contain media and be ready. By using this option, manual operator assignment is not required. The number for the drive can be obtained from the Media Manager configuration.

NOTES

tpconfig -d, tpconfig -l, and vmoprcmd may truncate long drive names. Use tpconfig -dl to obtain the full drive name.

EXAMPLES

Example 1 - Label a DLT cartridge media as dlt001
bplabel -m dlt001 -d dlt

Example 2 - Erase the DLT cartridge media with the label dlt102
bplabel -m dlt102 -d dlt -erase
SEE ALSO

See \textit{ltid} on page 549.
**bplist**

*bplist* – list the backed up and archived files on all NetBackup hosts

**SYNOPSIS**

```plaintext
```

On UNIX systems, the directory path to this command is:
/usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is:
`install_path\NetBackup\bin\`

**DESCRIPTION**

The *bplist* command shows a list of previously archived or backed up files according to the options that you specify. You can choose the file or directory and the time period that you want the listing to cover. Directories can be recursively displayed to a specified depth. *bplist* shows only the files that you have read access to. It lists the files only if an administrator account performs the user backup.

You also must own or have read access to all directories in the file paths. You can list the files that were backed up or archived by another client only if the NetBackup administrator has validated you to do so.

If you create the following directory with public-write access, *bplist* creates a debug log file in this directory that you can use for troubleshooting:

**UNIX systems:** `usr/openv/netbackup/logs/bplist/`

**Windows systems:** `install_path\NetBackup\logs\bplist\`

**OPTIONS**

- `-A` | `-B`
  
  Specifies whether to produce the listing from archives (`-A`) or backups (`-B`). The default is `-B`. 
-b | -c | -u

Specifies an alternate date-time to be used for printing with the -l option:

- b displays the backup date and time of each file.
- c displays the last inode modification date and time (UNIX systems) or creation date and time (Windows systems) for each file.
- u displays the last access date and time of each file.

The default is to display the time of the last modification of each file.

-C client

Specifies a client name to use for finding backups or archives to list. This name must be as it appears in the NetBackup configuration. The default is the current client name.

-F

Specifies that in the list output, symbolic links (which apply only to UNIX clients) end with a trailing @ and executable files with a trailing *.

cfilename

Names the file or directory to list. Any files or directories that you specify must be listed at the end, following all other options. If you do not specify a path, the default is the current working directory.

For Windows systems, use uppercase for the drive letter. For example:

C:\NetBackup\log1

For directories, if you do not use the -R option, include the trailing path separator as in the following:

UNIX systems: bplist -l "*/home/user1/*"

Windows systems: bplist -l "D:\WS_FTP.LOG\"

If you use the asterisk meta-character (*), use quotation marks around the file name for the command to work properly.

-flops options

Lists NetBackup files.

-I

Specifies a search that is case insensitive. The capitalization is not considered when it compares names (for example, Cat matches cat).

-k policy

Names the policy to search to produce the list. If not specified, all policies are searched.
-keyword  keyword_phrase

Specifies a keyword phrase for NetBackup to use when it searches for backups or archives from which to restore files. The phrase must match the one that was previously associated with the backup or archive by the -k option of bpbackup or bparestore.

You can use this option in place of or in combination with the other restore options to make it easier to restore backups and archives. Use the following meta-characters to help match keywords or parts of keywords in the phrase:

* matches any string of characters.

? matches any single character.

[] matches one of the sequence of characters that is specified within the brackets.

[- ] matches one of the range of characters, that is separated by the "-".

The keyword phrase can be up to 128 characters in length. All printable characters are permitted including space (" ") and period (".").

The phrase must be enclosed in double quotes ("...") or single quotes (‘...’).

The default keyword phrase is the null (empty) string.

---

**Note:** The keyword phrase is ignored when you use the following policy types: DB2, Informix-On-BAR, Oracle, SAP, MS-SQL-Server, Sybase.

---

-l

On Windows systems, -l shows the file details.

On UNIX systems, -l lists the following file details in a long format: Mode, owner, group, size in bytes, and time of last modification for each file (see the EXAMPLES section). The list shows the mode of each file as ten characters that represent the standard UNIX file permissions. The first character is one of the following:

- d (specifies a directory)

- l (specifies a link)

- m (specifies a file that migrated by Veritas Storage Migrator for UNIX or Veritas Data Lifecycle Manager)

- (specifies a file)

The next nine characters show the three sets of permissions. The first set shows the owner’s permissions, the next set shows the user-group permissions,
and the last set shows permissions for all other users. Each set of three specifies the read, write, and execute permissions as follows:

- r = the file is readable
- w = the file is writable
- x = the file is executable
- = the indicated permission is not granted

-listpolicy
Includes the schedule type and policy name in the command output.

-listseconds
Specifies that seconds granularity be used for the timestamp when the -1 option is used.

-nboptimized
Specifies the command filter the output to show only Windows images that were backed up with the optimized flag for Windows deduplication.

-nbnormal
Specifies the command filter the output to show only Windows images that were not backed up with the optimized flag for Windows deduplication.

-nt_files
Lists the files and directories in Windows format. This option applies only to Windows. For example: C:\users\test

-pi
Specifies a path-independent search, which means that NetBackup searches for a specified file or directory without regard to the path. For example, a file with the name test exists in the three following directories. A search for test finds all three instances of the file:

UNIX systems:

/tmp/junk/test
/abc/123/xxx/test
/abc/123/xxx/yyy/zzz/test

Windows systems:

\tmp\junk\test
\abc\123\xxx\test
\abc\123\xxx\yyy\zzz\test
On Windows systems, `-r` lists the disk images that were backed up. The default is to list file systems.

On UNIX systems, `-r` lists the raw partitions that were backed up. The default is to list file systems.

```
-R [n]
```
Recursively lists the subdirectories that are encountered to a depth of `n`. The default for `n` is 999.

```
-s date, -e date
```
Specifies the start date (`-s`) and end date (`-e`) for the listing.

`-s` specifies a start date and time for the listing. The resulting list shows only files in backups or the archives that occurred at or after the specified date and time.

The required date and time values format in NetBackup commands varies according to your locale. The `/usr/openv/msg/.conf` file (UNIX) and the `install_path\VERITAS\msg\LC.CONF` file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

For more about the locale of your system, see "About specifying the locale of the NetBackup installation" in the *NetBackup Administrator's Guide, Volume II*.

The valid range of dates is from 01/01/1970 00:00:00 to 01/19/2038 03:14:07. The default is the current date minus six months.

`-e` specifies an end date and time for the listing. The resulting list shows only files from the backups or the archives that occurred at or before the specified date and time. Use the same format for start date and time. The default is the current date and time.

```
-S master_server
```
UNIX systems: `-s` specifies the name of the NetBackup server. The default is the first `SERVER` entry that is found in the `/usr/openv/netbackup/bp.conf` file.

Windows systems: `-s` specifies the name of the NetBackup server. The default is the server designated as current on the Servers tab of the Specify NetBackup Machines dialog box. To display this dialog box, start the Backup, Archive, and Restore user interface on the client. Then click Specify NetBackup Machines on the File menu.
-t policy_type
    Specifies one of the following numbers that correspond to the policy type. The default is 0 for all clients except Windows, where the default is 13.

0 = Standard
4 = Oracle
6 = Informix-On-BAR
7 = Sybase
8 = MS-SharePoint
11 = DataTools-SQL-BackTrack
13 = MS-Windows
15 = MS-SQL-Server
16 = MS-Exchange-Server
17 = SAP
18 = DB2
19 = NDMP
20 = FlashBackup
21 = Split-Mirror
25 = Lotus Notes
29 = FlashBackup-Windows
35 = NBU-Catalog
39 = Enterprise-Vault
40 = VMware
41 = Hyper-V
44 = BigData

-T
Lists the directories in true-image backups. The default is to list non-true-image backups.

**Note:** TIR information does not appear for synthetic full backups, even though TIR information is used for synthetic full backups.
-Translateownership

On Linux systems for Linux VMware backups only: Translates the user ID (UID) and the group ID (GID) of the individual who owns the files to the user name and group name. By default for Linux VMware backups, bplist shows the UID and the GID.

The client on which you run the bplist command and -Translateownership option must be the same as the client that you specify with the -C option.

On operating systems other than Linux, this option has no effect.

-unix_files

Lists the files and directories in UNIX format. This option applies only to UNIX. For example: /C/users/test

EXAMPLES

Example 1 - List recursively in long format, the files that were backed up in /home/usr1 (UNIX) or D:\WS_RTP.LOG (Windows).

On UNIX systems:

```
# bplist -l -R /home/usr1
lrwxrwxrwx usr1;usr@ eng;None 0 Apr 28 12:25 /home/usr1/dirlink
drwxr-xr-x usr1;usr@ eng;None 0 Apr 04 07:48 /home/usr1/testdir
drwxr-x--- usr1;usr@ eng;None 0 Apr 04 07:49 /home/usr1/dir
-rwxr----- usr1;usr@ eng;None 1002 Apr 02 09:59 /home/usr1/dir/file
lrwxrwxrwx usr1;usr@ eng;None 0 Apr 04 07:49 /home/usr1/dir/link
```

On Windows systems:

```
# bplist -l -R D:\WS_FTP.LOG
-rwx------ bjm;usr@ bjm;None 64 Oct 10 2012 D:\WS_FTP.LOG
-rwx------ bjm;usr@ bjm;None 64 Oct 10 2012 D:\WS_FTP.LOG
-rwx------ bjm;usr@ bjm;None 64 Oct 10 2012 D:\WS_FTP.LOG
```

Example 2 - List the files that were backed up and associated with all or part of the keyword phrase "MyHomeDirectory".

UNIX: # bplist -keyword "*MyHomeDirectory*" -l /home/kwc/

Windows: # bplist -keyword "*MyHomeDirectory*" -l C:\home\kwc\n
Example 3 - List the files that were archived and associated with all or part of the keyword phrase "MyHomeDirectory"

UNIX: # bplist -A -keyword "*MyHomeDirectory*" -l /home/kwc/
Example 4 - Lists recursively and with details the output from `bplist` on a Windows master server from a Windows client. Enter the following command to list the files that were backed up on drive D of Windows client slater and associated with all or part of the keyword phrase "Win NT":

```
# bplist -keyword "*Win NT*" -C slater -R -l C:\client_data_2
```

The user column (`root;usr@`) for the Windows images displays the user that backed up the file and the owner@domain separated by a semicolon. The group column (`root;None`) for the Windows images is the group that backed up the file and the group@domain separated by a semicolon.

Example 5 - List the files from a Linux VMware backup and translate the UID and GID to the user name and the group name:

```
# bplist -Translateownership -S host0.example.com -C client0.example.com -R 1 -1 -t 40 -E -unix_files -b /user1_home
```

The user and group columns for the Linux images display the user name and the group name.

```
drwxr-xr-x user1 grp 0 Sep 09 10:39 /user1_home/
drwxr-xr-x user1 grp 0 Sep 09 10:39 /user1_home/user_data/
drwxr-xr-x root root 0 Sep 09 10:39 /user1_home/root_data/
drwxr-xrwx root root 0 Sep 09 10:39 /user1_home/root_data_write/
drwxr-xr-x root root 0 Sep 09 10:39 /user1_home/root_data.orig/
drwxr-xr-x user1 grp 0 Sep 09 10:39 /user1_home/444.txt/
```

**FILES**

**UNIX systems:** `/usr/openv/netbackup/logs/bplist/log.mmddyy`

**Windows systems:** `install_path\NetBackup\logs\bplist\*.log`

**SEE ALSO**

See `bp` on page 49.
See `bparchive` on page 51.
See `bpbackup` on page 57.
See `bprestore` on page 382.
bpmedia

bpmedia – freeze, unfreeze, suspend, or unsuspend NetBackup media

SYNOPSIS

bpmedia -freeze | -unfreeze | -suspend | -unsuspend -m media_id [-h host] [-v]

bpmedia -movedb -m media_id -newserver newservername [-newsvr_group groupname] [-oldserver oldservername] [-v]

bpmedia -movedb -allvolumes -newserver newservername -oldserver oldservername [-v]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The bpmedia command enables you to do the following:

- Freeze, unfreeze, suspend, or unsuspend NetBackup tape media. That is, it allows or disallows future backups or archives to be directed to the media. This command applies only to media that Media Manager manages.

- Move a media catalog entry from one server to another in a master and a media server cluster.

- Move ownership of tape media to a different media server. It changes all media database and image records that reference one server name (oldservername) to reference another server name (newservername).

Note: Under certain media or hardware error conditions, NetBackup automatically suspends or freezes media. If this action occurs, the reason is logged in the NetBackup Problems report. If necessary, you can use the bpmedia -unfreeze or -unsuspend options to reverse this action.

Any authorized user can run this command. For more about NetBackup authorization, see the NetBackup Security and Encryption Guide.
OPTIONS

-freeze
Freezes the specified media ID. When an active NetBackup media ID is frozen, NetBackup does not direct backups and archives to the media. All unexpired images on the media continue to be available for restores. NetBackup never deletes a frozen media ID from the NetBackup media catalog, nor is it unassigned in the NetBackup volume pool when it expires.

-unfreeze
Unfreezes the specified media ID. This option reverses the action of freeze and allows the media to be used for backups or archives again if it has not expired. If a media is expired when it is unfrozen, it is immediately unassigned in the NetBackup volume pool.

-suspend
Suspend the specified media ID. The action is the same as freeze except when the media ID expires, it is immediately unassigned in the NetBackup volume pool.

-unsuspend
Unsuspends the specified media ID. This option reverses the action of suspend and allows the media to be used for backups or archives again.

-movedb -newserver newservername [-newsrv_group groupname] [-oldserver oldservername]

Note: You cannot use the -movedb option with NetBackup server.

Moves a media catalog entry from one server to another in a master and a media server cluster. This command moves the media catalog entry for the specified media ID from oldservername to newservername. It updates the NetBackup image catalog to reflect that the media ID was moved. You can assume that after the move, newservername has access to the media.

-newserver newservername specifies the name of the host to which the entry is moved.

-newsrv_group groupname specifies the name of the new server group that is to own the media.

-oldserver oldservername specifies the name of the host where the catalog entry to be moved currently resides. If you do not specify oldservername, the system where the command runs is considered to be the old server.
The `movedb` option is most meaningful in the following configurations: A master and its media servers share a robotic library and have access to all the media in the robot. At a minimum, all NetBackup servers must use the same Enterprise Media Manager Database. With the same database, the media can move from one robotic library to another without losing their attributes and assignment status.

```
movedb -allvolumes -newserver newservername -oldserver oldservername
```

Moves all media that are assigned to one media server (oldservername) to another media server (newservername). This operation occurs on the EMM database, changing the `lastwritehost` of the media to `newservername`. The following is true for the media that belongs to a share group: If the `lastwritehost` was set to the oldservername, then the newservername must belong to the share group, and `lastwritehost` is changed to `newservername`.

If the first step succeeds, then the option changes the media server name for all fragments in the image database from oldservername to newservername. This action may take a long time, because the command must traverse the entire image database.

**Note:** You cannot use the `movedb` option with the NetBackup server.

```
m media_id
```

Specifies the media ID that requires action. The media ID must be six or fewer characters and must be in the NetBackup media catalog.

```
h host
```

Specifies the host name of the server where the media catalog resides. This option is required only if the volume was not written on the server where you run the `bpmedia` command. In this case, the media ID is in the NetBackup media catalog on the other server. You must specify the name of that server on the `bpmedia` command.

For example, assume that you have a master server named whale and a media server named eel. You run the following `bpmedia` command on whale to suspend media ID BU0001 that is in the media catalog on eel:

```
bpmedia -suspend -m BU0001 -h eel
```

Use the NetBackup Media List report to determine the host that has the volume in its media catalog.

```
v
```

Selects verbose mode. This option is only meaningful when NetBackup runs with debug log function on (that is, when the following directory exists):
UNIX systems:

/usr/openv/netbackup/logs/admin

Windows systems:

install_path\NetBackup\logs\admin

EXAMPLE

Assume that the master server is HOSTM, with HOSTS1 and HOSTS2 being media servers. It moves the media catalog entry for media ID DLT001 from HOSTS1 to HOSTS2 and updates the NetBackup image catalog. The following command is run on master server HOSTM:

```
# bpmedia -movedb -m DLT001 -newserver HOSTS2 -oldserver HOSTS1
```

FILES

UNIX systems:

/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/db/media/*

Windows systems:

install_path\NetBackup\logs\admin\*.log
install_path\NetBackup\db\media\*.log
bpmedialist

bpmedialist – display NetBackup tape media status

SYNOPSIS


bpmedialist -summary [-U | -L] [-brief] [-p pool_name] [-h host_name | -M master_server,...] [-owner host_name | group_name] [-v]

bpmedialist -mcontents -m media_id [-U | -l | -L] [-d density] [-h host_name | -M master_server,...] [-owner host_name | group_name] [-v] [-priority number]


On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

bpmedialist queries one or more NetBackup media catalogs and produces a report on the status of the NetBackup media. Authorized users can run this command.

For more about NetBackup authorization, see the NetBackup Security and Encryption Guide.

bpmedialist produces one of three reports: Media List Report, Media Summary Report, and Media Contents Report.

Media List Report

Media List (-mlist) report, provides information on either a single volume or all volumes in the NetBackup media catalog. This report does not apply to disk storage units. The report lists, for each volume in the report, the volume’s media ID, media server, and other attributes, which is the default report type.
If the `-U` option is used (default), the status field appears as English text. With the `−L` option, the status appears as a hexadecimal integer. The interpretation of the digits is given here. Any or all of these flags can be set. Settings other than those listed here correspond to unreported states.

`>= 0x2000` Media contains some encrypted images.

`>= 0x800` This tape is WORM (write once, read many).

`>= 0x400` Used for alternate server restores.

`>= 0x200` Multiplexing is TRUE.

`>= 0x080` Imported is TRUE.

`>= 0x040` Multiple retention levels is TRUE.

To determine the interpretation for the low-order status digit, compare the digit to the following values in order.

`>= 0x008` The status is Full.

`>= 0x004` This is an unreported state.

`>= 0x002` The status is Suspended.

`== 0x001` The status is Frozen.

`== 0x000` The status is Active.

The reported status is the status for the low-order digit that is combined with the status for the upper-order digits. For instance, for a status value of `0x040`, the media ID is active, and multiple retention levels are in effect.

The `-l` option produces a report in Short mode. Each media ID occupies one line of the report. The fields on this line are listed later in this description.

Any of the following fields that are not documented in that section are reserved for NetBackup internal use:

- media id
- partner id
- version
- density
- time allocated
- time last written
- time of expiration
- time last read
Media Summary Report

The Media Summary report lists (by server) summary statistics for active and inactive media, which is grouped according to expiration date. The report shows the expiration date for the media and the number of media at each retention level, and the status of each media ID.

Media Contents Report

The Media Contents report lists the contents of media as read directly from the media. It lists the backup IDs that are on a single media ID. It does not list each individual file. This report does not apply to disk storage units. Note that the storage unit may stay in use for some time after the break if the following occurs: You try to abort the command by entering `ctrl-c` and the requested media are not mounted or positioned. Each entry in the report appears as that area of the storage unit is read.

The `-l` format for the Media Contents report produces one line for each backup ID and contains the following fields.

For more detail, see the Media Contents Report section in the *NetBackup Administrator's Guide, Volume II.*
Any of the following fields that are not documented in that section are reserved for NetBackup internal use.

- Version (1 denotes a DB backup image, 2 denotes a regular backup image)
- Backup ID
- Creation time
- Expiration time
- Retention level
- Fragment number
- File number
- Block size (in bytes)
- Status
- media_id
- Size
- Reserved
- data_start
- Reserved
- client_type *
- copy_num *
- sched_type *
- Flags *
- opt_extra
- mpx_headers
- res1
- Policy name *
- Schedule label *

* These fields are significant only if version is 2.

OPTIONS

Report-type Options
bpmedialist produces one of four types of reports. An option on the command line determines the type of report that is produced. The report-type options are as follows:

-mlist

    Produces a Media List report (the default report type).

-summary

    Produces a Media Summary report.

-mcontents

    Produces a Media Contents report.

The bpmedialist report can appear in one of several formats. The report-format options are as follows:

-brief

    Produces a brief report. This option is available for the Media Summary report only. The default is a full report, which includes a breakdown of active and non-active media that report on each media ID status within these categories.

-U

    Reports in user mode (the default report mode). The report includes a banner that lists the column titles. The report style is descriptive, rather than terse.

-L

    Reports in long mode. This format produces the report with the most complete information. For instance, for the Media List report, the report lists each media ID attribute as a series of *keyword* = *value* pairs, one attribute per line. A value can be expressed as both a numeric value and a descriptive value.

-l

    Reports in short mode. This format produces a terse report. This option is useful for scripts or the programs that rework the listing contents into a customized report format.

The following are the remaining options used by bpmedialist:

-d density

    Reports on media of this density type. If the robot type is specified on the command line, the value for density should be consistent with the robot type. Available density types are:

    - 4mm - 4mm Cartridge
    - 8mm - 8mm Cartridge
    - dlt - DLT Cartridge
    - qscsi - 1/4 Inch Cartridge
**Note:** The following densities are supported only on NetBackup Enterprise Servers.

- **dlt2** - DLT Cartridge 2
- **dlt3** - DLT Cartridge 3
- **dtf** - DTF Cartridge
- **hcart** - 1/2 Inch Cartridge
- **hcart2** - 1/2 Inch Cartridge 2
- **hcart3** - 1/2 Inch Cartridge 3

-**h**  *host_name*
  
  The name of a host that contains the media to be reported. Use `-h` instead of `-M` to collect the contents list of expired media.

  To extract records for media from NDMP hosts, use the NDMP hostname, not the NetBackup for NDMP server hostname. The NCMP hostname is defined in the NDMP storage unit or EMM as an NDMP server type (or an associated EMM alias name) that is associated with that master server domain.

-**json**
  
  Prints the output in **JSON** (JavaScript Object Notation) format on a single line.

-**m**  *media_id*
  
  Reports on this media ID only. This option is required for the Media Contents report.

  For the Media List report, this option is optional. The default condition is that all media IDs are included in that report. The media ID can be provided in either uppercase or lowercase. The media ID must be six or fewer characters and must be in the NetBackup media catalog (that is, assigned from the NetBackup volume pool).

-**owner**  *host_name | group_name*
  
  Specifies the owner of the media list. The owner can be a host or a server group.

**Note:** NetBackup server has only one server (the master), so use the name of that server for *host_name*.

*host_name* is either the name of a host, or the character string **ALL**. If *host_name* is the name of a host, the query goes to the media catalog that resides on the system *host_name*. For the `-mcontents` option, this option can
appear once. For the -mlist and -summary options, this option can appear more than once. The default is all servers in the set of storage units for removable media.

The system *host_name* must allow access by the system running *bpmedialist*. *host_name* can be a media server for a master server other than the local master server. The default is the master server of the local cluster.

For a media server or for a master server other than the local master, 
*bpmedialist -h the_media_server* may complete faster than an equivalent *bpmedialist -M the_media_servers_master* command. The difference in response time can be significant if the media server from the -h command is local and the master server from the -M command is remote.

If *host_name* is ALL, the query goes to the local master server and its media servers.

*group_name* specifies the name of a server group or the character string ALL. If *group_name* is the name of a server group, the query returns the media that the server group owns. If *group_name* is ALL, the query returns the media that all the server groups own.

*M master_server,...*

A list of alternative master servers. This list is a comma-delimited list of host names. If this option is present, each master server in the list runs the *bpmedialist* command. If an error occurs for any master server, the report process stops at that point.

The report is the composite of the information that all the master servers in this list return. *bpmedialist* queries each of these master servers. Each master server in the list must allow access by the system that issues the *bpmedialist* command.

For -mcontents (Media Contents report) only, the master server returns media information from the media catalogs. This media information is for both the master and its media servers (except for NetBackup server, which does not support remote media servers). For example, if a media ID exists on a media server of one of the master servers in the -M list, the following occurs: The master retrieves the media information from the media server and returns it to the system running *bpmedialist*. In this case, both the master server and the media server must allow access by the system that issues the *bpmedialist* command.

The default is the master server for the server running *bpmedialist*.
Note: NetBackup server supports only one server, the master; the default in this case is always the NetBackup server master where you run `bpmedialist`.

- `p pool_name`
  Reports on the media IDs that belong to this volume pool. The default is all pools.

- `priority number`
  Specifies a new priority (number) for the media contents job (for a Media Contents report) that overrides the default job priority.

- `rl retention_level`
  Reports on the media that use this retention level. The retention level determines how long to retain backups and archives. The `retention_level` is an integer between 0 and 100 (default level is 1).

Note: If you run this command on a pre-NetBackup 8.0 media server, the output only displays the retention levels between 0 and 24.

Following are the retention levels with the installation values for the corresponding retention periods. Your site may have reconfigured the retention periods that correspond to the retention levels.

- 0 (one week)
- 1 (2 weeks)
- 2 (3 weeks)
- 3 (1 month)
- 4 (2 months)
- 5 (3 months)
- 6 (6 months)
- 7 (9 months)
- 8 (1 year)
- 9-100 (infinite, except 25 which is expire immediately)

- `rn robot_number`
  Reports on the robot by using this robot number. The robot number can be obtained from the Media and Device Management.

For rules about the use of this number, see the *NetBackup Administrator’s Guide, Volume II*. 
-rt robot_type
   Reports on a robot of this type. For non-robotic (stand-alone) devices select NONE. Valid robot types include the following:
   
   TLD - Tape Library DLT
   
   NONE - Not robotic

   Note that the following robot types apply only to NetBackup Enterprise Server:
   
   ACS - Automated Cartridge System

-v
   Selects verbose mode. This option causes bpmedialist to log additional information for debugging purposes. The information goes into the NetBackup administration daily debug log. This option is meaningful only when NetBackup has the debug logging enabled; that is, when the following directory is defined:

   For UNIX systems: /usr/openv/netbackup/logs/admin

   For Windows systems: install_path\NetBackup\logs\admin

EXAMPLES

Example 1 - Produce a media report for all media IDs that are defined for the master server and media servers of the local system.

   Note: For NetBackup server, the report includes only media IDs for the master server because remote media servers are not supported.

   # bpmedialist

   Server Host = hatt

   id   rl  images allocated last updated density kbytes restores
   vimages expiration last read   <-------- STATUS -------->
   ---------------------------------------------------------------------------
   143191 0  28 12/03/2012 23:02 12/22/2012 23:00 dlt 736288 1
   7 12/29/2012 23:00 12/09/2012 10:59
   144280 0  9 11/25/2012 11:06 12/01/2012 23:03 dlt 290304 0
   0 12/08/2012 23:03 N/A EXPIRED FROZEN
   AEK800 0 22 12/06/2012 03:05 12/23/2012 03:01 dlt 23213184 0
   7 12/30/2012 03:01 12/09/2012 10:48
Example 2 - Produce a media contents report for media ID AEK802. The report is partially listed as follows.

```bash
# bpmedialist -mcontents -m AEK802
media id = AEK802, allocated 01/08/2007 03:10, retention level = 0

File number 1
Backup id = hat_0915786605
Creation date = 01/08/2007 03:10
Expiration date = 01/15/2007 03:10
Retention level = 0
Copy number = 1
Fragment number = 2
Block size (in bytes) = 65536

File number 2
Backup id = hat_0915809009
Creation date = 01/08/2007 09:23
Expiration date = 01/15/2007 09:23
Retention level = 0
Copy number = 1
Fragment number = 1
Block size (in bytes) = 65536
```

Example 3 - Produce a Media List report for master servers hatt and duo. bpmedialist runs on the master server buff.

```bash
# bpmedialist -M hatt,duo
```

Server Host = hatt

<table>
<thead>
<tr>
<th>id</th>
<th>rl</th>
<th>images</th>
<th>allocated</th>
<th>last updated</th>
<th>density</th>
<th>kbytes</th>
<th>restores</th>
</tr>
</thead>
</table>
Example 4- Report on which of two hosts has a given media ID configured. The host hatt does not have A00004 configured in its media catalog. Therefore, it reports that the requested media ID was not found in the NetBackup media catalog or Enterprise Media Manager Database.

The host duo does have A00004 configured, so it produces a Media List report for A00004 (the command is all on one line).

# bpmedialist -mlist -h hatt -h duo -m A00004
requested media id was not found in NB media database and/or MM volume database

Server Host = duo

<table>
<thead>
<tr>
<th>id</th>
<th>rl</th>
<th>images</th>
<th>allocated</th>
<th>last updated</th>
<th>density</th>
<th>kbytes</th>
<th>restores</th>
</tr>
</thead>
<tbody>
<tr>
<td>vimages</td>
<td>expiration</td>
<td>last read</td>
<td>&lt;&lt;------- STATUS -------&gt;&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
<td>---------</td>
<td>------------</td>
<td>-------------</td>
<td>---------</td>
<td>--------</td>
<td>----------</td>
</tr>
<tr>
<td>A00004</td>
<td>0</td>
<td>0</td>
<td>11/16/2009 05:31</td>
<td>N/A</td>
<td>4mm</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

FILES

UNIX systems: /usr/openv/netbackup/logs/admin/*

Windows systems: install_path\NetBackup\logs\admin/*
bpminlicense

bpminlicense – manage NetBackup licenses

SYNOPSIS

bpminlicense [-path license_key_file | -M server] [-debug] [-verbose] -find_keys | -delete_keys | -add_keys keystring1...keystringn


bpminlicense -nb_ufid fid [-debug] [-verbose]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The bpminlicense utility manages NetBackup licenses. The preferred method to manage NetBackup licenses is to use the Help > License Keys panel in the NetBackup Administration Console. For UNIX servers, you may use the get_license_key utility to manage the NetBackup licenses. This action is preferred to this command.

Any authorized user can run this command.

For more about NetBackup authorization, see the NetBackup Security and Encryption Guide.

OPTIONS

-add_keys keystring1...keystringn

This option adds license keys to the license key file. It accepts one or more keys as input. By default, the license key file location is install_path\NetBackup\var\license.txt for Windows and /usr/openv/var/license.txt for UNIX and Linux.

-debug

Displays detailed information to standard error.
-delete_keys keystring1...keystringn
   Deletes one or more license keys that are specified with the key value from
   the license key file.

-find_keys keystring1...keystringn
   This option accepts one or more keystrings as input and finds it in license key
   file.

-list_keys
   Lists the licenses in the NetBackup license key file.

-M server
   Use the standard NetBackup license file from the specified NetBackup server.

-nb_features
   Lists only active NetBackup feature IDs. When this option is specified with the
   -verbose option, the command also lists the active licenses.

-nb_ufid fid
   Displays licensing information for a specific feature ID. For capacity-based
   features, the VALUE field is the total licensed capacity of all active license keys
   for the feature.

-path license_key_file
   Uses the specified license_key_file on the local system. The default is the
   standard NetBackup license file. The NetBackup license file is found in
   install_path\NetBackup\var\license.txt for Windows and
   /usr/openv/var/license.txt for UNIX and Linux.

-verbose
   Displays additional information to standard output. This option is ignored when
   used with the -nb_ufid option.

EXAMPLE

Example 1 - Display license information on feature 78, an OpenStorage Disk Option:

# bpminlicense -nb_ufid 78
0x05000000;PRID=6 (NetBackup Enterprise Server);FID=78 (OpenStorage
Disk Option);SERIAL=0;VALUE=10; DEXPIRE=2007/07/31 01:00:00 0 (Not
expired); UXDEXPIRE=1185861600 0 (Not expired);
UKEY=OENP-24NJ-PTJT-PPPP-PC6N-PPPP-PNPP-PPPP-P0C6

Example 2 - The administrator wants to know if an active SAN Client license is
installed:
# ./bpminlicense -verbose
OENC-CPP9-3ZUP-DO83-6PWB-8K4O-SKS7-774C-PPP6
OHNW-PPX2-PCDV-UPGP-PZUZ-NCZP-RXXO-GO49-G777-GOP

  file version = 0x05000000
  time added = 0x46388201 Wed May 02 07:20:17 2007
  hostname = hagar
  product ID = 6 NetBackup Enterprise Server
  serial number = 0
  key version = 0x05000000
  count = 0
  server platform = 0 Any platform
  client platform = 0 Any platform
  server tier = 10 NetBackup Enterprise Server
  client tier = 0 No tier
  license type = 4 Not for resale
  OEM ID = 16 Unknown OEM: 16
  Expiration = Not expired Tue Jul 31 01:00:00 2007
  Time Left = 84 Days
  Firm Expiration = Not expired Tue Jul 31 01:00:00 2007
  Feature ID = 84 SAN Client +
**bpnbat**

*bpnbat* – perform Authentication tasks from within NetBackup

**SYNOPSIS**

```
bpnbat [-AddDomain | -RemoveDomain] Private_Domain
bpnbat [-AddMachine]
bpnbat [-AddUser | -RemoveUser] Name Private_Domain
bpnbat -GetBrokerCert Broker_Name Broker_Port
bpnbat -Login [-Info answer_file] [-cf credential_file] [-LoginType AT|WEB|APIKEY]
bpnbat -LoginMachine
bpnbat -Logout [-LogoutType AT|WEB|APIKEY] [-cf credential_file]
bpnbat -RemoveBrokerCert host_name
bpnbat -RenewCred [-cf credential_file]
bpnbat -ShowBrokerCerts
bpnbat -ShowMachines
bpnbat -Version
bpnbat -WhoAmI [-cf credential_file] [-Verify]
```

On UNIX systems, the directory path to this command is
`/usr/openv/netbackup/bin/`

On Windows systems, the directory path to this command is
`install_path\NetBackup\bin\`

**DESCRIPTION**

The *bpnbat* command is a tool that enables a user to use the Veritas Product Authentication and Authorization Service.

This service contains the following two distinct parts:

- Authentication - prove who you are
- Authorization - check what you can do
bpnbat enables a user to do authentication tasks from within NetBackup.

If a command needs a password, it doesn’t echo the password or asterisks, which someone can use to narrow the password search space significantly.

NetBackup Access Control requires the user’s home directories to work correctly.

You must have administrator privileges to run the following command options:
-AddDomain, -RemoveDomain, -AddMachine, -AddUser, -RemoveUser, -LoginMachine, and -ShowMachines.

OPTIONS

[-AddDomain | -RemoveDomain] Private_Domain

These options enable an administrator that runs locally on an Authentication server to add or remove domains within the private Veritas Domain Database. These domains are not accessible from within any operating system. They are meaningful only within Veritas Product Authentication and Authorization Service. Use them where a centralized naming authority (such as a PDC/AD or NIS domain) is not available.

-AddMachine

Registers a computer in a private Veritas Product Authentication. The identity is placed in the private domain NBU_Machines@at.server.name. Run this option on your authentication broker (root +ab).

[-AddUser | -RemoveUser] Private_Domain

Enables an administrator that runs locally on an Authentication server to add or remove users from domains in the private Veritas Domain Database. These accounts are meaningful only within Veritas Product Authentication and Authorization Service. Use them when a centralized naming authority (such as PDC/AD or NIS domain) is not available.

-GetBrokerCert

Obtains a broker certificate without authenticating to a broker.

-Login [-Info answer_file] [-cf credential_file] [-LoginType AT|WEB|APIKEY]

Identifies yourself to the system. When you run this command with no options, you are prompted to enter a name, password, domain, authentication type, and a server to authenticate. The combination of a name, password, domain, and domain type creates a unique identity within an Enterprise-wide network. The first time a broker is contacted, you are asked if you want to trust that broker and authenticate them. You cannot use an untrusted broker.
**Note:** You must use the `bpnbdat -login` command to perform certain authorization token and host ID-based certificate-related operations.

The `-Info` option accepts the name, password, and domain information from an answer file. The password is optional in the answer file. You can also place the certificate in a credential file (if specified) or the default location. If you do not provide a password, you are prompted for the password when you run the command.

For the APIKEY login type, the answer file should contain the details in the following order:

- User name
- API key
- Master server

Example of a sample answer file:

```
administrator
A1Wmg0EmC4pKBX1Zjl61qlqJ0YE4-IRacjViMKLg9pUVaU-XJAnroQNaw1nKLanx
nbmaster1
```

**Warning:** Saving the user name and password in a plain text file is a potential security issue. Unauthorized users with read access to the text file can obtain the user name and password for the Veritas Product Authentication and Authorization Service to manually authenticate with the `bpnbdat` command. Make certain that you secure access to the answer text file.

The answer file is a text file with entries for the required information. The answer file for **AT** and **WEB** must contain the four lines that are shown in the order shown:

```
domain type
domain
user name
password
```

A sample answer file is:

```
NT
Sample_Domain
administrator
s@Mpl3
```

As previously explained, `password` is an optional value. The `domain type` value must be one of the values shown:
If you use an answer file, ensure that the appropriate `AUTHENTICATION_DOMAIN` is configured on the server. See the *NetBackup Security and Encryption Guide*.

The NetBackup Web Management Console Service (nbwmc) always runs on the NetBackup master server. The Authentication Broker normally runs on the NetBackup master server as well. But in certain instances, it can run on a host other than the master server.

The answer file for `APIKEY` must contain the three lines that are shown:

```
Login name
API key
Master server
```

If the `-LoginType` is `AT`, only a NetBackup AT broker log on for the master server is performed. If the `-LoginType` is `WEB` or `APIKEY`, only a NetBackup web application log on for the Authentication Broker or the master server is performed. If the `-LoginType` is not specified, both the `AT` and the `WEB` logons are performed if the Authentication Broker is on the master server. If the `-LoginType` is not specified and the Authentication Broker is not on the master server: the `WEB` logon succeeds and the `AT` logon fails. The `AT` logon fails with a security services status code 96. If the `-LoginType` is `APIKEY`, only API key logon is performed. The `-cf` option is not applicable if the `-LoginType` is `WEB` or `APIKEY`.

`-LoginMachine`

Identifies a computer that uses an account within the Veritas Security Subsystem private domain `NBU_Machines@at.server.name`. Run this option on your NetBackup Media, Master, and Clients. This option is similar to when you log on as a user to an authentication broker.

`-Logout [-cf credential_file] [-LogoutType AT|WEB|APIKEY]`

Invalidates the current user credentials that require the user to log on again to continue. Without the `-cf` option, the credential that is stored at the default location is expired. The `-cf` option points to the actual credential file, which allows a user to explicitly specify the credential to be expired.
If the -LogoutType is AT, only a NetBackup AT broker logout is performed. If the -LogoutType is WEB or APIKEY, it is a NetBackup web application logout. If the -LogoutType is not specified, both the AT and the web logout are performed. The -cf option is applicable only for the AT logout.

-RemoveBrokerCert server.name.com
Removes a trust of a specified authentication broker for all users except the root user (administrator). You can use this command to remove a broker when you no longer trust it. For example, an authentication broker is moved to a different corporate division.

-RenewCred [-cf credential_file]
Renews the current user credentials from the VxSS store or the credential file that is specified with the -cf option.

-ShowBrokerCerts
Lists all of the brokers that the user currently trusts. NetBackup trusts any broker that is listed to handle the authentication requests that are sent to it.

-ShowMachines
Lists all computers that have been added to the computers domain of a private Veritas Security Subsystem database by using the -AddMachines option. It also shows if DNS fully resolved the computer name. Run this option on your authentication broker (root +ab).

-Version
Retrieves the version of the executable.

-WhoAmI [-cf credential_file] [-Verify]
Specifies the identity you currently use within Veritas Product Authentication and Authorization Service. It lists the following:

- Name
- Domain
  For API key type of login, the domain is displayed as vrts.apikey
- Authentication broker who issued the credential
- The time a certificate expires
- The domain type that was used when the credential was created

EXAMPLES

Example 1 - The user uses -Login and the default port number to connect to the authentication broker that is called test.domain.veritas.com. (It is the server that handles the Authentication process.) An NIS account is used. Therefore, a domain
name that is associated with the NIS account is provided in addition to a user and password.

# bpnbat -Login
Authentication Broker: test.domain.veritas.com
Authentication port[ Enter = default]:
Authentication type (NIS, NISPLUS, WINDOWS, vx, unixpwd): NIS
Domain: domain.veritas.com
Name: username
Password:
You do not currently trust the server: test.domain.veritas.com, do you wish to trust it? (y/n): y
Operation completed successfully.

Example 2 - The -WhoAmI option verifies the identity that you currently use within the Veritas Product Authentication and Authorization Service.

# bpnbat -WhoAmI
Name: user name
Domain: domain.veritas.com
Issued by: /CN=broker/OU=root@eek.example.com/O=vx
Expiry Date: Oct 27 20:57:43 2009 GMT
Authentication method: NIS
Operation completed successfully.

Example 3 - Add a computer to the computer identities list:

# bpnbat -AddMachine
Machine Name: auto.domain.veritas.com
Password:
Operation completed successfully.

Next, it shows the computer identities list:

# bpnbat -ShowMachines
auto.domain.veritas.com
Operation completed successfully

Then it logs on a computer to a specified authentication broker:

# bpnbat -LoginMachine
Does this machine use Dynamic Host Configuration Protocol (DHCP)? (y/n) n
Authentication Broker: test.domain.veritas.com
Authentication port[ Enter = default]:
Name: auto.domain.veritas.com
Password:
Operation completed successfully.

Finally, you log into a computer to a specified authentication broker and a problem occurs:

If the user has a multi-NIC configuration or types the broker name incorrectly, a second prompt appears. It gives the user a second chance to enter the proper broker name. The following example assumes `sleemanNB` is a private NIC name. The public NIC name that Veritas Product Authentication and Authorization Service uses to build the authentication domain is `sleeman.example.com`. If a failure occurs with `-loginmachine`, the user has a second chance to enter an explicit primary host name for the authentication broker. (Failures include a bad computer name, wrong password, or incorrect broker name.) Refer to the following example:

```
# bpnbat -LoginMachine
Does this machine use Dynamic Host Configuration Protocol (DHCP)?
(y/n) n
Authentication Broker: sleemanNB
Authentication port[ Enter = default]:
Machine Name: challenger
Password:
Primary host name of broker: sleeman.example.com
Operation completed successfully.
```

**Example 4 - Obtain a broker certificate without authenticating to a broker. It expects a broker (test.domain.veritas.com) and a port (0 for default)**

```
# bpnbat -GetBrokerCert test.domain.veritas.com 0
Operation completed successfully.
```

**Example 5 - Lists all the brokers that the user currently trusts**

```
# bpnbat -ShowBrokerCerts
Name: root
Domain: root@test.domain.veritas.com
Issued by: /CN=root/OU=root@test.domain.veritas.com/O=vx
Expiry Date: Jun 12 20:45:19 2006 GMT
Authentication method: Veritas Private Security

Name: root
Domain: root@auto.domain.veritas.com
Issued by: /CN=root/OU=root@auto.domain.veritas.com/O=vx
Expiry Date: Feb 17 19:05:39 2006 GMT
```
Authentication method: Veritas Private Security
Operation completed successfully.

Example 6 - The `-RemoveBrokerCert` option removes a broker when the user no longer wants to trust it. In the following example, an authentication broker is moved to a different corporate division.

```bash
# bpnbat -RemoveBrokerCert test.domain.veritas.com
Operation completed successfully.
```

The user can now use the `-ShowBrokerCerts` option to display current certificates. The previously removed certificate is no longer displayed.

Example 7 - Show how to use an answer file to supply logon information for automated commands (cron, etc.).

For UNIX: The UNIX NIS domain name is `location.example.com`, the user name in this domain is `bgrable`, and the password is `hello456`. The corresponding answer file for `bpnbat -login` must contain the following four lines:

```
NIS
location.example.com
bgrable
hello456
```

If the answer file is located in `/docs` and is called `login.txt`, the `bpnbat command` executes as follows:

```bash
# bpnbat -login -info /docs/vslogin.txt
```

After the `bpnbat -login` command is run, commands like `bpbackup` can be run without authentication errors.

For Windows: The windows domain name is corporate, the user name in this domain is `jsmith`, and the user password is `hello123`. The corresponding answer file for `bpnbat -login` has to contain the following four lines:

```
NT
corporate
jsmith
hello123
```

If the answer file is located in `/docs` and is called `login.txt`, the `bpnbat command` executes as follows:

```bash
# bpnbat -login -info c:\docs\vslogin.txt
```
After the `bpnbat -login` command is run, commands like `bpbackup` can be run without authentication errors.

**Example 8 - How to use the`bpnbat -login` command with the `-LoginType` parameter.**

```bash
# bpnbat -login -LoginType AT
Authentication Broker: server.domain.com
Authentication port [0 is default]: 0
Authentication type (NIS, NISPLUS, WINDOWS, vx, unixpwd, ldap): unixpwd
Domain: server.domain.com
Login Name: root
Password: 
Operation completed successfully.

# bpnbat -login -LoginType WEB
Authentication Broker: server.domain.com
Authentication port [0 is default]: 0
Authentication type (NIS, NISPLUS, WINDOWS, vx, unixpwd, ldap): unixpwd
Domain: server.domain.com
Login Name: root
Password: 
Operation completed successfully.
```

**SEE ALSO**

See `bpnbaz` on page 251.

See `nbcertcmd` on page 574.
**bpbaz**

*bpbaz* – perform Authorization administration tasks from within NetBackup

**SYNOPSIS**


`bpbaz -[AddPerms | DelPerms] Permission_1[,Permission_2,...] -Group Group_Name -Object Object [-M server] [-Server server1.domain.com] [-CredFileCredential]`


`bpbaz -AddRBACPrincipal -User | -UserGroup Domain_Type:Domain_Name:User_Name [-reason "reason"]`


`bpbaz -[AddUser | DelUser] Domain_Type:Domain_Name:User_Name [-reason "reason"] [-CredFile Credential]`


`bpbaz -CheckUpgrade [-Server server1.domain.com]`

`bpbaz -Configureauth`


`bpbaz -ListGroupMembers Group_Name [-M server] [-Server server1.domain.com][-CredFile Credential]`


`bpbaz -LookupUser Domain_Type:Domain_Name:User_Name [-CredFile credential]`
bpbaz -ListUsers [-CredFile credential]

bpbaz -ListLockedUsers [-U | -l] [-User Domain_Type:Domain_Name:User_Name]


bpbaz -SetupAT [-fsa [Domain_Type:Domain_Name:User_Name]]

bpbaz -SetupAuthBroker [target.server.com [-out file] | -file progress_file]


bpbaz -SetupMaster [-fsa [Domain_Type:Domain_Name:User_Name]]


bpbaz -SetupExAudit -DisableExAudit

bpbaz -UnconfigureAuthBroker [target.server.com [-out file] | -file progress_file]

bpbaz -UnlockUser -User [Domain_Type:Domain_Name:User_Name]

bpbaz -UnhookSharedSecSvcsWithPBX [target.server.com [-out file] | -file progress_file]

bpbaz -Upgrade [-Silent] [-Server server1.domain.com]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is \install_path\NetBackup\bin\admincmd\n
DESCRIPTION

NetBackup uses the bpbaz command to access the authorization portion of NetBackup Product Authentication and Authorization Service. Authorization checks the rights on an object. This command enables you to do the following:
- **AddGroup** creates Az groups and **DelGroup** deletes Az groups. **DelGroup** deletes all the members of the group when you delete an Az group from the authorization engine. This operation is not reversible; if you remove a group, you revoke the rights that are granted to members of the group.

**Note:** An authorization (Az) group is a collection within the Authorization engine into which OS groups and OS users can be placed. When you add a user to an Az group, you grant them the rights and privileges that are associated with that group.

- **AddPerms** and **DelPerms** add and delete the specified permissions for the given role on individual policies from the main NetBackup resource objects. For more about permissions, see the NetBackup Administrator's Guide, Volume I.

- **AddPolicy** and **DelPolicy** add and delete policies from the main NetBackup resource objects.

- **AddRBACPrincipal** adds role-based access control (RBAC) permissions for a security administrator and a backup administrator to a specified user or user group. For more about permissions, see the NetBackup Web UI Security Administrator's Guide or the NetBackup Web UI Backup Administrator's Guide.

- **AddUser** and **DelUser** add and delete permissions on individual policies from the main NetBackup resource objects. When used with the enhanced auditing feature, **AddUser** and **DelUser** grant and revoke NetBackup administrator privileges for enhanced auditing. For enhanced auditing, you do not have to include the OSGroup, Server or CredFile options.

- **AllowAuthorization** and **DisallowAuthorization** specify which computers are allowed or not allowed to perform authorization checks. The security administrator must specify which servers (master or media) can examine the Authorization database to perform authorization checks.

- **AllClients** deploys the security certificate to all the available clients.

- **AllMediaservers** deploys the security certificate to all the available media servers.

- **CheckUpgrade** determines if an upgrade of existing authorization information is needed for the specified server. If so, this option returns 61. Only NetBackup installers use this option.

- **Configureauth** configures the Authentication Broker.
Incorrect information for the domain name results in failures during the configuration of Authentication Broker and NetBackup Access Controls. To correct this problem, use this command to configure Authentication Broker:

- **GetConfiguredHosts** obtains NBAC status on the host. Either the **-all** or **target.server.com** option is required for this command.

- **GetDomainInfosFromAuthBroker** requests broker domain maps from the authorization broker.

- **ListGroupMembers** lists the group member that is associated with a particular group defined by **Group_Name**.

- **ListGroup** lists the defined groups

- **ListMainObjects** lists the current permissions for each group on each of the main NetBackup objects. This list is an informative view that you can use to verify changes to permissions on an object. This option shows the permissions each group has within the authorization system.

- **ListPerms** lists the current permissions on NetBackup resource and policies. It shows all applicable permissions for a given object or object type within the database. This option helps the user to create meaningful customizations to their authorization.

- **ListPolicyObjects** displays all objects or object collections that are associated with the specified policy.

- **ListUser** lists all users who have administrator privileges. This parameter is only used in enhanced auditing mode.

- **ListLockedUsers** lists all user accounts that are locked.

- **LookupUser** searches for users to determine if the user has administrative privileges. This parameter is only used in enhanced auditing mode.

- **ProvisionCert** generates an authentication certificate for the specified host and is unique to that host. The certificate must be generated for each host and cannot be pushed from one host to another. An authentication certificate is required on the media servers that host the NetBackup CloudStore Service Container (nbcssc). For more information, see the NetBackup Cloud Administrator's Guide.

The security certificate is also required on master servers, media servers, and clients to establish a secure communication with the NetBackup-Java Administration Console.

For more information, see the NetBackup Cloud Administrator's Guide.
**Note:** Starting with NetBackup 8.3, this option is only required when the media server version is older than 8.3. If your master server is 8.3, and your media server is 8.1.2, this option is still required.

- **-SetupAT** generates credentials for all nodes in a clustered master environment. Run this command after NetBackup installation or upgrade.
- **-SetupAuthBroker** sets up the authentication broker to use NBAC.
- **-SetupClient** sets up NBAC on the client. Run it after `bpnbaz -SetupMaster` has been completed successfully. It can be run from the master server. It expects connectivity between the master server and target client systems. By default, NBAC messages are logged to a file in the local directory that is called `SetupClient.nbac`. The following is an example of the format of this file:

```
client1.server.com
#client2.server.com #SUCCESS (0) @ (07/16/10 12:09:29)
client3.server.com #INTERNAL_ERROR(68) @ (07/16/10 12:09:39)
```

- The first line indicates that client1.server.com has not yet been contacted at all.
- The second line indicates that client2.server.com has been successfully contacted. Each success is commented out (with a leading #) and not contacted multiple times.
- The third line indicates that client3.server.com has been contacted but an error has occurred. Errors are printed out on the command line with a recommendation of what to do. The error number that is indicated in the logs may indicate the problem.

- **-SetupMaster** sets up the master server to use NBAC. The `bpnbaz -SetupMaster` command contains no user arguments. You are prompted for the password for your current operating system user identity. The authorization server and authentication broker must be installed and running on the master server.
  - `SetupMaster` adds root/administrator by default to the NBU_Security Admin group. The first time that you use `SetupMaster` with the `-fsa` option adds the first security administrator member to the NBU_Security Admin group. If you have configured NBAC already using `SetupMaster` without the `-fsa` option, use the `-AddUser` option to add any more members.

- **-SetupMedia** sets up the media server to use NBAC. An NetBackup administrator group member can run the `bpnbaz -SetupMedia` command after `bpnbaz -SetupMaster` has been completed successfully. It can be run from the master server.
server and expects connectivity between the master server and target media server systems. By default, NBAC messages are logged to a file in the local directory that is called SetupClient.nbac. Refer to the SetupClient description of an example of the file format.

- **SetupSecurity** sets up the initial security information. It must be run as root on the Az server.
- **ShowAuthorizers** lists the computers that are allowed to perform authorization checks.
- **-U** list type is user.
- **-UnlockUser** unlocks the specified user account.
- **-User** is optional for the **-ListLockedUsers** parameter. It lists information about the specified user account. Data is returned only if the user account is locked. This option is required when using the **-UnlockUser** parameter.
- **-UnconfigureAuthBroker** removes the configuration from the Authorization Broker.
- **-UnhookSharedSecSvcsWithPBX** unhooks the shared Authentication and Authorization services from PBX in Windows Server Failover Clustering (WSFC) environments.
- **-Upgrade** modifies the NetBackup operation schema by adding authorization objects. In addition, this option upgrades default user accounts with default permissions for these new objects. You must have NBU_Security Admin privileges.

For more about NBAC and the use of the `bpnbaz` command, see the *NetBackup Security and Encryption Guide*.

To use this command and its associated options, you must be a member of the NetBackup Security Administrators group (NBU_Security Administration). The only exception is with the **SetupSecurity** command.

You must have local administrator privileges on the authorization server to run this command.

When you use `bpnbaz`, assume that the master server and the Az server are the same computer.

---

**Note:** The use of NetBackup Access Control requires the user’s home directories to work correctly.
NetBackup has enhanced the audit capability that helps to audit users without having to enable NBAC. NetBackup administrators can delegate NetBackup administrator privileges to designated users. For more information about enhanced auditing and the use of the `bpnbaz` command with this feature, see the NetBackup Security and Encryption Guide.

**OPTIONS**

- **-all**
  Scans all the storage units or policies and collects all the associated unique host names that are found in the policies. You can scan in a sorted order. The results are written to the progress file.

  ```plaintext
  client.server.com
  ```

  Specifies the name of a single target host. Use this option to add a single additional host for use with NBAC.

- **-CredFile Credential**
  Specifies a file name (Credential) from which to obtain a Veritas Product Authentication and Authorization Service credential, rather than the default location.

- **-disable**
  Disables NBAC (USE_VXSS = PROHIBITED) on targeted hosts.

- **-DisableExAudit**
  Disables Enhanced Auditing mode. You must restart the NetBackup services after you run this command. For additional information about Enhanced Auditing, see Auditing NetBackup Operations in the NetBackup Security and Encryption Guide.

- **Group_Name**
  Identifies the authorization group on which an operation is to be performed. NetBackup does not allow user groups to be nested.

- **Domain_Type:Domain_Name:User_Name**
  The `Domain_Type` variable is the domain to which the user or group belongs, and the `User_Name` variable defines the applicable user or group name designating the NetBackup administrator.

- **-dryrun**
  Generates a list of computers to receive the security certificate. The exact details of how this option works depends on the parameter with which it is used.

  ```plaintext
  dryrun, when used with ProvisionCert
  ```
Generates a list of hosts to receive the security certificate and writes that list to the file name that is provided in the -out option. The -dryrun option only works with the –AllMediaservers and the –AllClients parameters. Generates a list of hosts to receive the security certificate and writes that list to the file name that is provided in the -out option. If the -out file option is not provided, then the host list is written to the default DeploySecurityCerts.progress file.

- dryrun, when used with either SetupMedia or SetupClient
Generates a list of media server names or client names depending on the option used. The command writes the list of names to the log. This option works with client.server.com and media.server.com but the intention is to use it with the -all option. Generates the list of media server names and writes them to the log. The log file name is SetupMedia.nbac if the command is used with SetupMedia option. The log file name is SetupClient.nbac if the command is used with SetupClient option.
If you have more than 250 clients, use -dryrun with -SetupClient to see all of the clients that are visible to the master server.

- file progress_file
Specify a different file name for the progress log. If -file is used, the input and the output files are the same, which allows multiple rounds to execute without changing the command. Use the progress file iteratively by feeding the file back in multiple times until all clients are available online.

- fsa
Provisions a specific OS user as the NetBackup administrator. You are asked for the password for your current OS user identity.

Group_Name
Adds the users by creating a unique enterprise account name, following this format: Authentication type:Domain_Type:User_Name
The supported Authentication types for this variable are the following:
- Nis - Network Information Services
- NISPLUS - Network Information Services Plus
- Unixpwd - UNIX Password file on the Authentication server
- WINDOWS - Primary Domain Controller or Active Directory
- Vx - Veritas Private database.

- images
- images searches all images for unique host names. Do not use this option with large catalogs unless you include the -dryrun option. This option discovers
all unique clients that are contained in the image catalog. Older catalogs may contain a large number of decommissioned hosts, renamed hosts, and hosts relocated to new masters. Run-time can increase significantly as this command tries to contact unreachable hosts.

-M server
  Specifies the name of the master server as defined in the variable server. This server name may be different from the local host name.

Machine_Name
  Specifies the computer to be allowed or disallowed to perform authorization checks. The security administrator must specify which master servers or media servers can examine the Authorization database to perform authorization checks.

media.server.com
  Specifies the name of a single target host. Use this option to add a single additional host for use with NBAC.

-Object Object
  Controls the access to specified objects or object collections.

-OSGroup
  Defines a named collection of authentication principals that are established in a native operating system and treated as a single entity. All members of an authentication group or OS group are from the same authentication domain.

-out file
  Specifies a custom output file name. By default, the output is written to the SetupMedia.nbac file. Use this option with the -all option.

Permission_1[,Permission_2,...]
  Permissions for the role that is given to the designated object or policy.

policy_name
  Specifies the name of the policy from the main NetBackup resource objects.

-ProvisionCert media_server_name
  Generates an authentication certificate for the media server that is indicated.

-reason "reason"
  For enhanced auditing, the reason indicates the reason why the command is used. The reason text string that is entered is captured and appears in the audit report. The string must be enclosed in double quotes ("...") and cannot exceed 512 characters. In addition, it cannot begin with a dash character (-) and must not contain the single quotation mark symbol (').
-Server server1.domain.com

This option specifies the Az server being used. Currently we expect the Az server and the NetBackup master server to exist on the same system.

Determines if an upgrade of existing authorization information is needed for the specified server. If so, this option returns "61". Only NetBackup installers use this option.

-SetupExAudit

Enables Enhanced Auditing mode. You must restart the NetBackup services after you run this command. For additional information about Enhanced Auditing, see Auditing NetBackup Operations in the NetBackup Security and Encryption Guide.

-Silent

Directs the upgrade operation to automatically enhance the permissions of groups to account for new objects in the system. This option occurs only for the default groups, and only if those groups have never been changed.

target.server.com

Specifies the name of a single target host. Use this option to find the NBAC status on a single host. It captures the status of the host in the ConfiguredHosts.nbac file.

EXAMPLES

Example 1 - Create and list an Az group.

An Az group is a collection within the Authorization engine where other OS groups and OS users are placed. This collection is the building block against which permissions are applied on the objects within the database. If you add a user to an Az group, you grant them all the rights and privileges that are associated with that group. When a user is placed in more than one group, that user’s effective permissions are as follows: the logical "or" of the applicable permissions of each group to which the user belongs. The following example demonstrates how to create and list an existing Az group:

# bpnbaz -AddGroup "New Group 1" -server test.domain.veritas.com
Operation completed successfully.
# bpnbaz -ListGroups -server test.domain.veritas.com
Administrators
Operatorsroo
Security Administrators
Resource Management Applications
Applications
New Group 1
Example 2 - Delete an Az group.

If you delete an Az group from the authorization engine, all the members are removed from the group. This operation is not reversible. When you remove a group, you revoke the rights that are granted to members of the group. Therefore, carefully consider the implications of deleting groups.

```
# bpnbaz -DelGroup "New Group 1" -server test.domain.veritas.com
Operation completed successfully.
```

```
# bpnbaz -ListGroups -server test.domain.veritas.com
Administrators
Operators
Security Administrators
Resource Management Applications
Applications
NBU_Unknown
NBU_User
NBU_Operator
NBU_Media Device Operator
NBU_Admin
NBU_Executive
NBU_Security Admin
NBU_Database Agent Operator
NBU_Database Agent Administrator
Operation completed successfully.
```

Example 3 - Add and remove users from Az groups (and List group members)

Add users by creating a unique enterprise name of the following format:

```
Authentication type:Domain to which user or group belongs:user or group name
```

The following are the Supported Authentication types:

- **Nis** - Network Information Services
- **NisPlus** - Network Information Services Plus
Unixpwd - UNIX Password file on the Authentication server

WINDOWS - Primary Domain Controller or Active Directory

Vx - Veritas Private database

```
# bpnbaz -AddUser NBU_Operator
nis:domain.veritas.com:ssosa -server test.domain.veritas.com
Operation completed successfully.
# bpnbaz -ListGroupMembers
NBU_Operator -server test.domain.veritas.com
==========
Type: User
Domain Type: nis
Domain:domain.veritas.com
Name: jdimagio
==========
Type: User
Domain Type: nis
Domain:domain.veritas.com
Name: ssosa
Operation completed successfully.
# bpnbaz -DelUser NBU_Operator
nis:domain.veritas.com:ssosa -server test.domain.veritas.com
Operation completed successfully.
# bpnbaz -ListGroupMembers
NBU_Operator -server test.domain.veritas.com
==========
Type: User
Domain Type: nis
Domain:domain.veritas.com
Name: jdimagio
Operation completed successfully.
```

Example 4 - List applicable permissions

The -ListPerms option shows all applicable permissions for a given object or object type within the database. This information helps the user to create meaningful customizations to their authorization.

```
# bpnbaz -ListPerms -server
test.domain.veritas.com
  Object Type: Unknown
  Browse
  Object Type: Media
    Browse
```
Operation completed successfully.

Example 5 - List main objects

The -ListMainObjects option lists the current permissions for each group on each of the main NetBackup objects. This list is an informative view that can be used to verify changes to permissions on an object. It shows what permissions each group has within the authorization system.

```
# bpnbaz -ListMainObjects -server test.domain.veritas.com
.
NBU_RES_Policy:
  Role: NBU_User
    Unknown
  Role: NBU_Media Device Operator
    Browse
    Read
  Role: NBU_Executive
    Read
    Browse
  Role: NBU_Database Agent Operator
    Unknown
    Role: NBU_Unknown
  Unknown
  Role: NBU_Operator
    Browse
    Read
  Role: NBU_Admin
```
Browse
New
Activate
Backup
Read
Delete
Deactivate

Role: NBU_Security Admin
    Unknown
Role: NBU_Database Agent Administrator
    Unknown
Role: Administrators
    Unknown
Role: Operators
    Unknown
Role: Applications
    Unknown
Role: NBU_Security Admin
    Unknown

... 

NBU_RES_Job:
    Role: NBU_Media Device Operator
        Browse
        Suspend
        Cancel
        Read
        Resume
        Delete
    Role: NBU_Executive
        Browse
        Read
    Role: NBU_Database Agent Operator
        Unknown
    Role: NBU_User
        Unknown
    Role: NBU_Unknown
        Unknown
    Role: NBU_Operator
        Browse
        Suspend
        Cancel
        Read
        Resume
Delete
Role: NBU_Admin
Browse
Delete
Resume
Read
Suspend
Cancel
Role: NBU_Security Admin
Unknown
Role: NBU_Database Agent Administrator
Unknown
Role: Administrators
Unknown
Role: Operators
Unknown
Role: Applications
Unknown
Role: NBU_Security Admin
Unknown
...
Operation completed successfully.

Example 6 - Add and delete permissions from an object or policy

Delete all permissions from an object for a given group. Add the permissions that are specified for the given role to the object or policy in question.

# bpnbaz -AddPerms Browse,Read,
New,Delete -Group TestGroup1 -Object NBU_RES_Job -server test.domain.veritas.com
Operation completed successfully.
# bpnbaz -ListMainObjects -server test.domain.veritas.com
NBU_RES_Unknown:
  Role: NBU_User
  ...
NBU_RES_Job:
  Role: NBU_Media Device Operator
    Browse
    Suspend
    Cancel
    Read
    Resume
Delete
Role: NBU_Executive
   Browse
   Read
Role: NBU_Database Agent Operator
   Unknown
Role: TestGroup1
   Read
   Delete
   New
   Browse
Role: NBU_User
   Unknown
Role: NBU_Unknown
   Unknown
Role: NBU_Operator
   Browse
   Suspend
   Cancel
   Read
   Resume
   Delete
Role: NBU_Admin
   Browse
   Delete
   Resume
   Read
   Suspend
   Cancel
Role: NBU_Security Admin
   Unknown
Role: NBU_Database Agent Administrator
   Unknown
Role: Administrators
   Unknown
Role: Operators
   Unknown
Role: Applications
   Unknown
Role: NBU_Security Admin
   Unknown
NBU_RES_Service:
   Role: NBU_Unknown
Operation completed successfully.
# bpnbaz -DelPerms -Group TestGroup1 -Object NBU_RES_Policy -server test.domain.veritas.com
Operation completed successfully.

Example 7 - Specify what servers can perform authorization checks

This example also views what servers can perform authorization checks. In addition, it also disallows a server from performing authorization checks.

The -AllowAuthorization option specifies which computers are allowed to perform authorization checks. The security administrator must specify which servers (Master or Media) are permitted to examine the Authorization database to perform authorization checks. The following examples demonstrate how to allow or disallow a computer to perform authorization.

# bpnbaz -AllowAuthorization butterball.domain.veritas.com -server test.domain.veritas.com
Operation completed successfully.

# bpnbaz -ShowAuthorizers -server test.domain.veritas.com
==========
Type: User
Domain Type: vx
Domain: NBU_Machines@test.domain.veritas.com
Name: butterball.domain.veritas.com
Operation completed successfully.
# bpnbaz --DisallowAuthorization butterball.domain.veritas.com -server test.domain.veritas.com
Operation completed successfully.
# bpnbaz -ShowAuthorizers -server test.domain.veritas.com
Operation completed successfully.

Example 8 - Set up initial security boot strapping

The user must run the -SetupSecurity option as root on the Az server. The user must then provide the logon information for the first NetBackup Security administrator.

Note: The root user on the system upon which the Az server is installed is always a security administrator.
# bpnbaz -SetupSecurity
test.domain.veritas.com -server test.domain.veritas.com
Authentication Broker: test.domain.veritas.com
Authentication port[ Enter = default]:
Domain: domain.veritas.com
Name: ssosa
Password: Authentication type (NIS, NISplus, WINDOWS, vx, unixpwd: NIS
Operation completed successfully.

SEE ALSO

See bpnbat on page 242.
bppficorr

bppficorr – list the persistent snapshot information in the NetBackup catalog for a specified client and delete catalog entries for the snapshots that no longer exist

SYNOPSIS

bppficorr [-media] [-hoursago hours] [-policy policy_name] -client client_name

bppficorr -rotation -policy policy_name -client client_name -fim fim_args

bppficorr -delete_snapshot -fragment_id fragment_id -client client_name [-cnum copy_number] [-ctype MIRROR | NON_MIRROR]

bppficorr -report -clientlist snapshot_client_list_file

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

For the specified client, bppficorr lists the persistent snapshots currently found in the NetBackup catalog. Without the -media option, bppficorr compares the catalog information to the actual information on the client. It removes any entries in the catalog that do not have corresponding snapshots on the client. This option is useful if a snapshot on the client is renamed or removed.

Note: NetBackup manages persistent snapshots. Do not rename or remove a persistent snapshot; otherwise, the data cannot be restored.

The output of bppficorr goes to standard output.

You must have administrator privileges to initiate this command.
OPTIONS

-client client_name
  A required option. NetBackup lists the persistent snapshot information in the
  NetBackup catalog for this client. This name must be as it appears in the
  NetBackup catalog. By default, bppficorr searches for all clients.

-clientlist snapshot_client_list_file
-cnnum copy_number
-ctype MIRROR | NON-MIRROR
-delete_snapshot
-fim fim_args
-fragment_id fragment_id
-hoursago hours
  Includes the images that were written up to n hours ago (1 or greater). The
  default is all images.

-media
  Lists all persistent snapshot entries in the NetBackup catalog for the client that
  is specified on the -client option. The list includes the backup IDs and the
  media descriptions for each backup ID.

  For more about the media description, See the NetBackup Administrator’s
  Guide, Volume II.

-policy policy_name
  NetBackup lists the persistent snapshot information in the NetBackup catalog
  for this policy for the specified client. The default is all policies that include the
  client that is specified on the -client option.

-report
-rotation

NOTES

bppficorr writes activity log information to the /usr/openv/netbackup/logs/admin
directory (UNIX systems) or the install_path\NetBackup\logs\admin directory
(Windows systems). You can use the information in the directory for troubleshooting.

EXAMPLES

Example 1 - Resynchronize the NetBackup catalog with a client’s actual snapshots:
# bppficorr -client lupine

Example 2 - Display the snapshots that are currently in the catalog for client lupine:

# bppficorr -media -client lupine

Sample output:

<table>
<thead>
<tr>
<th>backup_id</th>
<th>created</th>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Mon Oct 7 08:01:20 2002</td>
<td>vxfs_pfi:34:vxfs:/ora8:VX+NBU+PFI+ORA+2002.10.07.08h01m20s</td>
</tr>
<tr>
<td>3</td>
<td>Sun Oct 6 00:00:59 2002</td>
<td>vxfs_pfi:34:vxfs:/V1fs/VX+NBU+PFI+FS+2002.10.06.00h00m59s</td>
</tr>
</tbody>
</table>
bpplcatdrinfo

bpplcatdrinfo – list, modify, or set the disaster recovery policies

SYNOPSIS

bpplcatdrinfo policy_name [-v] [-M master_server] -L | -l | -U
bpplcatdrinfo policy_name -set | -modify [-v] [-M master_server,...]
    [-generation generation] [-reason "string"] [-e email] -p path [-u user] [-pwd password] [-cp critical_policy_name1 critical_policy_name2 ...

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\

DESCRIPTION

The bpplcatdrinfo command lists, sets, and modifies the disaster recovery and
critical policy information for policies of type NBU-Catalog:

Authorized users can initiate this command.

For more about NetBackup authorization, see the NetBackup Security and
Encryption Guide.

Note:

It is not recommended that users modify or delete automanaged policies.

If the user modifies the policy, they must make sure that the policy continues to
meet the service level objective as defined by the protection plan.

If the user deletes the policy, they must make sure that the asset is added to another
protection plan that meets the service level objective.

OPTIONS

-cp critical_policy_name1 ...
   Lists the policy names that need to be added as critical policies.
-e email
    Specifies the email address where the disaster recovery information is sent
    when a catalog backup completes.

-g generation
    Ensures that the command acts on a specific generation or version of a policy.
    The generation value increments each time a policy is saved. Use bpplinfo
    or bpplist to list the current generation value. If no generation is specified,
    the command acts on the current version.

-L
    Displays the listing in long format. See EXAMPLE that follows.

-l
    Displays the listing in short format; this option produces a terse listing. It also
    is called raw output mode. See EXAMPLE that follows.

-M master_server,...
    Lists alternative master servers. This option consists of a comma-delimited list
    of host names. If this option is present, each master server in the list runs the
    bpplcatdrinfo command. Each master server in the list must allow access
    by the system that issues the bpplcatdrinfo command. If an error occurs for
    any master server, the process stops at that point.
    If bpplcatdrinfo produces a list, the list is the composite of the returned
    information from all the master servers in this list.
    If bpplcatdrinfo adds, deletes, or modifies a client (explained later), the
    change is made on all the master servers in this list.

-modify
    Updates only the specified fields in the catalog policy. The fields that are not
    specified remain unchanged.

-p path
    Specifies the disk path where the disaster recovery information is stored when
    the catalog backup runs.

policy_name
    Specifies the name of the policy whose disaster recovery information is set,
    modified, or listed.

-pwd password
    Specifies the password if one is needed to access the path (-p). The -u option
    specifies the user ID.
-reason "string"
Indicates the reason that you choose this command action. The reason text string is captured and appears in the audit report. Enclose this string with double quotes ("..."). The string must not exceed 512 characters. It cannot begin with a dash character (-) nor contain a single quotation mark (’).

-set
Modify updates of the specified fields in the catalog policy. The fields that are not specified are cleared.

-U
Displays the listing in user format. This output format is exactly the same as -L.

-u user
The user ID that is used with the password (-pwd) to access the path (-p).

-v
Selects the verbose mode. This option causes bpplcatdrinfo to log additional information for debugging purposes. The information goes into the NetBackup administration daily debug log. This option is meaningful only when you enable the debug log function (that is, when the following directory is defined):

UNIX systems: /usr/openv/netbackup/logs/admin
Windows systems: install_path\NetBackup\logs\admin

EXAMPLE
Set the disaster recovery information path, username, password, email, and four critical policies for NBU-Catalog policy catpol. Then list the catalog disaster recovery configuration for catpol in long format (-L) and short format (-l).

# bpplcatdrinfo catpol -set -e test@domain.com -p /drx -u test -pwd passwd -cp pol1 pol2 pol3 pol4
# bpplcatdrinfo catpol -L
Catalog Disaster Recovery Configuration:
  Email Address:  test@domain.com
  Disk Path:     /drx
  User Name:     test
  Pass Word:     xxxx
  Critical policy:
      pol1
      pol2

NetBackup Commands
bpplcatdrinfo 274
pol3
pol4

# bpplcatdrinfo catpol -l
DR_EMAIL test@domain.com
DR_PATH /drx
DR_MEDIA_ID *NULL*
DR_DENSITY 0
DR_USER_NAME test
DR_PASSWORD 1
DR_CRITICAL_POLICY pol1 pol2 pol3 pol4

SEE ALSO

See bpplinclude on page 289.
See bpplinfo on page 297.
See bppllist on page 324.
See bppolicynew on page 363.
bpplclients

bpplclients – administer clients within NetBackup policies

SYNOPSIS

bpplclients policy_name | {[-allunique | -allunique_hw_os] [-pt policy_type]} [-L | -l | -U | -noheader] [-M master_server,...] [-v] [-include_discovered]

bpplclients policy_name [-M master_server,...] [-v] [-generation generation] [-reason "string"] -add host_name hardware_os [-priority priority]

bpplclients policy_name [-M master_server,...] [-v] [-generation generation] [-reason "string"] -delete host_name ...

bpplclients policy_name [-M master_server,...] [-v] [-generation generation] [-reason "string"] -modify host_name [-hardware hardware] [-os os] [-priority priority]

bpplclients policy_name -rename old_client_name new_client_name [-os os] [-priority priority] [-hardware hardware] [-generation generation] [-reason "string"]

bpplclients policy_name [-M master_server,...] [-v] [-generation generation] [-reason "string"] {add_rac_database db_unique_name dbid} | {delete_rac_database db_unique_name dbid} {add_rac_pdb db_unique_name dbid pluggable_database_name} | {delete_rac_pdb db_unique_name dbid pluggable_database_name}

bpplclients policy_name [-M master_server,...] [-v] [-generation generation] [-reason "string"] {add_availability_group -ag_name availability_group_name [-cluster cluster_name] [-ag_id availability_group_ID]} | {delete_availability_group -ag_name availability_group_name [-cluster cluster_name] [-ag_id availability_group_ID]}

bpplclients policy_name [-M master_server,...] [-v] [-generation generation] [-reason "string"] {add_availability_group_database -ag_name availability_group_name -database database_name [-cluster cluster_name] [-ag_id availability_group_ID]} | {delete_availability_group_database -ag_name availability_group_name...}
bpplclients does one of the following:

- Produces a listing of clients.
- Adds a new client to a policy.
- Deletes a list of clients from a policy.
- Modifies an existing client in a policy.
- Adds a SQL Server object to a SQL Server Intelligent policy: instance, instance group, a specific database in an instance, availability group, or availability database.
- Deletes a SQL Server object from a SQL Server Intelligent policy: instance, instance group, a specific database in an instance, availability group, or availability database.
- Adds an Oracle object to an Oracle Intelligent Policy: instance, instance group, a specific pluggable database in an instance, or RAC database.
Deletes an Oracle object from an Oracle Intelligent Policy: instance, instance
group, a specific pluggable database in an instance, or RAC database.

For the -add, -delete, and -modify options, bpplclients returns to the system
prompt immediately after it submits the client change request to NetBackup. To
determine whether the change was successful, run bpplclients again to list the
updated client information.

When the listing option is used, the list is ordered alphabetically by client name.
Each client entry is on a single line, with a single entry for each client.

Authorized users can initiate this command.

For more about NetBackup authorization, see the NetBackup Security and
Encryption Guide.

Note:

It is not recommended that users modify or delete automanaged policies.

If the user modifies the policy, they must make sure that the policy continues to
meet the service level objective as defined by the protection plan.

If the user deletes the policy, they must make sure that the asset is added to another
protection plan that meets the service level objective.

OPTIONS

bpplclients consists of two forms. The bpplclients form that you use determines
the options that you use with bpplclients.

The first form of bpplclients has no options and produces a listing of information
about the clients for all policies. For SQL Server Intelligent policies, bpplclients
produces a list of the instance groups or the instances and databases for all policies.
If you have other policy types, it is best to use bpplclients policy_name to display
the backup selections for an MS-SQL-Server policy.

The second form of bpplclients produces a listing of information about the clients
for a single policy or for all policies. The following options apply to this form:

- add_availability_group -ag_name availability_group_name [-cluster
  cluster_name] [-ag_id availability_group_ID]

  This option applies to SQL Server Intelligent Policies. Adds an availability group
to the policy.

  In the policy attributes (bpplinfo), -client_list_type must be set to 3
  (AVAILABILITY_GROUP). For advanced and basic availability groups, provide
  the -cluster cluster_name. For read-scale availability groups, provide the
-ag_id availability_group_ID. You can add availability groups and availability databases to the same policy. You cannot add instance groups, instances, or standalone databases to a policy that contains availability groups or availability databases.

-add_availability_group_database -ag_name availability_group_name -database database_name [-cluster cluster_name] [-ag_id availability_group_ID]

This option applies to SQL Server intelligent policies. Adds a specific availability database to the policy.

In the policy attributes (bpplinfo), -client_list_type must be set to 3 (AVAILABILITY_GROUP). For advanced and basic availability groups, provide the -cluster cluster_name. For read-scale availability groups, provide the -ag_id availability_group_ID. You can add availability groups and availability databases to the same policy. You cannot add instance groups, instances, or standalone databases to a policy that contains availability groups or availability databases.

-add_rac_database db_unique_name dbid

This option applies to Oracle Intelligent Policies. Adds a RAC database to the policy. In the policy attributes (bpplinfo), -client_list_type must be set to 4 (RAC_DATABASE).

-add host_name hardware os [priority]

Adds a client to the policy. If the local system has defined the maximum number of clients already, an error is returned. The maximum number of clients is unlimited (the installation default) for NetBackup Enterprise Server and 4 for NetBackup Server. Specify the host name, hardware type, and operating system. The priority option is not implemented at this time.

To back up a Nutanix Acropolis Cluster, you must add the display name of the virtual machine. The display name of a virtual machine is case-sensitive and it must not include a space.

For the NAS-Data-Protection policy, the clients are the NAS storage arrays or filers. You can add a NetApp filer as client entry in this policy in the form of cluster@StorageVirtualMachine and for Nutanix in the form of NutanixFileServer@NAS-Array-Asset.

-add_instance_database instance_name database_name host_name

This option applies to SQL Server intelligent policies. Adds a specific database in an instance to the policy.

In the policy attributes (bpplinfo), -client_list_type must be set to 1 (INSTANCE). You can add instances and databases to the same policy. You
cannot add instances groups, availability groups, or availability databases to a policy that contains instances or standalone databases.

```
-add_instance_pdb instance_name pluggable_database_name host_name
```

This option applies to Oracle Intelligent Policies. Adds a specific pluggable database in an instance to the policy.

```
-add_instance instance_name host_name
```

This option applies to SQL Server and Oracle Intelligent Policies. Adds an instance to the policy.

In the policy attributes (`bpplinfo`), `-client_list_type` must be set to 1 (`INSTANCE`). You can add instances and databases to the same policy. You cannot add instances groups, availability groups, or availability databases to a policy that contains instances or standalone databases.

```
-add_instance_group instance_group_name
```

This option applies to SQL Server and Oracle Intelligent Policies. Adds an instance group to the policy.

In the policy attributes (`bpplinfo`), `-client_list_type` must be set to 2 (`INSTANCE_GROUP`). You cannot add instances, standalone databases, availability groups or availability databases to a policy that contains instances or instances groups.

```
-delete_availability_group -ag_name availability_group_name [-cluster cluster_name] [-ag_id availability_group_ID]
```

This option applies to SQL Server intelligent policies. Deletes an availability group from the policy. For advanced and basic availability groups, provide the `-cluster cluster_name`. For read-scale availability groups, provide the `-ag_id availability_group_ID`.

```
-delete_availability_group_database -ag_name availability_group_name -database database_name [-cluster cluster_name] [-ag_id availability_group_ID]
```

This option applies to SQL Server intelligent policies. Deletes an availability database from the policy. For advanced and basic availability groups, provide the `-cluster cluster_name`. For read-scale availability groups, provide the `-ag_id availability_group_ID`.

```
-delete_rac_db db_unique_name dbid
```

This option applies to Oracle Intelligent Policies. Deletes a RAC database from the policy.

```
-delete host_name ...
```

Deletes one or more clients from the policy. Up to 20 clients can be deleted at a time. Specify the clients as a space-delimited list of host names.
-delete_instance {instance_name host_name [instance_name2 host_name2] [...]}  
This option applies to SQL Server and Oracle Intelligent Policies. Deletes an instance from the policy. Up to 20 instances can be deleted at a time. Group instances and host names in a space-delimited list.

-delete_instance_database {instance_name1 database_name1 host_name1 [instance_name2 database_name2 host_name2] [...]}  
This option applies to SQL Server intelligent policies. Deletes a database in an instance from the policy. Up to 20 databases can be deleted at a time. Group database names, instance names, and host names in a space-delimited list.

-delete_instance_pdb instance_name pluggable_database_name host_name  
This option applies to Oracle Intelligent Policies. Deletes a pluggable database in an instance from a policy.

-delete_instance_group instance_group_name ...  
This option applies to SQL Server and Oracle Intelligent Policies. Deletes an instance group from the policy. Up to 20 instance groups can be deleted at a time. Specify the names in a space-delimited list.

-generation generation  
Ensures that the command acts on a specific generation or version of a policy. The generation value increments each time a policy is saved. Use bpplinfo or bppllist to list the current generation value. If no generation is specified, the command acts on the current version.

-hardware hardware  
Specifies the hardware type of this client. In the dialog box for adding clients to a policy with the Backup Policy Management utility, select one of the hardware types.

-include_discovered  
This option lists the virtual machines that were discovered and selected the last time a VMware or Hyper-V intelligent policy ran. It also lists the host that performed the virtual machine discovery, such as the media server. This option is ignored if the intelligent policy has never been run.

When the option is used with -allunique, it additionally lists the virtual machines that were discovered and selected in the last run of all VMware and Hyper-V intelligent policies.

When the option is used with -allunique -pt policy_type and the policy_type is either VMware or Hyper-V, it lists the virtual machines that were discovered and selected in the last run of all VMware or all Hyper-V intelligent policies.
-L
Displays the listing in long format. No two-line header appears at the top of the listing; the header is embedded in the line for each client. The line for each client includes the following fields:
Client/HW/OS/Pri: (the header)
Client name
Hardware type
Operating system
Priority
Ignore the four additional fields. They are either unused or used for internal processes.

-l
Displays the listing in short format; this option produces a terse listing. It also is called raw output mode. No two-line header appears at the top of the listing; the header is embedded in the line for each client. The listing consists of the following fields:
Field 1 = Client name
Field 2 = Hardware. The operating system type of the client. Example: Linux
Field 3 = Operating system name of the client. Example: RedHat
Field 4 = Priority. The priority of the client in the specified policy.
Fields 5-7 are unused.
This option is useful for scripts or the programs that rework the listing contents into a customized report format.

-M master_server,...
Lists the alternative master servers. This option consists of a comma-delimited list of host names. If this option is present, each master server in the list runs the \( \text{bpplclients} \) command. Each master server in the list must allow access by the system that issues the \( \text{bpplclients} \) command. If an error occurs for any master server, the process stops at that point.
If \( \text{bpplclients} \) produces a list, the list is the composite of the returned information from all the master servers in this list.
If \( \text{bpplclients} \) adds, deletes, or modifies a client (explained later), the change is made on all the master servers in this list.
-modify host_name ...

Modifies the attributes for a client within a policy. The client was added to the policy previously. The attribute values follow the client name and replace the previous equivalent attribute values for this client. You must modify at least one of the client’s attributes. -priority is not implemented at this time.

-noheader

Displays the listing without any header. The listing consists of one line for each client, which contains the hardware type, operating system, and client name.

-os os

Specifies a different operating system for the client. In the dialog box for adding clients to a policy with the Backup Policy Management utility, select one of the operating systems.

The values that you choose for the hardware and the -os options must form a valid combination.

policy_name | {[-allunique | -allunique_hw_os] [-pt policy_type]}

If the policy_name option is used it must be the first option on the command line.

The policy_name specifies the name of a policy. It lists client information only for that policy.

If you use -allunique without the -pt policy_type option, the command lists client information for all policies that are defined for NetBackup on the master server.

If you use -allunique -pt policy_type, the command lists the client information for only the clients that belong to that policy type.

The -allunique_hw_os without the -pt policy_type option lists all unique hosts based on host name, hardware, and operating system information.

If you use -allunique_hw_os -pt policy_type, the command lists all unique hosts based on host name, hardware, and operating system information for all clients that belong to that policy type.

-pt policy_type

Specifies the policy type by entering one of the following character strings (the default is Standard):

BigData
DataStore
DataTools-SQL-BackTrack
DB2
Deployment
Enterprise-Vault
FlashBackup
Hyper-V
Informix-On-BAR
Lotus-Notes
MS-Exchange-Server
MS-SharePoint
MS-SQL-Server
MS-Windows
NAS-Data-Protection
NBU-Catalog
NDMP
Oracle
PureDisk-Export
SAP
Split-Mirror
Standard
Sybase
Vault
VMware

-priority priority
   Not implemented.

policy_name
   Identifies the policy that has the client. This option must be the first option on
   the command line.

-reason "string"
   Indicates the reason that you choose this command action. The reason text
   string is captured and appears in the audit report. Enclose this string with double
   quotes ("..."). The string must not exceed 512 characters. It cannot begin with
   a dash character (-) nor contain a single quotation mark (').

-rename old_client_name new_client_name
   old_client_name specifies the current name of the client and new_client_name
   specifies the new name.

-U
   Displays the listing in user format. The listing consists of one line for each
   client, which contains the hardware type, operating system, and client name. A
   two-line header begins the listing which is the default format.
-v

Selects the verbose mode. This option causes `bpplclients` to log additional information for debugging purposes. The information goes into the NetBackup administration daily debug log. This option is meaningful only when you enable the debug log function (that is, when the following directory is defined):

UNIX systems: /usr/openv/netbackup/logs/admin

Windows systems: install_path\NetBackup\logs\admin

This option must precede the `-add`, `-delete`, or `-modify` option on the command line.

EXAMPLES

Example 1 - While the master server runs, list the clients that are known to the master server.

```bash
# bpplclients

Hardware   OS       Client
---------- -----------  ---------
Windows-x64 Windows2008 marmot
HP9000-800  HP-UX 11.23 squash
```

This command can also be entered on a client named `hatt`, with the same results.

Example 2 - List the defined clients for the policy `onepolicy`:

```bash
# bpplclients onepolicy

Hardware   OS       Client
---------- -----------  ---------
Solaris     Solaris10 jeckle
RS6000      AIX5       streaky
HP9000-800  HP-UX 11.31 shark
```

Example 3 - Add the client `marmot` to the policy `twopolicy` on the master servers `serv1` and `serv2`. The hardware type for `lynx` is `HP9000`; the operating system is `HP-UX 11.23`. The default priority is used.

```bash
# bpplclients twopolicy -M serv1,serv2 -add lynx HP9000 HP-UX 11.23
```

Example 4 - Delete the clients `marmot` and `vole` from the policy `twopolicy` on the master servers `serv1` and `serv2`.

```bash
# bpplclients twopolicy -M serv1,serv2 -delete marmot vole
```
Example 5 - While the master server hat runs, list client information for policy BackTrack on master server beaver:

```
# bpplclients BackTrack -M beaver
Hardware  OS     Client
----------  --------  -------
Solaris    Solaris10 saturn
```

**RETURN VALUES**

An exit status of zero (0) means that the command ran successfully.

Any exit status other than zero (0) means that an error occurred.

If the administrative log function is enabled, the exit status is logged in the administrative daily log under the log directory:

UNIX systems: /usr/openv/netbackup/logs/admin

Windows systems: install_path\NetBackup\logs\admin

It has the following form:

bpplclients: EXIT status = exit status

If an error occurred, a diagnostic precedes this message.

**FILES**

UNIX systems:

/usr/openv/netbackup/logs/admin/*
/usr/openv/NetBackup/db/policy/policy_name/clients

Windows systems:

install_path\netbackup\logs\admin/*
install_path\NetBackup\db\policy\policy_name\clients

**SEE ALSO**

See bpplinfo on page 297.
bppldelete

bppldelete – delete policies from the NetBackup database

SYNOPSIS

bppldelete  policyname  [-verbose]   [-M master_server,...]  [-generation generation]  [-reason "string"]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

bppldelete deletes policies from the NetBackup database.

Any authorized user can initiate this command.

For more about NetBackup authorization, see the NetBackup Security and Encryption Guide.

Note:

It is not recommended that users modify or delete automanaged policies.

If the user modifies the policy, they must make sure that the policy continues to meet the service level objective as defined by the protection plan.

If the user deletes the policy, they must make sure that the asset is added to another protection plan that meets the service level objective.

OPTIONS

-g generation generation

Ensures that the command acts on a specific generation or version of a policy. The generation value increments each time a policy is saved. Use bpplinfo or bppllist to list the current generation value. If no generation is indicated, the command acts on the current version.
-M master_server,

    Deletes the policy information for a specific master server(s). For example, to delete policy MWF_PM from master server Saturn, enter the following:

    bppldelete MWF_PM -M Saturn

policyname

    Specifies the policy to remove from the NetBackup database.

-reason "string"

    Indicates the reason why you choose this command action. The reason text string that you enter is captured and appears in the audit report. Enclose this string with double quotes ("..."). The string must not exceed 512 characters. It cannot begin with a dash character (-) nor contain a single quotation mark (').

-verbose

    Selects verbose mode for logging.
bpplinclude

bpplinclude – maintain list of files automatically backed up by NetBackup policy

SYNOPSIS

bpplinclude policy_name [-v] [-M master_server,...] -L | -l [-generation generation] [-exclude_volumes]

bpplinclude policy_name [-v] [-M master_server,...] [-generation generation] -add pathname or directive ... | -add -f filename | -addtoquery query_string... | -addtoquery -f filename | -delete pathname or directive ... | -delete -f filename | -deletefromquery query_string... | -deletefromquery -f filename | -modify old_pathname new_pathname ... [-reason "string"] [-exclude_volumes]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

bpplinclude maintains the policy file list for a NetBackup policy. The policy file list is the list of files that are backed up when NetBackup runs an automatic backup for the policy. The policy file list does not apply to user backups or archives since users select the files when they start those operations.

bpplinclude performs one of the following operations:

- Adds the pathnames to the policy file list
- Deletes the pathnames from the policy file list
- Modifies the pathnames in the policy file list
- Displays the policy file list for a policy
- Excludes specified volumes from a policy. This option is only applicable for the NAS-Data-Protection policy type.

For most policies, the -add, -delete, and -modify options include a list of pathnames. The list of pathnames must be the final part of the bpplinclude command line. The pathname must be the entire path from the root of the file system to the desired location.
For the pathname syntax for your client type, see the NetBackup Administrator's Guide, Volume I.

The last part of the path can be a file name, a directory name, or a wildcard specification. You can enclose pathnames in quotes. Use enclosing quotes if the pathname contains special characters or a wildcard specification.

Filepath rules do not verify the existence of the input directories or files. NetBackup backs up only the files it finds and does not require that all entries in the list be present on every client.

For most database agents, the input entries are scripts or a directive. See the NetBackup guide that comes with the database agent product for additional information. Also see the \-add pathname\ option.

The added entries to the policy file list can be directives, rather than pathnames for the following: certain policy attributes (such as Allow multiple data streams) and add-on products (such as NetBackup for NDMP).

See the NetBackup Administrator’s Guide, Volume I or the NetBackup guide for the extension product.

The options \-l\ and \-L\ produce nearly identical displays of the policy file list.

bpplinclude sends its error messages to stderr. bpplinclude sends a log of its activities to the NetBackup admin log file for the current day.

Authorized users can initiate this command.

For more about NetBackup authorization, see the NetBackup Security and Encryption Guide.

---

Note:

It is not recommended that users modify or delete automanaged policies.

If the user modifies the policy, they must make sure that the policy continues to meet the service level objective as defined by the protection plan.

If the user deletes the policy, they must make sure that the asset is added to another protection plan that meets the service level objective.

---

OPTIONS

- \-add pathname \ ...

Adds the specified \pathname\ to the policy file list. The \pathname\ can be a directory, file name, script, or directive.
A pathname must be enclosed in quotes ("" ) if it contains special characters, such as blank (" " ), or a wildcard specification. Use a blank to separate two pathnames, not a comma. `bpplinclude` interprets a comma as part of the pathname; it concatenates two or more comma-delimited pathnames into a single pathname with embedded commas. The command does not verify the syntax or the existence of the pathnames.

For MS-SQL-Server Intelligent Policies, this option adds a SQL Server object to the backup selections. Valid values are `WHOLE_DATABASE`, the name of a filegroup, or the name of a file. `WHOLE_DATABASE` backs up all databases in the SQL Server instance. When you add a filegroup or file, that object is included for all databases in the policy that contain a filegroup or file with that name. Use the `bpplclients` command to configure the list of instances and databases that is configured for the policy.

For NAS-Data-Protection policy, you can specify backup selection in the following format:

```
nfs:<array>StorageArrayIPAddress</array><nas_head>Filer_or_NAS_Server</nas_head><nas_share./volume_name</nas_share>"
```

Example:

NetApp:

```
nfs:<array>10.0.0.1</array><nas_head>ExampleNAS</nas_head><nas_share>/nas_share_01</nas_share>
```

Nutanix AFS:

```
nfs:<array>Example.company.com</array><nas_head>EXAMPLE_AFS</nas_head><nas_share>/afs_share_01</nas_share>
```

- `add -f filename`
  Adds all files that are listed in `filename` to the policy file list.

- `addtoquery query_string...`
  Adds the specified query string to the end of the policy query rules, or creates a query if none exists. Quotes ("" ) must be escaped with a backslash (\). For more details and examples, refer to the `NetBackup for VMware Guide`.

- `addtoquery -f filename`
  Add an entry to the query rules from the specified file, or creates a query if none exists. In the file, quotes ("" ) do not need to be escaped.

  For more details and examples, refer to the `NetBackup for VMware Guide`. 

-delete pathname ...
   Deletes the specified pathnames, file name, script, or directive from the policy
   file list. Refer to -add for the pathname-list syntax. If you delete an item from
   the policy file list, you still can recover any backups or archives for that item.
   This option must be the final entry on the command line.

-delete -f filename
   Deletes the specified file in filename from the policy file list.

-deletefromquery query_string...
   Deletes the specified query string from the policy query rules.
   For more details and examples, refer to the NetBackup for VMware Guide.

-deletefromquery -f filename
   Deletes the file entries from the query rules.
   For more details and examples, refer to the NetBackup for VMware Guide.

-exclude_volumes
   Excludes specified volumes from being backed up when the policy is executed.
   Currently, applicable only for the NAS-Data-Protection policy.

-generation generation
   Ensures that the command acts on a specific generation or version of a policy.
   The generation value increments each time a policy is saved. Use bpplinfo
   or bppplist to list the current generation value. If no generation is indicated,
   the command acts on the current version.

-L
   Displays the contents of the policy file list in long format.

-l
   Displays the contents of the policy file list in compact format.

Note: The -l and -L displays are similar.

-modify {old_path_name new_path_name}
   Modifies an entry in the policy file list. The values are a list of pathname pairs
   {old_path_name new_path_name}. For each pathname pair, new_name_path replaces
   old_name_path in the policy file list. If no list entry matches
   old_path_name, then new_path_name is not entered into the policy file list.
   Refer to the -add option for the pathname syntax. Delimit the list entries with
   spaces, both within a pathname pair and between pathname pairs. This option
   must be the final entry on the command line.
-M master_server,...
   A list of master servers. This list is a comma-separated list of host names. If
   this option is present, the command is run on each of the master servers in
   this list. The master servers must allow access by the system that issues the
   command. If an error occurs for any master server, the process stops at that
   point in the list. The default is the master server for the system where the
   command is entered.

policy_name
      Specifies the policy for which the policy file list is to be set.

-reason "string"
      Indicates the reason why you choose this command action. The reason text
      string that you enter is captured and appears in the audit report. Enclose this
      string with double quotes ("..."). The string must not exceed 512 characters. It
      cannot begin with a dash character (-) nor contain a single quotation mark (').

-v
      Selects the verbose mode for logging. This option is meaningful only when you
      run with the debug log function on (that is, when the following directory is
      defined):

      UNIX systems:

      /usr/openv/netbackup/logs/admin

      Windows systems:

      install_path\NetBackup\logs\admin

EXAMPLES

Example 1 - While the backup runs on another master server kiwi, display the policy
file list for policy oprdoc_policy on the master server plim:

# bpplinclude oprdoc_policy -L -M plim

Include: /oprdoc (UNIX systems)
Include: c:\oprdoc (Windows systems)

Example 2 - Add and delete the pathnames that include one wildcard entry to
illustrate bpplinclude interpretation of wildcards:

UNIX systems:

# bpplinclude mkbpolicy -add /yap /y*
# bpplinclude mkbpolicy -L
Include: yap
Include: /y*
# bpplinclude mkbpolicy -delete /y*
# bpplinclude mkbpolicy -L
        Include: /yap

Windows systems:

# bpplinclude mkbpolicy -add C:\yap C:\y*
# bpplinclude mkbpolicy -L
        Include: C:\yap
        Include: C:\y*/y*
# bpplinclude mkbpolicy -delete C:\y*
# bpplinclude mkbpolicy -L
        Include: C:\yap

Note: bpplinclude does not interpret the wildcard entry y* for -delete as meaning that both yap and y* should be deleted. Only y* is deleted from the include list for mkbpolicy. The interpretation of the wildcard occurs during the actual backup when NetBackup selects files to back up.

Example 3 - Add two entries to the policy file list for a policy, then modify them:

UNIX systems:

# bpplinclude mkbpolicy -add "/ima file" "/ura file"
# bpplinclude mkbpolicy -L
        Include: /ima file
        Include: /ura file
bpplinclude mkbpolicy -modify "/ima file" "/ima file 2" "/ura file"
        "/ura file 2"
bpplinclude mkbpolicy -L
        Include: /ima file 2
        Include: /ura file 2

Windows systems:

# bpplinclude mkbpolicy -add "C:\ima file" "C:\ura file"
# bpplinclude mkbpolicy -L
        Include: C:\ima file
        Include: C:\ura file
# bpplinclude mkbpolicy -modify "C:\ima file" "C:\ima file 2"
        "C:\ura file" "C:\ura file 2"
# bpplinclude mkbpolicy -L
Example 4 - Add a raw partition to the policy file list for the policy rc (UNIX clients).
The full path name for the device is used (the command is all on one line):

bpplinclude rc -add /devices/sbus@2,0/dma@2,81000/esp@2,80000/sd@6,0:h,raw

For more about UNIX raw partitions, see the NetBackup Administrator’s Guide, Volume I.

Example 5 - Display the policy file list for the policy mkb_policy:

# bpplinclude mkb_policy -l

UNIX systems:

INCLUDE /etc/services
    INCLUDE /etc/aliases
    INCLUDE /usr/bin

Windows systems:

INCLUDE C:\services
    INCLUDE C:\aliases
    INCLUDE C:\Programs

Example 6 - Add vm17 to the list of values in the query rules of policy1.

# bpplinclude policy1 -addtoquery ,"vm17"

Example 7 - Delete a query from a policy.

# bpplinclude policy1 -deletefromquery -f qfile1

Example 8 - Add a SQL Server filegroup to the policy file list.

# bpplinclude sql_policy -add FG1

FILES

UNIX systems:

/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/db/policy/policy_name/includes

Windows systems:
SEE ALSO

See `bpplclients` on page 276.
See `bpplinfo` on page 297.
See `bpschedule` on page 401.
See `bppldelete` on page 287.
See `bppllist` on page 324.
bpplinfo – manage or display policy attributes for NetBackup

SYNOPSIS

```
bpplinfo policy_name -L | -l | -U [-v] [-M master_server,...]

bpplinfo policy_name -set | -modify [-v] [-M master_server,...]
[-reason "string"] [-generation generation] [-active | -inactive]
[-pt policy_type] [-job_subtype sub_type] [-ut] [-ef effective_time]
[-residence label] [-pool label] [-priority number] [-rfile flag]
[-blkincr flag] [-multiple_streams flag] [-keyword "keyword phrase"]
[-encrypt flag] [-collect_tir_info value] [-compress flag] [-crossmp flag]
[-follownfs flag] [-policyjobs max_jobs] [-chkpt flag]
[-chkpt_intrvl interval] [-collect_bmr_info flag]
[-application_consistent flag] [-sg server_group | *ANY* | *NONE*]
[-data_class_class | *NULL*] [-res_is_stl 0 | 1]
[-granular_restore_info 0 | 1] [-ignore_client_direct 0 | 1]
[-use_accelerator 0 | 1] [-application_discovery 0 | 1]
[-discovery_lifetime seconds] [-ASC_apps_attr agent:;truncatelogs=1[0],...]
[-optimized_backup 0 | 1]
[-ExchangeSource source [-Exchange2010Server server,...]]
[-client_list_type type] [-selection_list_type type]
[-application_defined value,...] [-dynamic_multi_streaming flag 0 | 1 [-max_streams_per_volume [1-20]] [-max_files_in_batch [1-2000]]]
[-use_backup_host_pool flag 0 | 1 [-backup_host_pool "backup host pool name"] [-use_vendor_change_tracking flag 0 | 1]
[-ora_bkup_arch_file_name_fmt "[file_name_fmt]"
[-ora_bkup_ctrl_file_name_fmt "[file_name_fmt]"
[-ora_bkup_data_file_name_fmt "[file_name_fmt]"
[-ora_bkup_fra_file_name_fmt "[file_name_fmt]"
[-ora_bkup_set_id "[set_id]" [-ora_bkup_data_file_args "[args]"
[-ora_bkup_arch_log_args "[args]"
[-snapshot_method_args keyword=value,keyword=value,...] [-dynamic_multi_streaming flag 0 | 1 [-max_streams_per_volume number] [-max_files_in_batch number]]
[-use_backup_host_pool flag 0 | 1 [-backup_host_pool "name"]
[-use_vendor_change_tracking flag 0 | 1]

bpplinfo policy_name -set | -modify -deployment_package item
-deployment_media_server media_server [-deployment_limit_jobs max_concurrent_jobs] [-deployment_master_server master_server]
```
bpplinfo initializes, modifies, or displays the attribute values for a NetBackup policy. Authorized users can initiate this command. For more about NetBackup authorization, see the NetBackup Security and Encryption Guide.

bpplinfo consists of two forms. The options that you use with bpplinfo depend on the form of bpplinfo being used.

The first form of bpplinfo displays policy information. The -L, -l, and -U options lists the policy information in different ways.

The second form of bpplinfo initializes or modifies the policy attributes.

- **-set** initializes or reinitializes policy attributes to their default values, except for those attributes that are specified on the current command line.

- **-modify** modifies the policy attributes specified on the current command line. The rest of the policy attributes not on the current command line remain unchanged.
**Warning:** To modify policy attributes, use the `-modify` option. This option affects only the attributes that you specify on the command line. Be careful how you use the `-set` option, which resets all attributes to their default values, except those that are specified on the command line. If you use `-set` to change one or two attributes, you may inadvertently return all the unspecified attributes to their default values.

**Note:** It is not recommended that users modify or delete automanaged policies.

If the user modifies the policy, they must make sure that the policy continues to meet the service level objective as defined by the protection plan.

If the user deletes the policy, they must make sure that the asset is added to another protection plan that meets the service level objective.

**OPTIONS**

`policy_name -L | -l | -U`

Lists the information for this policy. This option is required.

- `-L` specifies a long list type and produces a listing with one policy attribute per line, in the format `policy_attribute: value`. The value can be expressed both in numeric and name form. Fields in the list include:
  - Policy Type
  - Policy Generation (version)
  - Active
  - Follow NFS Mounts (applies only to NetBackup Enterprise Server)
  - Cross Mount Points
  - Client Compress
  - Collect TIR Info
  - Policy Priority
  - Ext Security Info
  - File Restore Raw
  - Client Encrypt
  - Max Jobs/Policy
  - Mult. Data Stream
  - Snapshot Method
  - Snapshot Method Arguments

NetBackup Commands

bpplinfo
Perform Offhost Backup
Backup Copy
Use Data Mover
Data Mover Type
Use Alternate Client
Alternate Client Name
Use Virtual Machine
Hyper-V Server
Enable Instant Recovery
Disaster Recovery
Collect BMR Info
Max Frag Size
Checkpoint Restart
Residence
Volume Pool
Share Group
Data Classification
Residence is Storage Lifecycle Policy
Granular Restore
Generation
Backup Host Pool Name
Use Vendor Change Tracking
Dynamic Multi-Stream
Max Streams/Volume
Max Files in batch

-l specifies a short list type and produces a terse listing. This option is useful for scripts or the programs that rework the listing contents into a customized report format. A short listing contains the following information for the specified policy:

Line 1: "INFO", client_type, follow_nfs_mounts, client_compress, priority, proxy_client, client_encrypt, disaster_recovery, max_jobs_per_policy, cross_mount_points, max_frag_size, active, collect_tir_info, block_incr,
ext_sec_info, i_f_r_f_r, streaming, frozen_image, backup_copy, effective_date,
policy ID, number_of_copies, checkpoint, chkpt_interval, policy_info-unused1,
pfi_enabled, offhost_backup, use_alt_client, use_data_mover,
data_mover_type, collect_bmr_info, res_is_ss, granular_restore_info,
job_subtype

Line 2: "KEY", keyword
Line 3: "BCMD", backup_command
Line 4: "RCMD", restore_command
Line 5: "RES", residence
Line 6: "POOL", pool
Line 7: "FOE", this field is not used

-U specifies a user list type and produces a listing with one policy attribute per line, in the format policy_attribute: value. This listing is similar to the -L listing, but contains fewer fields.

-v
Selects the verbose mode. This option causes bpplinfo to log additional information for debugging purposes. The information goes into the NetBackup administration daily debug log. This option is meaningful only when NetBackup enables the debug log function (that is, when the following directory is defined):

UNIX systems: /usr/openv/netbackup/logs/admin

Windows systems: install_path\NetBackup\logs\admin

-M master_server,...
A list of alternative master servers. This list is a comma-delimited list of host names. If this option is present, each master server in the list runs the bpplinfo command. Each master server in the list must allow access by the system that issues the bpplinfo command. If an error occurs for any master server, the process terminates at that point.

For the display form of bpplinfo, the report is the composite of the returned information from all the master servers in this list. bpplinfo queries each of these master servers. The master server returns information from its policy catalog.

For the policy-definition form of bpplinfo, the policy is created or modified on each master server in the list.

The default is the master server for the system running bpplinfo.
The second form of `bpplinfo` initializes attribute values for a policy or modifies the attribute values for a policy. The following options apply to this form:

**Note:** Not all options apply to every policy type. For example, if the policy type is MS-Windows, `bpplinfo` accepts the options `-compress` and `-crossmp`. When `bpplinfo` completes, it returns a zero status. However, NetBackup handles the policy with the MS-Windows policy type as though the options were not set.

- **-active | -inactive**
  Set the policy to active or inactive. If the policy is active, NetBackup runs all its automatic schedules and permits user-directed backups and archives to be used. A policy must be active for an automatic backup to occur (the default).
  
  If the policy is inactive, NetBackup does not run any automatic schedules or permit user-directed schedules to be used. This option is useful to inactivate a policy temporarily to prevent schedules from being used.

- **-application_consistent flag**
  Specifies that the virtual machine is quiesced before a persisted hardware snapshot is taken (flag=1). Otherwise, the hardware snapshot does not quiesce the virtual machine (flag=0) (default condition).

- **-application_defined value,**...
  This option only applies to a SQL Server Intelligent Policy. The `client_list_type` must be set to 1, 2, or 3. The values that are defined for this option apply to database operations, unless the value is preceded with `TL_`.
  
  An exception is `VDI_TIMEOUT`. The value is applied to both database backups and transaction log backups.
  
  This option can use one or more of the following values:
  
  - **STRIPEs=value** or **TL_STRIPEs=value** - Divides the backup operation into multiple concurrent streams. A stream corresponds to a job in the activity monitor. For example, if STRIPEs=3 is set, each database is backed up using three jobs. The value range is 1-32. The default value is 1.
  
  - **BUFFERS=value** or **TL_BUFFERS=value** - The buffer size that SQL Server uses for reading and writing backup images. The value range is 1-32. The default value is 2.
  
  - **MAX_TRANSFERSIZE=value** or **TL_MAX_TRANSFERSIZE=value** - Specifies the maximum size of an I/O transfer (buffer read-write) between SQL Server and the NetBackup SQL Agent. Calculated as 64 KB *
2^MAX_TRANSFER_SIZE. The range value is 0-6 (64 KB-4 MB). The default value is 6 (4 MB).

- **BLOCK_SIZE=value or TL_BLOCK_SIZE=value** - Sets the incremental size that SQL Server uses for reading and writing backup images and can be set for each backup operation. All data transfers are a multiple of this value up to the MAX_TRANSFER_SIZE. Calculated as 512 bytes * 2^BLOCK_SIZE. The range value is 0-7 (512 B-64 KB). The default value is 7 (64 KB).

- **BATCH_SIZE=value or TL_BATCH_SIZE=value** - The number of backup operations to start simultaneously. The range value is 1-32. The default value is 1.

- **CHECKSUM=0 | 1 | 2 or TL_CHECKSUM=0 | 1 | 2** - Controls if SQL Server performs backup checksums. The default is 0.
  0 = No checksum is performed.
  1 = Checksums are performed and the backup continues even if SQL detects an error.
  2 = Checksums are performed, but the backup stops if any errors are detected.

- **CONVERT_BACKUP=0 | 1 or TL_CONVERT_BACKUP=0 | 1** - Converts a differential or a transaction log backup to a full backup if no full backup exists for the database.
  For more information, see the NetBackup for SQL Server Administrator’s Guide.

- **COMPRESSION=0 | 1 or TL_COMPRESSION=0 | 1** - Controls if SQL Server backup compression is used. If you enable SQL Server compression, do not enable NetBackup compression. The default is 0.
  0 = Compression is not enabled.
  1 = Compression is enabled.

- **SKIP_OFFLINE=0 | 1 or TL_SKIP_OFFLINE=0 | 1** - Controls how the agent deals with the databases with a status that prevents NetBackup from successfully backing up the database. These statuses include offline, restoring, recovering, and emergency mode, etc. When this option is enabled, the agent skips the backup of that database. NetBackup does not log an error for these databases. The job details indicate if a database is skipped. The default is 0.
  0 = Offline databases are not skipped and a failed job are generated for each offline database.
  1 = Offline databases are skipped and no failures are generated for skipped databases.
- **COPYONLY=0 | 1** - This option allows SQL Server to create an out-of-band backup so that it does not interfere with the normal backup sequence. The default value is unchecked except for full database persistent frozen image backups. The default is 0.
  0 = Backup is not copy-only.
  1 = Backup is performed as copy-only.

- **SKIP_READONLY_FGS=0 | 1** - This option can exclude any filegroups that are read-only from the backup. The resulting backup is a partial image because the image does not contain all filegroups. The default is 0.
  0 = Read-only filegroups are not skipped.
  1 = Read-only filegroups are skipped.

- **TL_*** - All values that have a TL_* correspond to transaction log backups (for example, when the transaction log schedule is run).

- **TL_TRUNCATE_LOGS=0 | 1** - Determines if the transaction log is truncated at the end of the backup. The default is 1.
  0 = Logs are not truncated.
  1 = Logs are truncated.

- **PREFERRED_REPLICA** - Determines how to perform instance or availability group backups.
  0 = Performs the backup on the specified instance.
  1 = Backups always occur on the primary replica.
  2 = Honors your SQL Server backup preferences and protects the preferred replica.
  3 = Skips any availability databases on the instance.

- **VDI_TIMEOUT** - The timeout interval for the SQL Server Virtual Device Interface. The selected interval is applied to both database backups and transaction log backups. The range value is 300–2147483647. The default value is 300.

- **-application_discovery 0 | 1**
  Enables the VMware policy to automatically select virtual machines for backup when you create a policy for vCloud Director.

- **-ASC_apps_attr agent::*;truncatelogs=1|0*,...**
  Enables the file-level recovery of database data for Exchange, SQL Server, or SharePoint. The agent value can be exchange, mssql, or sharepoint.

  You can enable (;truncatelogs=1) and disable (;truncatelogs=0) truncate logs for Exchange and SQL Server.

  The following are several examples that show how to use this option:
To enable Exchange file recovery: `-ASC_apps_attr exchange:

To enable Exchange, SQL Server, and SharePoint file recovery: `-ASC_apps_attr exchange:,mssql:,sharepoint:

To enable SQL Server recovery and truncate logs: `-ASC_apps_attr mssql:;truncatelogs=1

To truncate Exchange logs and not truncate SQL Server logs (note the final colon): `-ASC_apps_attr exchange:;truncatelogs=1,mssql:

To enable both Exchange and SQL Server with truncate logs: `-ASC_apps_attr exchange:;truncatelogs=1,mssql:;truncatelogs=1

`-blkincr` flag

**Note:** This option applies only if you are running NetBackup Enterprise Server and also have Veritas Oracle Edition, which supports block-level incrementally.

0 (disabled) or 1 (enabled). Perform block-level-incremental backups for clients in this policy.

If 1, perform block-level-incremental backups.

If 0, disable block-level-incremental backups.

`-client_list_type` type

This option is used for MS-SQL-Server and Oracle policies.

If 0, the type is **HOST**. This policy is the legacy MS-SQL-Server or Oracle policy. The valid schedule types are **FULL** and **USER**.

The following types apply to a SQL Server or Oracle Intelligent Policy. The valid schedules types are **FULL**, **INCR**, and **TLOG**.

If 1, the type is **INSTANCE** and you can add registered instances or databases in the instances to the policy.

If 2, the type is **INSTANCE_GROUP** and you can add registered instance groups to the policy.

The following type applies only to SQL Server Intelligent Policies.

If 3, the type is **AVAILABILITY_GROUP** and you can add availability groups with registered replicas to the policy.

The following type applies only to Oracle Intelligent Policies.

If 4, the type is **RAC_DATABASE** and the client type for backup is Oracle RAC.
-chkpt [1|0]
  Enables and disables the checkpoint restart for the policy. If 1, the command enables the checkpoint restart. If 0, the command disables the checkpoint restart. The default is 0.

-chkpt_intrvl interval
  Enables and disables the checkpoint interval for the policy. The variable interval is the checkpoint interval in minutes. The default interval is 15 minutes. The range for this interval is between 5 minutes and 180 minutes. If the checkpoint restart is not enabled, then this parameter has no effect.

-collect_tir_info value
  Collect true image recovery (TIR) information. True-image recovery allows NetBackup to restore a directory to exactly what it was at the time of any scheduled full or incremental backup. The files that are deleted before the selected backup time are not restored. After this attribute is enabled, NetBackup starts to collect additional information. It begins with the next full or incremental backup for the policy.

  If 0, NetBackup does not keep track of true-image-recovery information.

  If 1, NetBackup collects TIR information.

  If 2, NetBackup collects TIR information and tracks client files.

-collect_bmr_info flag
  Collect Bare Metal Restore information.

  If flag is 0, do not collect Bare Metal Restore information.

  If flag is 1, collect Bare Metal Restore information.

  If -collect_bmr_info is set to 1 and Bare Metal Restore is not licensed or the policy type is not Standard or MS-Windows, bpplinfo fails.

  If -collect_bmr_info is set to 1 but the policy does not collect true image restore information with move detection, Bare Metal Restore ignores the following: incremental backups and restore files from the last full backup.

-compress flag
  Specifies whether to compress files or not. If set to 1 (enabled), the client software compresses the selected files onto the media. Compression reduces the size of the backup files and the storage media required, but may increase the total backup time. If set to 0 (disabled), the files are not compressed onto the media (the default condition). Note compression is independent of the VxFS compression.

  This option has no effect on the hardware compression that may be available on the storage unit.
-crossmp flag
    0 (disabled) or 1 (enabled). Specifies whether to cross mount points during backups or not.

    If 1, NetBackup backs up or archives all files and directories in the selected path, regardless of the file system on which they reside.

    If 0, NetBackup backs up or archives only those files and directories on the same file system as the selected file path (the default).

    This attribute can affect the Follow NFS policy attribute, which applies only to NetBackup Enterprise Server.

    For more about the cross mount point attribute, see the NetBackup Administrator’s Guide, Volume I.

-data_class class
    Specifies the data classification (for example, gold or platinum).

-deployment_cert_source (cert_store | file)
    Use this option to indicate the source of the certificate for Windows hosts. Use -deployment_cert_source cert_store to indicate a Windows certificate store. Use -deployment_cert_source file to indicate that the certificate is in a file. If you use the -win_eca_cert_store option, you must specify -deployment_cert_source cert_store. In all other cases, use -deployment_cert_source file.

-deployment_components javagui_jre=(include | exclude | match)
    Use this option to specify if the Java GUI and JRE should be present on the target systems after the deployment job runs.

    A value of include indicates that you want these components to be installed or upgraded on the target systems.

    A value of exclude indicates that you do not want the components on the target systems. Any preexisting Java GUI and JRE components are removed.

    A value of match indicates that you want to preserve the current state of the Java GUI and JRE components. The components are upgraded if they are present on the pre-upgraded system. The components are not installed if they are not present on the pre-upgraded system.

-deployment_limit_jobs max_concurrent_jobs
    The maximum number of jobs that are allowed per policy. You can only use this option with the Deployment policy type.
-**deployment_master_server** *master_server*

If the client has multiple master servers, the *master_name* value is the master server that contains the repository. You can only use this option with the Deployment policy type.

-**deployment_media_server** *media_server*

The name of the media server that communicates with and deploys packages to the policy’s clients. Packages are cached on the media server to minimize communication and improve performance. The package repository resides on the master server. You can only use this option with the Deployment policy type.

-**deployment_package** *item*

The name of the package you want installed. You can only use this option with the Deployment policy type.

-**deployment_unix_stage_loc** *path*

Used to specify an alternate staging location for UNIX or Linux clients. Currently not used.

-**deployment_use_existing_certs** 0 | 1

Use this option to specify if you want the installation to use existing certificates if they are available. Use 1 to enable this option and 0 to disable this option.

-**deployment_win_stage_loc** *path*

Used to specify an alternate staging location for Windows clients. Currently not used.

-**disaster** 0 | 1

Collect required information for Intelligent Disaster Recovery. This attribute applies only when you back up Windows clients.

0 = Do not allow disaster recovery (Default)

1 = Allow disaster recovery

-**discovery_lifetime** *seconds*

Specifies the time in seconds to reuse the VM selection query results.

-**dynamic_multi_streaming** flag 0 | 1

Enable dynamic multistreaming for NAS-Data-Protection policy type. A value of 1 allows dynamic multistreaming and a value of 0 does not allow dynamic multistreaming.

- **-max_streams_per_volume** *number*: Specify the maximum number of streams per volume between 1 to 20. The default value is two.
-max_files_in_batch number: Specify the maximum number of files in a batch between 1 to 2000. The default value is 500.

-ef effective time
  This time specifies the time the policy is active.

-encrypt flag
  Specifies whether files should be encrypted or not. If flag is set to 1, encryption is enabled.

-Exchange2010Server server,...
  For an Exchange DAG, a list of one or more servers in the DAG that you select as preferred backup sources. The preferred server list is required if
  -ExchangeSource is 1, unless the database only has an active copy. The list is ignored if -ExchangeSource is 2 and is optional if -ExchangeSource is 0.

-ExchangeSource source
  Indicates what database backup source you want to use for an Exchange Database Availability Group (DAG). The default is 0. The following are the possible values for this option:
  - 0 - Backs up the passive copy of a database or the passive server. For a DAG, you can also configure a preferred server list. NetBackup backs up the passive copy on a server in the preferred server list. If the passive copy is not available, NetBackup backs up the active copy.
  - 1 - Backs up the passive copy of a database or passive server. For a DAG, you must also configure a preferred server list. NetBackup backs up the passive copy on a server in the preferred server list.
  - 2 - Backs up the active copy of a database or active node. For Exchange 2010 and later, the preferred server list is ignored.
  - 3 - Disables the database backup source.

-follownfs flag

Note: This option applies only to NetBackup Enterprise Server.

0 (disabled) or 1 (enabled). Specifies whether to follow NFS mount points or not. For MS-Windows policy types, setting this flag affects the policy attribute Backup network drives instead of the Follow NFS attribute.

If 1, NetBackup backs up or archives any NFS-mounted files encountered.

If 0, NetBackup does not back up or archive any NFS-mounted files encountered (the default).
The behavior of this attribute varies depending on the setting of the Cross Mount Points attribute.

For more about the Cross Mount Points attribute, see the NetBackup Administrator’s Guide, Volume I.

-granular_restore_info flag

Enables or disabled the granular recovery attribute, which restores the individual objects that reside within a database backup image. This attribute is available for MS-Exchange_Server, MS-SharePoint, and MS-Windows (for Active Directory).

If 1, display granular restore information.

If 0, do not display granular restore information.

For more information about granular restores, see the NetBackup for Exchange Administrator’s Guide, Volume I.

-ignore_client_direct 0 | 1

Enables (0) or disables (1) client-side deduplication.

-job_subtype DUPLICATE | LIVEUPDATE, INDEXING

Allows the generic policies for the Duplicate feature or the LiveUpdate feature to be displayed. By default, the policies for these two features are not displayed.

-keyword "keyword phrase"

The value is associated with all backups created by using this policy. The keyword phrase can be used to link related policies. It can also be used during restores to search only for the backups that have the keyword phrase association.

-M master_server,...

Same as explained earlier.

-multiple_streams flag

0 (disabled) or 1 (enabled). Allow Multiple data streams.

If 1, allow multiple data streams.

If 0, disable multiple data streams.

-optimized_backup 0 | 1

Enables the backup of deduplicated data that some Microsoft Windows operating system versions provide. If a client has a deduplicated file system configured, NetBackup backs up the deduplicated data. If the client is not set up for deduplication or does not support it, then a normal file backup occurs.
-ora_bkup_arch_file_name_fmt "[file_name_fmt]"
  Specifies the Oracle RMAN backup piece names for the archived redo logs. Ensure that the format ends with _$t to indicate a timestamp. NetBackup uses this timestamp as part of its search criteria for catalog images. Without this timestamp, performance might degrade as the NetBackup catalog grows.

  Specify an empty string (""") for the file_name_fmt to cause the default format to be used.

-ora_bkup_ctrl_file_name_fmt "[file_name_fmt]"
  Specifies the Oracle RMAN backup piece names for the control files. Ensure that the format ends with _$t to indicate a timestamp. NetBackup uses this timestamp as part of its search criteria for catalog images. Without this timestamp, performance might degrade as the NetBackup catalog grows.

  Specify an empty string (""") for the file_name_fmt to cause the default format to be used.

-ora_bkup_data_file_name_fmt "[file_name_fmt]"
  Specifies the Oracle RMAN backup piece names for the data files. Ensure that the format ends with _$t to indicate a timestamp. NetBackup uses this timestamp as part of its search criteria for catalog images. Without this timestamp, performance might degrade as the NetBackup catalog grows.

  Specify an empty string (""") for the file_name_fmt to cause the default format to be used.

-ora_bkup_fra_file_name_fmt "[file_name_fmt]"
  Specifies the Oracle RMAN backup piece names for the Fast Recovery Area (FRA). Ensure that the format ends with _$t to indicate a timestamp. NetBackup uses this timestamp as part of its search criteria for catalog images. Without this timestamp, performance might degrade as the NetBackup catalog grows.

  Specify an empty string (""") for the file_name_fmt to cause the default format to be used.

-ora_bkup_arch_log_args "[key=value,...]"
  The key=value pairs are used to override the default arguments that are used when backing up Oracle archived redo logs using RMAN. Any key not explicitly specified is reset to the default value. Specify an empty string (""") to reset all keys to the default values. Use a comma (,) to separate key value pairs. Spaces are not permitted. The keys and their values are as follows:

  ■ INCLUDE_ARCH_LOGS - Includes the archived redo logs in the full and the incremental schedule backups. Valid values are 0 and 1, the default is 1.
- **DELETE_ARCH_LOGS_AFTER_COPIES** - Delete the archived redo logs after they are successfully backed up one or more times. You can omit this key or set the key to 0 to not delete the logs after the backup. The default is 0.

- **NUM_STREAMS** - The number of parallel backup streams that can be used in a backup operation. RMAN is instructed to allocate a concurrent channel for each stream. The default value is 1.

- **SPECIFY_MAX_LIMITS** - Must be enabled to modifying these additional keys. Valid values are 0 and 1, the default is 0.

- **NUM_FILES_PER_BACKUP_SET** - Specifies the maximum number of archived redo log files to include in each backup set (FILES_PER_SET). If not specified, the RMAN default is used.

- **SIZE_BACKUP_SET** - Specifies a maximum size for each backup set in kilobytes (MAX_SET_SIZE). If not specified, the RMAN default is used.

- `ora_bkup_data_file_args "[key=value,...]"`
  Specifies the key=value pairs that are used to override the default arguments that are used when backing up Oracle data files using RMAN. Any key not explicitly specified is reset to the default value. Specify an empty string ("") to reset all keys to the default values. Use a comma (,) to separate key value pairs. Spaces are not permitted. The keys and their values are as follows:

- **NUM_STREAMS** - The number of parallel backup streams that can be used in a backup operation. RMAN is instructed to allocate a concurrent channel for each stream. The default value is 1.

- **SKIP_READ_ONLY or FORCE_READ_ONLY** - Enable read-only tablespace options. The SKIP option ignores the read-only tablespace during backup. FORCE means that RMAN backs up all files. Only one of the two may be enabled concurrently. Valid values are 0 and 1, the default is 0.

- **OFFLINE** - Shut down the Oracle database and put it in the mount state before the backup. Valid values are 0 and 1, the default is 0.

- **SKIP_OFFLINE** - Direct the backup operation to not access offline data files. Valid values are 0 and 1, the default is 0.

- **SPECIFY_MAX_LIMITS** - Must be enabled to modifying these additional keys. Valid values are 0 and 1, the default is 0.

- **READ_RATE** - Specifies the maximum number of kilobytes (KB) that RMAN reads each second on this channel (RATE). This parameter sets an upper limit for bytes read so that RMAN does not consume too much disk bandwidth and degrade performance. If not specified, the RMAN default is used.
- **SIZE_BACKUP_PIECE** - Specifies the maximum size, in kilobytes, of each backup piece that is created on this channel (MAXPIECESIZE). If not specified, the RMAN default is used.

- **NUM_OPEN_FILES** – Controls the maximum number of input files that the backup operation can have open at any given time (MAXOPENFILES). If not specified, the RMAN default is used.

- **NUM_FILES_PER_BACKUP_SET** - Specifies the maximum number of input files to include in each backup set (FILESPERSET). If not specified, the RMAN default is used.

- **SIZE_BACKUP_SET** - Specifies a maximum size for each backup set in kilobytes (MAXSETS_SIZE). If not specified, the RMAN default is used.

```
policy_name -set | -modify
```

Initializes or modifies attributes for this policy. This option is required.

- `-set` initializes (or reinitializes) attributes for the policy to their default values, except for those attributes that the options on the current command-line set.

- `-modify` modifies attributes for the policy. Attributes not explicitly set by options on the current command line do not change their values.

```
policyjobs max_jobs
```

The maximum number of concurrent jobs that NetBackup allows for this policy (corresponds to the Limit Jobs per Policy setting in the administration interface). The value of `max_jobs` is always greater than or equal to 0.

For the default or when `-policyjobs` is 0, `bpplinfo` sets `max_jobs` to a value that corresponds to unlimited. The maximum number of jobs is 8 for NetBackup and 999 for NetBackup Enterprise Server.

```
pool label
```

Specifies the volume pool for the policy. The default is NetBackup. The volume pool should be one of the volume pools for the policy storage unit. This attribute is not relevant if a disk storage unit is the residence for the policy. If the policy storage unit is Any_available (Residence: - appears on the `bpplinfo` display), the volume pool for any storage unit can be selected. If "*NULL*" is specified, the volume pool is set to NetBackup. To display the configured volume pools, run the following command:

```
UNIX systems: /usr/openv/volmgr/bin/vmpool -listall
```

```
Windows systems: install_path\Volmgr\bin\vmpool -listall
```
-priority number
The priority of this policy in relation to other policies. Priority is greater than or equal to 0. This value determines the order in which policies are run. The higher the value, the earlier the policy is run. The default is 0, which is the lowest priority.

-pt policy_type
Specify the policy type by entering one of the following character strings (the default is Standard):

BigData
DataStore
DataTools-SQL-BackTrack
DB2
Deployment
Enterprise-Vault
FlashBackup
Hyper-V
Informix-On-BAR
Lotus-Notes
MS-Exchange-Server
MS-SharePoint
MS-SQL-Server
MS-Windows
NAS-Data-Protection
NBU-Catalog
NDMP
Oracle
PureDisk-Export
SAP
Split-Mirror
Standard
Sybase
Vault
VMware

-reason "string"
Indicates the reason why you choose this command action. The reason text string that you enter is captured and appears in the audit report. Enclose this string with double quotes ("..."). The string must not exceed 512 characters. It cannot begin with a dash character (-) nor contain a single quotation mark (').
-res_is_stl 0 | 1

Specify this flag only when the name of the storage unit and the name of the storage lifecycle policy are the same. In all other cases this flag is ignored. The possible values are as follows:

0 - the residence is a non-storage life cycle policy
1 - the residence is a storage lifecycle policy

-residence label

Specifies the label of the storage unit for storing the backups that were created according to this schedule. The default is Any_available, which allows the policy to use any storage unit whose On demand only attribute is set to No. Specify the storage unit if the policy must use a specific storage unit. You must select the desired storage unit if it has the On demand only attribute set to Yes. If ""NULL"" is specified, the residence for the schedule is set (or reset) to Any_available. The policy residence determines the residence for the policy schedules, unless the Override Policy Storage Unit setting on an individual schedule specifies a residence. Run bpstulist to display the set of defined storage units.

-rfile flag

0 (disabled) or 1 (enabled).

If 1, allow Individual File Restore From Raw.
If 0, disable Individual File Restore From Raw.

For a FlashBackup policy, this option is ignored, since the attribute is always enabled.

Note: Advanced Client is available only if you are running NetBackup Enterprise Server and have the separately-priced option.

-selection_list_type type

This option is used for MS-SQL-Server policies. The value you choose determines the type of backup selections or file list items you can add with the bpplinclude command.

If 0, the type is HOST. This type must be used with the legacy MS-SQL-Server policy. The only backup selection that is valid for this type is the path of the backup batch file.

The following types apply only to a SQL Server Intelligent Policy.

If 1, the type is WHOLE_DATABASE. The only backup selection that is valid for this type is WHOLE_DATABASE.
If 3, the type is **DATAFILE**. The only backup selection that is valid for this type is the name of the file.

If 7, the type is **FILEGROUP**. The only backup selection that is valid for this type is the name of the filegroup.

- **sg [server_group | *ANY* | *NONE*]**

  Specifies the server group(s) for the schedule. Do not use this option if the schedule resides on a disk storage unit. If *NONE* is specified, the writing media server owns the media that this policy writes. If *ANY* is specified, EMM chooses the media owner. *ANY* is the default value. Otherwise, the named share group owns the media. Specify a share group for each copy to display the configured share groups. Enter the following command:

  UNIX systems:

  ```
  /usr/openv/netbackup/bin/admincmd/nbsvrgrp -list -summary
  ```

  Windows systems:

  ```
  install_path\NetBackup\bin\admincmd\nbsvrgrp -list -summary
  ```

- **-snapshot_method_args keyword=value,keyword=value,...**

  Specifies the arguments for the snapshot method for a VMware policy. The following are the keywords and their values that you can specify:

  - **disable_quiesce**. The state of virtual machine I/O during the snapshot. The following are the allowed values:
    - 0 virtual machine quiesce is enabled or 1 virtual machine quiesce is disabled.

  **Caution**: Veritas does not recommend that you disable quiesce. In most cases, this option should be enabled.

  **Note**: To use this option, VMware Tools must be installed on the virtual machine.

  **Note**: To use this option with Linux virtual machines, you must also install the SYMCquiesce utility.

  - **drive_selection**. For the virtual machines that have multiple virtual disks, determine the kind of disks on the virtual machine that are included in the backup. This option can reduce the size of the backup, but should be used with care. The following are the allowed values:
include all disks, 1 exclude boot disk, or 2 exclude data disks.

- **enable_vCloud.** Enables backup of the virtual machines that reside in a vCloud environment. Requires the automatic selection of virtual machines. The following are the allowed values:
  0 disabled or 1 enabled.

- **exclude_swap.** Exclude the data in the swapping and paging files from the backup. If the files are restored, they are restored as empty files. The following are the allowed values:
  0 disabled or 1 enabled.

- **file_system_optimization.** Reduces the size of the backup image by excluding any unused or deleted blocks within the file system on the virtual machine. This option supports the following file systems: Windows NTFS, and Linux ext2, ext3, and ext4. The following are the allowed values:
  0 disabled or 1 enabled.

- **ignore_irvm.** Ignore any virtual machine that was restored with Instant Recovery for VMware if the virtual machine is running from a NetBackup NFS datastore. The following are the allowed values:
  0 disabled or 1 enabled.

- **multi_org.** Allow the query rules to select virtual machines from different vCloud Director organizations and back them up to the same storage unit. The following are the allowed values:
  0 disabled or 1 enabled.

- **nameuse.** The type of name by which NetBackup recognizes virtual machines when it selects them for backup. The following are the allowed values:
  0 VM host name, 1 VM display name, 2 VM BIOS UUID, 3 VM DNS name, or 4 VM instance UUID

- **post_events.** The backup related events to send to the vCenter server. To post events to vCenter, NetBackup must perform the backup through a vCenter server. If NetBackup accesses the ESX server directly, the backup information cannot be displayed in vSphere Client. You must set the following permissions in vCenter: Log event, Manage custom attributes, and Set custom attribute. The following are the allowed values:
  0 no events, 1 all events, or 2 error events.

- **rHz.** The wait time (in seconds) before the snapshot is retried. The default is 10 seconds. The following are the allowed values:
  0 to 3600, inclusive.

- **rLim.** The number of times the snapshot is retried. The default is 10. The following are the allowed values:
■ rTO. The timeout period (in minutes) for completion of the snapshot. The default is 0, which means no timeout. The following are the allowed values: 0 to 1440, inclusive.

■ serverlist. A colon-delimited list of virtual machine servers that NetBackup communicates with for this policy. To specify no server list, enter serverlist=.

■ skipnodisk. Do not back up a replicated (passive) VM in a vCenter Site Recovery Manager (SRM) environment if that VM has no vmdk files. NetBackup skips that VM and backs up the corresponding active VM, which has vmdk files. The following are the allowed values: 0 disabled or 1 enabled.

■ snapact. This option specifies the action that NetBackup takes when a snapshot is discovered before NetBackup creates a new snapshot for the virtual machine backup. After it creates a snapshot, NetBackup usually deletes the snapshot when the backup completes. If snapshots are not automatically deleted (whether created by NetBackup or not), the performance of the virtual machine may eventually decline. The following are the allowed values: 0 continue backup, 1 abort if any snapshot(s) exist, 2 remove NetBackup snapshot(s) and continue backup, or 3 abort if NetBackup snapshot(s) exist.

■ trantype. How the snapshot data travels from the VMware datastore to the VMware backup host. The following are the allowed values: san, hotadd, nbd, or nbdssl.
To specify more than one transport method, separate each with a colon. The order of modes indicates priority. For example, the following specification selects two modes and tries nbd first:
trantype=nbd:hotadd

■ Virtual_machine_backup. Allows restore of individual files from the backup. With or without this option, you can restore the entire virtual machine. The following are the allowed values: 1 disabled or 2 enabled

■ vmdk_ca. The name of the VMware custom attribute that specifies the disk or disks to exclude from backups. For example, vmdk_ca=NB_DISK_EXCLUDE_LIST.
Set the value for the attribute on each virtual machine or managed host, as appropriate. The attribute must have comma separated values of device
controllers for the disks to be excluded. For example:

\[ \text{scsi0-0, ide0-0, sata0-0}. \]

- `vmdk_list`. Colon separated values of device controllers for the disks to exclude from VMware backups. For example:

\[ \text{vmdklist=scsi0-0:ide0-0:sata0-0}. \]

- `-unix_eca_cert_path path`
  
  Use this option to specify the path to the certificate file and the certificate file name for UNIX and Linux hosts.

- `-unix_eca_crl_check_level (use_cdp | use_path | disabled)`
  
  Specifies how you want to handle the Certificate Revocation List on UNIX and Linux hosts. Specify `use_cdp` to use the CRL defined in the certificate. Specify `use_path` to specify the path to the CRL. Specify `disabled` to not use a CRL.

- `-unix_eca_crl_path path`
  
  Use this option to specify the path to the external certificate authority file for UNIX and Linux hosts. If you use the `-unix_eca_crl_check_level use_path` option, this option is required.

- `-unix_eca_key_passphrasefile path`
  
  Use this option to provide the path to the passphrase file on UNIX and Linux hosts. This option is not required.

- `-unix_eca_private_key_path path`
  
  Use this option to specify the path to the private key file and the private key file name on UNIX and Linux hosts.

- `-unix_eca_trust_store_path path`
  
  This option lets you specify the path to the trust store and the trust store file name on UNIX and Linux hosts.

- `-use_accelerator 0 | 1`
  
  Specifies that you want to use the NetBackup Accelerator which increases the speed of full backups through change detection techniques on the client.

  If 1, enable NetBackup Accelerator.

  If 0, disable NetBackup Accelerator.

  For more about NetBackup Accelerator, see the *NetBackup Administrator's Guide, Volume I*.

- `-use_backup_host_pool flag 0 | 1`
  
  Specifies if you want NetBackup to use a backup host pool. A backup host pool is a group of master or media servers that is used for backups. A value of 1 enables the use of backup host pool. A value of 0 disables the use of
backup host pool. When -use_backup_host_pool is enabled, use the
-backup_host_pool name option to specify the backup host pool name.

-use_vendor_change_tracking flag 0 | 1
Enable vendor change tracking for incremental backups. Specify 1 to allow
vendor change tracking for incremental backups. A value of 0 does not allow
vendor change tracking for incremental backups.

-ut
If any of the date or the time arguments follow -ut, they are accepted as UNIX
time, instead of the standard time format. The -ut option is used primarily for
Java.

-win_eca_cert_path path
Use this option to specify the path to the certificate file and the certificate file
name for Windows hosts.

-win_eca_cert_store path
Use this option to specify the path to the Windows certificate store. You must
enter the certificate location as
Certificate_Store_Name\Issuer_Distinguished_Name\Subject_Distinguished_Name.

-win_eca_crl_check_level (use_cdp | use_path | disabled)
Specifies how you want to handle the Certificate Revocation List on Windows
hosts. Specify use_cdp to use the CRL defined in the certificate. Specify
use_path to specify the path to the CRL. Specify disabled to not use a CRL.

-win_eca_crl_path path
Use this option to specify the path to the external certificate authority file for
Windows hosts. If you use the -win_eca_crl_check_level use_path option,
this option is required.

-win_eca_key_passphrasefile path
Use this option to provide the path to the passphrase file on Windows hosts.
This option is not required.

-win_eca_private_key_path path
Use this option to specify the path to the private key file and the private key
file name on Windows hosts.

-win_eca_trust_store_path path
This option lets you specify the path to the trust store and the trust store file
name on Windows hosts.
EXAMPLES

**Note:** References to NFS Mounts in the following examples apply only to NetBackup Enterprise Server.

Example 1 - Set the storage unit of the policy `tstpolicy` to `tstunit` and view the results:

```
# bpplinfo tstpolicy -modify -residence tstunit
# bpplinfo tstpolicy -L
```

**Policy Type:** Standard (0)
**Active:** no
**Effective:** no
**Follow NFS Mounts:** no
**Cross Mount Points:** no
**Client Compress:** no
**Collect TIR Info:** no
**Policy Priority:** 0
**Ext Security Info:** no
**File Restore Raw:** no
**Client Encrypt:** no
**Max Jobs/Policy:** 8
**Mult. Data Streams:** 1
**Block Level Incremental:** no
**Perform Snapshot Backup:** no
**Backup Copy:** 0
**Date Mover Type:** 2
**Use Alternate Client:** no
**Alternate Client Name:** (none)
**Enable Instant Recovery:** no
**Disaster Recovery:** 0
**Collect BMR Info:** no
**Max Frag Size:** 0 MB (1048576 MB)
**Checkpoint Restart:** no
**Residence:** tstunit
**Volume Pool:** NetBackup
**Use Backup Host Pool:** no
**Backup Host Pool Name:** (none)
**Use Vendor Change Tracking:** no
**Dynamic Multi-Stream:** no
Max Streams/Volume: 4
Max Files in batch: 300

Example 2 - Activate the policy named test1 without modifying any other policy attributes, enter the following:

```
# bpplinfo test1 -modify -active
```

Example 3 - Return the attributes of tstpolicy to their default values, perform the following:

```
# bpplinfo tstpolicy -set
# bpplinfo tstpolicy -L
```

Policy Type: Standard (0)
Active: yes
Follow NFS Mounts: no
Cross Mount Points: no
Client Compress: no
Collect TIR Info: no
Policy Priority: 0
Ext Security Info: no
File Restore Raw: no
Client Encrypt: no
Multiple Streams: 0
Disaster Recovery: 0
Max Jobs/Policy: 8
Disaster Recovery: 0
Collect BMR Info: no
Max Frag Size: 0 MB (1048576 MB)
Residence: -
Volume Pool: NetBackup

Example 4 - Display a short listing for the policy that is named mkbpolicy:

```
# bpplinfo mkbpolicy -l
INFO 0 0 0 0 *NULL* 0 0 99 0 0 0 0 0 0 0 0 *NULL* 1
KEY my temp directory
BCMD *NULL*
RCMD *NULL*
RES mkbunit *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL*
POOL NetBackup *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL*
FOE 0 0 0 0 0 0 0 0 0 0
```

Example 5 - Configure the Oracle policy that is named mypolicy. This example uses two RMAN channels concurrently for the data file backups. The example also
skips read-only data files and includes no more than four files in each backup set. Remember that any key that is not explicitly set is automatically reset to the default value. Confirm the changes afterwards.

```
# bpplinfo mypolicy –modify –ora_bkup_data_file_args NUM_STREAMS=2,
  SKIP_READ_ONLY=1,FORCE_READ_ONLY=0,SPECIFY_MAX_LIMITS=1,
  NUM_FILES_PER_BACKUP_SET=4

# bpplinfo mypolicy –L
Oracle Backup Data File Arguments: NUM_STREAMS=2,
  SKIP_READ_ONLY=1,FORCE_READ_ONLY=0,SPECIFY_MAX_LIMITS=1,
  NUM_FILES_PER_BACKUP_SET=4
```

FILES

UNIX systems:

```
/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/db/policy/policy_name/info
```

Windows systems:

```
install_path\NetBackup\logs\admin/*
install_path\NetBackup\db\policy\policy_name\info
```
bpplist

bpplist – list policy information

SYNOPSIS


On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

bpplist lists policies within the NetBackup database.

Any authorized users can initiate this command.

For more about NetBackup authorization, see the NetBackup Security and Encryption Guide.

OPTIONS

-allpolicies

Lists all policies.

-hwos

Lists possible hardware and the operating system.

-inclusion_discovered

This option lists the virtual machines that were discovered and selected the last time a VMware or Hyper-V intelligent policy ran. It also lists the host that performed the virtual machine discovery, such as the media server. This option is ignored if the intelligent policy has never been run.

Please be aware you cannot use this option with the -inventory option.

When the option is used with -byclient client, it lists information on the VMware and Hyper-V intelligent policies that discovered and selected the specified client (virtual machine) in the last policy run.
When the option is used with `-allpolicies`, it lists the virtual machines that were discovered and selected for all VMware and Hyper-V intelligent policies.

`-L`
Displays a full (long) listing. See the `policyname` option for details on the fields shown.

`-l`
Displays the information in raw output mode.

`-M master_server,...`
Lists the policy information for one or more specified masters.

`-U`
Displays information in user list mode. This listing is similar to the long-type list, but it has fewer entries.

`-byclient client`
Lists the policy information for all policies that contain the client indicated.

`-include_automanaged`
Lists all policies, including automanaged policies. Automanaged policies are generated when a workload administrator protects an asset by subscribing to a protection plan. Protection plans are created by using the NetBackup Service Level Objectives (SLO) technology. Automanaged policy names use the prefix `SLOENGINE_MANAGED+`.

`-inventory`
Creates an inventory of the current NetBackup policies and compares it to the previously created inventory. You can create touch file `LOG_CLASS_QUERIES` in `/usr/openv/netbackup` to log changes to policies.

The changes are logged in `/usr/openv/netbackup/logs/PolicyQueries.log`. The customer is responsible for the administration of the log file (periodic truncation, etc.).

Please be aware you cannot use this option with the `-include_discovered` option.

`-keyword "keyword phrase"`
The value is associated with all backups created by using this policy. The keyword phrase can be used to link related policies. It can also be used during restores to search only for the backups that have the keyword phrase association.

`policyname`
Specifies the policy in the NetBackup database.
The following describes the fields in the output of a `bppllist policyname` command:

**CLASS**
- Field 1 - Policy name
- Field 2 - Name (internal)
- Field 3 - Options
- Field 4 - Protocol version
- Field 5 - Time zone offset from GMT
- Field 6 - Audit reason

**INFO**
- Field 1 - Policy type
  
  0 = Standard (UNIX and Linux clients),
  1 = Proxy,
  4 = Oracle,
  6 = Informix-On-BAR,
  7 = Sybase,
  8 = MS-SharePoint portal server,
  11 = DataTools-SQL-BackTrack,
  13 = MS-Windows,
  15 = MS-SQL-Server,
  16 = MS-Exchange-Server,
  17 = SAP,
  18 = DB2,
  19 = NDMP,
  20 = FlashBackup,
  21 = Splitmirror,
  25 = Lotus Notes,
  29 = FlashBackup-Windows,
  35 = NBU-Catalog,
  36 = Generic,
  38 = PureDisk export,
  39 = Enterprise_Vault,
  40 = VMware,
  41 = Hyper-V,
  44 = BigData,
  46 = Deployment
- Field 2 - Follow NFS mounts. 0 = no, 1 = yes
- Field 3 - Client compress. 0 = no, 1 = yes
- Field 4 - Job priority. Valid values are 0-99999.
- Field 5 - Proxy client.
- Field 6 - Client encrypt. 0 = no, 1 = yes
- Field 7 - Disaster recovery. Catalog use DR file option. 0 = no, 1 = yes
- Field 8 - Maximum jobs allowed per client. Valid values are 0-999.
- Field 9 - Cross mount points. 0 = no, 1 = yes
- Field 10 - max frag size (deprecated)
- Field 11 - Active. Specifies if the policy is active or not. 0 = yes, 1 = no
- Field 12 - Collect TIR (true image restore) info. 0 = do not collect TIR info,
  1 = collect TIR info without move detection,
  2 = collect TIR info with move detection
- Field 13 - Enable block level incremental backups. 0 = no, 1 = yes
- Field 14 - Ext_sec_info.
- Field 15 - Individual file restore from raw
- Field 16 - Streaming
- Field 17 - Frozen image (internal use)
- Field 18 - Backup copy (internal use)
- Field 19 - Date when policy becomes effective
- Field 20 - Class ID
- Field 21 - Number of backup copies to create. Valid values are 1-4.
- Field 22 - Enable checkpoints. 0 = no, 1 = yes
- Field 23 - Checkpoint interval.
- Field 24 - Unused.
- Field 25 - Enable Instant Recovery. 0 = no, 1 = yes
- Field 26 - Perform off-host backup. 0 = no, 1 = yes
- Field 27 - Enable use alternate client for backup. 0 = no, 1 = yes
- Field 28 - Enable data mover. 0 = no, 1 = yes
- Field 29 - Data mover type
  - -1 = Unknown data mover type, 1 = Third-party copy, 2 = Media server copy, 3 = Network attached storage, 5 = NDMP
- Field 30 - Collect BMR (Bare Metal Restore) information. 0 = no, 1 = yes
- Field 31 - Storage service (lifecycle) is in use by residence. 0 = no, 1 = yes
- Field 32 - Enable granular restore. 0 = no, 1 = yes
- Field 33 - Job subtype (internal)
- Field 34 - Use virtual machine. 0 = No virtual machine, 1 = VMware, 2 = Hyper-V, 3 = VxVI
- Field 35 - Ignore the client side deduplication setting. 0 = no, 1 = yes
- Field 36 - Enable Exchange Database backup source. String output.
- Field 37 - Generation.
- Field 38 - Application discovery. 0 = no, 1 = yes. Enabled intelligent policy processing.
- Field 39 - Discovery lifetime. Time in seconds for which application discovery is valid.
- Field 40 - Enable fast backup. 0 = no, 1 = yes
- Field 41 - Optimized backup. 0 = no, 1 = yes. Enables the backup of deduplicated data that some Microsoft Windows operating system versions provide. If a client has a deduplicated file system configured, NetBackup backs up the deduplicated data. If the client is not set up for deduplication or does not support it, then a normal file backup occurs.
- Field 42 - client_list_type. This option is used for MS-SQL-Server policies. If 0, the type is HOST. This policy is the legacy MS-SQL-Server policy. The valid schedule types are FULL and USER. The types that are shown apply only to a SQL Server Intelligent Policy. The valid schedules types are FULL, INCR, and TLOG. If 1, the type is INSTANCE and you can add registered instances or databases in the instances to the policy. If 2, the type is INSTANCE_GROUP and you can add registered instance groups to the policy.
- Field 43 - select_list_type. This option is used for MS-SQL-Server policies. The value determines the type of backup selections or file list items. If 0, the type is HOST. This type must be used with the legacy MS-SQL-Server policy. The only backup selection that is valid for this type is the path of the backup batch file. The types that are shown apply only to a SQL Server Intelligent Policy. If 1, the type is WHOLE_DATABASE. The only backup selection that is valid for this type is WHOLE_DATABASE. If 3, the type is DATAFILE. The only backup selection that is valid for this type is the name of the file. If 7, the type is FILEGROUP. The only backup selection that is valid for this type is the name of the filegroup.
- Field 44 - Application consistent. Specifies that the virtual machine is quiesced before a persisted hardware snapshot is taken (1). Otherwise, the hardware snapshot does not quiesce the virtual machine (0 - default condition).

KEY
- Field 1 - Policy keyword phrase (string).
RES
- Field 1 - Residence or storage unit, one for each copy
POOL
- Field 1 - volume pool name, one for each copy
FOE
- Field 1 - Fail on error. 0 = continue, 1 = fail all copies
SHAREGROUP
- Field 1 - Media share group (media owner), a value pair for each copy

**DATACLASSIFICATION**
- Field 1 - Policy data classification. platinum = highest classification, gold = 2nd highest, silver = 3rd highest, bronze = lowest rank

**HYPERVSERVER**
- Indicates that the policy is for a Hyper-V server

**NAMES**
- Generic list of names defined by the query type

**BCMD**
- This field is obsolete and is scheduled to be removed from NetBackup.

**RCMD**
- This field is obsolete and is scheduled to be removed from NetBackup.

**APPLICATIONDEFINED**
- Application or client defined multipurpose string

**ORABKUPDATAFILEARGS**
- Lists the values used to override the default arguments for Oracle data files backup using RMAN

**ORABKUPARCHLOGARGS**
- Lists the values used to override the default arguments for Oracle archived redo log backup using RMAN

**CLIENT**
- Client in the policy

**SCHED**
- Field 1 - Schedule name for the specified policy
- Field 2 - Backup type for the schedule. 0 = Full schedule, 1 = Differential incremental schedule, 2 = User backup schedule, 3 = User archive schedule, 4 = Cumulative incremental schedule.
- Field 3 - Number of multiplexing copies to run. Valid values are 1-32.
- Field 4 - Frequency of the schedule in seconds. Valid values are 1-2147040000 (3550 weeks).
- Field 5 - Retention level of the schedule. All retention levels except 9 and 25 are user editable. Valid values are 0-100. See the `-rl retention_level`
option description for a complete list of default values and their retention levels.

**Note:** If you run this command on a pre-NetBackup 8.0 media server, the output only displays the retention levels between 0 and 24.

- Field 6 - u_wind/o/d. Reserved for future use
- Fields 7-8 - Reserved for future use
- Field 9 - Alternate read server
- Field 10 - Maximum fragment size in megabytes
- Field 11 - Calendar. 0 = Schedule is frequency-based, 1 = Schedule is calendar-based with no retries, 2 = Schedule is calendar-based with retries
- Field 12 - Number of copies that are configured for a backup. Valid values are 2-4.
- Field 13 - Fail on error setting for each copy
- Field 14 - Synthetic backup. 0 = no, 1 = yes
- Field 15 - PFI fast recover enable. 0 = no, 1 = yes
- Field 16 - Priority of migration job
- Field 17 - Storage service (lifecycle) used for residence. 0 = no, 1 = yes
- Field 18 - Checksum change detection enable. 0 = no, 1 = yes

**SCHEDCALEDATES**
- Exclude calendar dates in Epoch time. Example: To exclude dates of 06/04/2013, 06/07/2013 and 06/18/2013 (all at 05:00:00 GMT) is shown as follows: SCHEDCALEDATES 1346734800 1346994000 1347944400

**SCHEDCALENDAR**
- If schedule type is CALENDAR, this field indicates whether retries are allowed after run day. 0 = no, 1 = yes

**SCHEDCALDAYOFWEEK**
- Include calendar days of week in day-week format, where day is 1-7 (Sunday is 1) and week is week number of the month. Example: To include days of the week Sunday, Week 1; Tuesday, Week 1; Wednesday, Week 4 is shown as follows: SCHEDCALDAYOFWEEK 1,1;3,1;4,4

**SCHEDWIN**
Seven pairs of the form start,duration, which expresses the start and duration of the window for each day of the week. The starting day is Sunday. Start value is the number of seconds past midnight. Duration is the number of seconds past start.

**SCHEDRES**

- Residence or storage unit, a value pair for each copy (storage_unit storage_unit). Example: 2 copies are specified, with copy 1 going to stu_msdp_myhost1, and copy 2 going to stu_advdisk_myhost2: SCHEDRES stu_msdp_myhost1 stu_advdisk_myhost2 *NULL* *NULL* *NULL* *NULL* *NULL* *

**SCHEDPOOL**

- Pool, a value pair for each copy (volume_pool_name volume_pool_name). Example: 2 copies are specified, with copy 1 going to pool NetBackup, and copy 2 going to pool MediaPool_1: SCHEDRES NetBackup MediaPool_1 *NULL* *NULL* *NULL* *NULL* *NULL* *

**SCHEDRL**

- Retention level of the schedule. All retention levels except 9 and 25 are user editable. Valid values are 0-100. See the `-rl retention_level` option description for a complete list of default values and their retention levels.

**Note:** If you run this command on a pre-NetBackup 8.0 media server, the output only displays the retention levels between 0 and 24.

**SCHEDFOE**

- Fail on error. A value pair for each copy. 0 = continue, 1 = fail all copies

**SCHEDSG**

- Share group (media owner), a value pair for each copy. Example: Copies are defined, the first copy having a share group of NONE, the second copy have a share group of ANY. SCHEDSG *NONE* *ANY* *NULL* *NULL* *NULL* *NULL* *

`-verbose`

Selects verbose mode for logging.
**bpplsched**

bpplsched – add, delete, or list NetBackup schedules

**SYNOPSIS**

```


bpplsched policy_name [-v] [-M master_server,...] -add sched_label [-st sched_type] [-freq frequency] [-mpxmax mpx_factor] [-number_copies number] [-synthetic 0|1] [-pfi_fast_recovery 0|1] [-rl retention_level [,rl_copy,...]] [-residence storage_unit_label [,stunit_copy,...]] [-pool volume_pool_label [,pool_copy,...] [-res_is_stl 0|1] [-fail_on_error 0|1[,0|1,...,0|1]] [-sg share_group [,share_copy,...] [-window start duration] [-cal 0|1|2] [-ut] [-incl mm/dd/yyyy] [-excl mm/dd/yyyy] [-weekday day_name week [day_name week]...] [-dayomonth 1-31 [1-31]... | l] [-xweekday day_name week [day_name week]...] [-xdayomonth 1-31 [1-31]... | l] [-generation generation] [-reason "string"] [[SLP_Internal_Policy] -slpwindow]
```

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
**DESCRIPTION**

bpplsched does one of the following:

- Add a new schedule to a policy.
- Delete one or more schedules from a policy.
- List one or all schedules in a policy.
Note:

Veritas recommends that users do not modify or delete automanaged policies. If the user modifies the policy, they must make sure that the policy continues to meet the service level objective as defined by the protection plan. If the user deletes the policy, they must make sure that the asset is added to another protection plan that meets the service level objective.

For the `-add` and `-delete` options, `bpplsched` returns to the system prompt immediately after it submits the schedule change request to NetBackup. To determine whether the change was successful, run `bpplsched` again to list the updated schedule information.

The `-slpwindow` option lets you set up a schedule for a storage lifecycle policy (SLP) that is based on a time window and only supports start time and end time. You must use the predefined policy name `SLP_Internal_Policy`, and the schedule type must be `UBAK` (User Backup).

When the listing option is used, a single entry for each schedule appears even if the `-M` option is used. The `-l` form lists the following information for each schedule:

**SCHED**

Field 1 - Schedule name for the specified policy

Field 2 - Backup type for the schedule. 0 = Full schedule, 1 = Differential incremental schedule, 2 = Cumulative incremental schedule, 3 = User backup schedule, 4 = User archive schedule

Field 3 - Number of multiplexing copies to run. Valid values are 1-32.

Field 4 - Frequency of the schedule in seconds. Valid values are 1-2147040000 (3550 weeks).

Field 5 - Retention level of the schedule. All retention levels except 9 and 25 are user editable. Valid values are 0-100. See the `-rl retention_level` option description for a complete list of default values and their retention levels.

Note: If you run this command on a pre-NetBackup 8.0 media server, the output only displays the retention levels between 0 and 24.

Field 6 - u_wind/o/d. Reserved for future use

Fields 7-8 - Reserved for future use

Field 9 - Alternate read server

Field 10 - Maximum fragment size in megabytes
Field 11 - Calendar. 0 = Schedule is frequency-based, 1 = Schedule is calendar-based with no retries, 2 = Schedule is calendar-based with retries

Field 12 - Number of copies that are configured for a backup. Valid values are 2-4.

Field 13 - Fail on error setting for each copy

Field 14 - Synthetic backup. 0 = no, 1 = yes

Field 15 - PFI fast recover enable. 0 = no, 1 = yes

Field 16 - Priority of migration job

Field 17 - Storage service (lifecycle) used for residence. 0 = no, 1 = yes

Field 18 - Checksum change detection enable. 0 = no, 1 = yes

SCHEDCALENDAR

- If schedule type is CALENDAR, this field indicates whether retries are allowed after run day. 0 = no, 1 = yes

SCHEDCALEDATES

- Exclude calendar dates in Epoch time.
  Example: To exclude dates of 06/04/2013, 06/07/2013 and 06/18/2013 (all at 05:00:00 GMT) is shown as follows:

  SCHEDCALEDATES 1346734800 1346994000 1347944400

SCHEDCALDAYOFWEEK

- Include calendar days of week in day-week format, where day is 1-7 (Sunday is 1) and week is week number of the month.
  Example: To include days of the week Sunday, Week 1; Tuesday, Week 1; Wednesday, Week 4 is shown as follows:

  SCHEDCALDAYOFWEEK 1,1;3,1;4,4

SCHEDCALEDATES

- Exclude calendar dates in Epoch time. Example: To exclude dates of 09/04/2012, 09/07/2012 and 09/18/2012 (all at 05:00:00 GMT) is shown as follows:

  SCHEDCALEDATES 1346734800 1346994000 1347944400

SHAREGROUP

- Field 1 - Media share group (media owner), a value pair for each copy

DATACLASSIFICATION
- Field 1 - Policy data classification. platinum = highest classification, gold = 2nd highest, silver = 3rd highest, bronze = lowest rank

**SCHEDWIN**

- Seven pairs of the form `start,duration`, which expresses the start and duration of the window for each day of the week. The starting day is Sunday. `Start` value is the number of seconds past midnight. `Duration` is the number of seconds past start.

**SCHEDRES**

- Residence or storage unit, a value pair for each copy (storage_unit storage_unit). Example: 2 copies are specified, with copy 1 going to `stu_msdp_myhost1`, and copy 2 going to `stu_advdisk_myhost2`:

```
SCHEDRES stu_msdp_myhost1 stu_advdisk_myhost2 *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL*
```

**SCHEDPOOL**

- Pool, a value pair for each copy (volume_pool_name volume_pool_name). Example: 2 copies are specified, with copy 1 going to `NetBackup`, and copy 2 going to `MediaPool_1`:

```
SCHEDRES NetBackup MediaPool_1 *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL*
```

**SCHEDRL**

- Retention level of the schedule. All retention levels except 9 and 25 are user editable. Valid values are 0-100. See the `-rl retention_level` option description for a complete list of default values and their retention levels.

**Note:** If you run this command on a pre-NetBackup 8.0 media server, the output only displays the retention levels between 0 and 24.

**SCHEDFOE**

- Fail on error. A value pair for each copy. 0 = continue, 1 = fail all copies

**SCHEDSG**

- Share group (media owner), a value pair for each copy. Example: Copies are defined, the first copy having a share group of `NONE`, the second copy have a share group of `ANY`.

```
SCHEDSG *NONE* *ANY* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL*
```
If the \(-M\) option is used, \texttt{bpplsched} performs the operation on each of the master servers that are listed. For instance, if \texttt{bpplsched} adds a schedule, \texttt{bpplsched} adds the schedule to the policy on each of the master servers that is listed for \(-M\). If \(-M\) is used on a listing request, the listing is composed of returned information from all of the master servers in the \(-M\) list. If the command fails for any of the master servers, activity stops at that point.

To modify an existing NetBackup schedule, use the NetBackup command \texttt{bpplschedrep}.

Authorized users can initiate this command.

For more about NetBackup authorization, see the \textit{NetBackup Security and Encryption Guide}.

**OPTIONS**

These options are common to all forms of \texttt{bpplsched}:

\texttt{policy\_name}

The name of the policy that contains the schedules. The policy must exist before you run this command. This option is required, and must be the first one on the command line.

\texttt{\(-M\) master\_server,...}

A list of alternative master servers. This list is a comma-separated list of host names. If this option is present, each master server in the list runs the \texttt{bpplsched} command. Each master server in the list must allow access by the system that issues the \texttt{bpplsched} command.

If this option is present, the command is run on each master server in the list. If an error occurs for any master server, the process terminates at that point.

If \texttt{bpplsched} produces a listing, the listing is the composite of the returned information from all the master servers in this list.

If \texttt{bpplsched} adds or deletes a schedule, all master servers in this list receive the change.

\texttt{-v}

Selects the verbose mode. This option causes \texttt{bpplsched} to log additional information for debugging purposes. The information goes into the NetBackup administration debug log. This option is meaningful only when NetBackup enables the debug log function (that is, when the following directory is defined):

Windows systems:

\texttt{install\_path\NetBackup\logs\admin}
UNIX systems:

/usr/openv/netbackup/logs/admin

The remaining options depend on the form of `bpplsched`. The first form of `bpplsched` adds a schedule to the named policy. The following options apply to this form of `bpplsched`:

`-add sched_label [suboptions]`

Add a single schedule to the named policy.

The sub-options for the `-add` option are explained later in this description. These are attributes of the schedule being added.

For more about schedules and their attributes, see the NetBackup Administrator’s Guide, Volume I.

`-cal 0 | 1 | 2`

Indicates whether `bpplsched` follows a calendar-based schedule or a frequency-based schedule.

0 = frequency-based schedule
1 = calendar-based schedule with no retries after run day
2 = calendar-based schedule with retries after run day

`-dayomonth 1-31 [1-31]... | l`

Specifies the day or days of every month to run the schedule. Enter `l` (lowercase `L`) to run the last day of every month, whether the month contains 28, 29, 30, or 31 days.

For example, to run the policy backup on the 14th day and the 28th day of every month, enter the following:

`-dayomonth 14 28`

To run the last day of every month, enter:

`-dayomonth l`

`-excl mm/dd/yyyy`

Indicates to exclude this single date.

`-fail_on_error 0|1[,0|1,...,0|1]`

Specifies whether to fail all other copies if one copy fails. If no parameter is specified, 0 is default for all copies. Specify a value for each copy.

0 = Do not fail the other copies
1 = Fail other copies
-freq frequency
Determines how often backups run. Represents the number of seconds between
the backups that are initiated according to this schedule. When it is omitted on
the command line, the default value is 604800 (duration of one week in
seconds).

geneneration generation
Ensures that the command acts on a specific generation or version of a policy.
The generation value increments each time a policy is saved. Use bpplinfo
or bppllist to list the current generation value. If no generation is indicated,
the command acts on the current version.

-incl mm/dd/yyyy
Indicates to include this single date.

-mpxmax mpx_factor
The maximum number of jobs for this schedule that NetBackup multiplexes on
any one drive. mpx_factor is an integer that can range from 1 through 8 for
NetBackup Server and 1 through 32 for NetBackup Enterprise Server. A value
of one (1) means that backups for this schedule are not multiplexed. The default
is no multiplexing.

-number_copies number
Specify the number of simultaneous backup copies. The valid value range is
1-4. The default is 1.

-pfi_fast_recovery 0|1
Enables the user to turn on the feature to retain snapshots for instant recovery.
The default value is 0, which means this feature is disabled. A value of 1,
enables this feature.

-pool volume_pool_label[,pool-copy,...]
The name of the volume pool. This choice overrides the policy-level volume
pool. If you enter "NULL", NetBackup uses the volume pool that is specified
at the policy level. The default is to use the volume pool that is specified at the
policy level. The volume pool label cannot be None. If you do not specify a
volume pool at either the schedule level or the policy level, NetBackup uses a
default value of NetBackup.

When you specify -number_copies greater than 1, specify a pool for each
copy. If the storage unit is a disk enter "NULL" for that copy.

-reason "string"
Indicates the reason why you choose this command action. The reason text
string that you enter is captured and appears in the audit report. Enclose this
string with double quotes ("..."). The string must not exceed 512 characters. It cannot begin with a dash character (-) nor contain a single quotation mark (').

-res_is_stl
Identifies that the data in the storage unit is storage lifecycle.

-residence storage_unit_label[,stunit-copy,...]
The name of the storage unit, which specifies the location of the backup images. The value "NULL" causes NetBackup to use the storage unit that is specified at the policy level. The default is for NetBackup to use the storage unit that is specified at the policy level. If you do not specify a storage unit at either the schedule level or the policy level, NetBackup uses the next storage unit available.

When you specify -number_copies greater than 1, specify a residence for each copy.

-rl retention_level[,ri-copy,...]
The retention level determines how long to retain backups and archives. The retention_level is an integer between 0 and 100. The default retention level is 1. Valid retention levels and their corresponding default retention times are listed later in this description.

---

**Note:** If you run this command on a pre-NetBackup 8.0 media server, you can only specify a retention level between 0 and 24.

---

When you specify -number_copies greater than 1, specify a retention level for each copy.

---

**Caution:** You can change the retention period that is associated with each level by using the NetBackup administration interface. Therefore, your configuration may have different values for each level than those shown here. Use the NetBackup administration interface to determine the actual retention periods before you make any changes with this command.

---

Otherwise, backups can expire sooner than you expect, which results in loss of data.

- 0 (one week)
- 1 (2 weeks)
- 2 (3 weeks)
- 3 (1 month)
-sg share_group [,share_copy,...]
Specifies the share group(s) for the schedule. Do not use this option if the schedule resides on a disk storage unit. If *NONE* is specified, the writing media server owns the media that this policy writes. If *ANY* is specified, EMM chooses the media owner. *ANY* is the default value. Otherwise, the named share group owns the media. Specify a share group for each copy to display the configured share groups. Enter the following:

UNIX systems:
/usr/openv/netbackup/bin/admincmd/nbsvrgrp -list -summary

Windows systems:
install_path\NetBackup\bin\admincmd\nbsvrgrp
-list -summary

[SLP_Internal_Policy] -slpwindow
Adds, deletes, or lists time windows for an SLP_Internal_Policy. You can perform this action in the following two ways:

bpplsched -slpwindow

bpplsched SLP_Internal_Policy -slpwindow

-st sched_type
The type of the schedule. The default schedule type is FULL. The following list contains the possible values for this attribute with their meanings:

FULL - full
INCR - differential incremental
CINC - cumulative incremental
TLOG - transaction log
UBAK - user backup
UARC - user archive
Pre-check - Runs the NetBackup preinstall environment checker. You can only use this option with the Deployment policy type.

StagePackage - Moves a package to the client, but does not install it. Also performs the precheck operation. You can only use this option with the Deployment policy type.

InstallPackage - Installs the specified package. Also performs the precheck and stagepackage operations. If you already performed the stagepackage operation, the installpackage command does not move the package again. You can only use this option with the Deployment policy type.

-synthetic 0|1
Enables the user to determine which schedule occurs. A value of zero (0) means that the schedule is a real (non-synthetic) backup schedule. (0 is the default.) A value of one (1) means that the schedule is a synthetic backup schedule.

-ut
If any of the date or the time arguments follow -ut, they are accepted as UNIX time, instead of the standard time format. The -ut option is used primarily for Java.

-weekday day_name week [day_name week]...
Specifies a day of the week, and the week of the month, as a run day in the schedule.
- The day_name is: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday.
- The week is the number of the week in the month. A week begins on Sunday and ends on Saturday. Valid values are 1-5.

For example, to instruct the policy to run every Sunday of the month, enter:

-weekday Sunday 1 Sunday 2 Sunday 3 Sunday 4 Sunday 5

-window start duration
Specifies when NetBackup can run the backups for this schedule. Every day of the week has the same window.

start is the time at which the backup window opens for this schedule. This time is the number of seconds since midnight. This number is an integer between 0 and 86399 (86400 seconds in a day).

duration is the length of time that the window remains open. The time unit is seconds. This unit is a non-negative integer.
-xdayomonth 1-31 [1-31]... | 1
  Specifies the day or days of the month that you want to exclude as run days in the schedule. Use 1 (lowercase L) to indicate the last day of the month.
  For example, to instruct the policy to not run on the 14th and 15th of the month, enter:
  -xdayomonth 14 15

-xweekday day_name week [day_name week]...
  Specifies the day of the week and week of the month, to exclude as a run day in the schedule.
  ■ The day_name is: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday.
  ■ The week is the number of the week in the month. Valid values are 1-5.
  For example, to instruct the policy to not run on the first and the third Mondays of the month, enter:
  -xweekday Monday 1 Monday 3

The second form of bpplsched deletes one or more schedules from the named policy. The following option applies to this form of bpplsched:

-delete sched_label
  Delete the listed schedules from the named policy. Separate the elements of the sched_label list with spaces. There can be up to 25 labels in the list.

The third form of bpplsched deletes all schedule from the named policy. The following option applies to this form of bpplsched:

-deleteall
  Delete all schedules from the named policy.

The fourth form of bpplsched produces a listing of information about the schedules for the named policy. The following options apply to this form of bpplsched:

-l
  The list type is short (the default list type). This option produces a terse listing that includes all attributes for the schedule. Each schedule occupies one line of the listing. Most attribute values are expressed numerically. This option is useful for scripts or the programs that rework the listing contents into a customized report format.

-L
  The list type is long. This listing includes all attributes for the schedule. Some attribute values are descriptive terms, rather than numbers.
- `label sched_label`
  List the attributes for this schedule in the named policy. The default is to list information for all schedules for the named policy.

- `-U`
  The list type is user. This listing is similar to the long-type list, but it has fewer entries. Most attribute values are descriptive terms, rather than numbers.

**EXAMPLES**

Example 1 - List the information for schedule user within policy `tstpolicy` in two different ways. The first display is in long mode. The second is in User mode, which shows fewer entries than the Long mode display.

```
# bpplsched tstpolicy -L -label user
Schedule:   user
  Type:          UBAK (2)
  Frequency:    1 day(s) (86400 seconds)
  Retention Level: 0 (1 week)
  u-wind/o/d:  0 0
  Incr Type:    DELTA (0)
  Incr Depends: (none defined)
  Max Frag Size: 0 MB (1048576 MB)
  Maximum MPX:  1
  Number copies: 1
  Fail on Error: 0
  Residence:   (specific storage unit not required)
  Volume Pool:  (same as policy volume pool)
  Daily Windows:
    Day   Open       Close     W-Open     W-Close
    Sunday 000:00:00 024:00:00 000:00:00 024:00:00
    Monday 000:00:00 024:00:00 024:00:00 048:00:00
    Tuesday 000:00:00 024:00:00 048:00:00 072:00:00
    Wednesday 000:00:00 024:00:00 072:00:00 096:00:00
    Thursday 000:00:00 024:00:00 096:00:00 120:00:00
    Friday 000:00:00 024:00:00 120:00:00 144:00:00
    Saturday 000:00:00 024:00:00 144:00:00 168:00:00

# bpplsched tstpolicy -U -label user
Schedule:   user
  Type:          User Backup
  Retention Level: 0 (1 week)
  Maximum MPX:  1
  Number copies: 1
```
Fail on Error:0
Residence: (specific storage unit not required)
Volume Pool: (same as policy volume pool)

Daily Windows:
- Sunday 00:00:00 --> Sunday 24:00:00
- Monday 00:00:00 --> Monday 24:00:00
- Tuesday 00:00:00 --> Tuesday 24:00:00
- Wednesday 00:00:00 --> Wednesday 24:00:00
- Thursday 00:00:00 --> Thursday 24:00:00
- Friday 00:00:00 --> Friday 24:00:00
- Saturday 00:00:00 --> Saturday 24:00:00

Example 2 - While in operation on the system hatt, list information for the schedule named full in policy tstpolicy, as defined on the master server beaver:

```
# bpplsched tstpolicy -M beaver -L -label full
```

Schedule: full
Type: FULL (0)
Frequency: 0+ day(s) (14400 seconds)
Retention Level: 0 (1 week)
u-wind/o/d: 0 0
Incr Type: DELTA (0)
Incr Depends: (none defined)
Max Frag Size: 0 MB (1048576 MB)
Maximum MPX: 1
Number copies: 1
Fail on Error: 0
Residence: (specific storage unit not required)
Volume Pool: (same as policy volume pool)

Daily Windows:
- Sunday 00:00:00 Open Close W-Open W-Close
- Monday 00:00:00 24:00:00 048:00:00 072:00:00
- Tuesday 00:00:00 24:00:00 072:00:00 108:00:00
- Wednesday 00:00:00 24:00:00 108:00:00 144:00:00
- Thursday 00:00:00 24:00:00 144:00:00 180:00:00
- Friday 00:00:00 24:00:00 180:00:00 216:00:00
- Saturday 00:00:00 24:00:00 216:00:00 252:00:00

Example 3 - Add new schedule full_2 to the policy tstpolicy on beaver, then list the new schedule in long mode (-L). These commands run on the system hatt.

```
# bpplsched tstpolicy -M beaver -add full_2
# bpplsched tstpolicy -M beaver -label full_2 -L
```
Schedule: full_2
Type: FULL (0)
Frequency: 7 day(s) (604800 seconds)
Retention Level: 1 (2 weeks)
u-wind/o/d: 0 0
Incr Type: DELTA (0)
Incr Depends: (none defined)
Max Frag Size: 0 MB (1048576 MB)
Maximum MPX: 1
  Number copies: 1
  Fail on Error: 0
  Residence: (specific storage unit not required)
Volume Pool: (same as policy volume pool)
Daily Windows:
Day       Open       Close       W-Open       W-Close
Sunday    000:00:00  000:00:00  000:00:00  000:00:00
Monday    000:00:00  000:00:00  000:00:00  000:00:00
Tuesday   000:00:00  000:00:00  000:00:00  000:00:00
Wednesday 000:00:00  000:00:00  000:00:00  000:00:00
Thursday  000:00:00  000:00:00  000:00:00  000:00:00
Friday    000:00:00  000:00:00  000:00:00  000:00:00
Saturday  000:00:00  000:00:00  000:00:00  000:00:00

Example 4 - Delete the specified schedules from policy tstpolicy:

# bpplsched tstpolicy -delete full_3 user user_2 user_3

Example 5 - List the schedule information for policy tstpolicy:

# bpplsched tstpolicy -L
Schedule: full
Type: FULL (0)
Frequency: 1 day(s) (86400 seconds)
Retention Level: 0 (1 week)
u-wind/o/d: 0 0
Incr Type: DELTA (0)
Incr Depends: (none defined)
Max Frag Size: 0 MB (1048576 MB)
Maximum MPX: 1
  Number copies: 1
  Fail on Error: 0
  Residence: (specific storage unit not required)
Volume Pool: (same as policy volume pool)
Daily Windows:
Day Open Close W-Open W-Close
Sunday 00:00:00 24:00:00 00:00:00 24:00:00
Monday 00:00:00 24:00:00 02:48:00 04:00:00
Tuesday 00:00:00 24:00:00 04:00:00 07:20:00
Wednesday 00:00:00 24:00:00 07:20:00 09:56:00
Thursday 00:00:00 24:00:00 09:56:00 12:00:00
Friday 00:00:00 24:00:00 12:00:00 14:40:00
Saturday 00:00:00 24:00:00 14:40:00 16:80:00

Schedule: user
Type: UBAK (2)
Frequency: 1 day(s) (86400 seconds)
Retention Level: 0 (1 week)

Incr Type: DELTA (0)
Incr Depends: (none defined)
Max Frag Size: 0 MB (1048576 MB)
Maximum MPX: 1
Number copies: 1
Fail on Error: 0
Residence: (specific storage unit not required)
Volume Pool: (same as policy volume pool)

Example 6 - Add a new schedule, full, with a window from 11 P.M. to midnight. The second `bpplsched` lists the information for schedule full:

```bash
# bpplsched elevenpm -add full -window 82800 3600
bpplsched elevenpm -U -label full
Schedule: FULL (0)
Type: Full Backup
Frequency: every 7 days (604800 seconds)
Retention Level: 1 (2 weeks)
Maximum MPX: 1
Number copies: 1
```
Example 7 - Add an SLP schedule called `dup_tape1` with a window open from 6:00 to 10:00 a.m. Use the predefined policy name `SLP_Internal_Policy` and the UBAK schedule type. This window has no properties.

```
# bpplsched SLP_Internal_Policy -add dup_tape1 -window 21600 14400 -st UBAK -slpwindow
```

Example 8 - List the SLP windows that were created for your system. The output lists all the attributes for the two schedules.

```
# bpplsched -slpwindow -L
Schedule: Default_24x7_Window
Type: UBAK (2)
Frequency: 7 day(s) (604800 seconds)
   Excluded Dates---------
      No specific exclude dates entered
      No exclude days of week entered
Retention Level: 0 (1 hour)
u-wind/o/d: 0 0
Incr Type: DELTA (0)
Alt Read Host: (none defined)
Max Frag Size: 0 MB
PFI Recovery: 0
Maximum MPX: 1
Number Copies: 1
Fail on Error: 0
Residence: (specific storage unit not required)
Volume Pool: (same as policy volume pool)
Server Group: (same as specified for policy)
Residence is Storage Lifecycle Policy: 0
Daily Windows:
Day    Open    Close    W-Open    W-Close
```
**FILES**

**UNIX systems:**

```plaintext
/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/db/policy/policy_name/schedule
```
Windows systems:

install_path\NetBackup\logs\admin\*
install_path\NetBackup\db\policy\policy_name\schedule

SEE ALSO

See bpplschedrep on page 350.
bpplschedrep

bpplschedrep – modify NetBackup schedule attributes

SYNOPSIS

bpplschedrep policy_name sched_label [ -M master_server,...] [-v]
[-generation generation] [-st sched_type] [-freq backup_frequency]
[-mpxmax mpx_factor] [-cal 0|1|2] [-incl mm/dd/yyyy] [-excl
mm/dd/yyyy] [-delincl mm/dd/yyyy] [-delexcl mm/dd/yyyy] [-weekday
day_name week [day_name week]...] [-daymonth 1-31 [1-31]... | 1]
[-xweekday day_name week [day_name week]...] [-xdaymonth 1-31
[1-31]... | 1] [-delxdaymonth 1-31 [1-31]... | 1] [-delweekday
day_name week [day_name week]...] [-ci] [-ce] [-cw] [-cd]
[-number_copies number] [-rl retention_level[,rl-copy2, ...]]
[-fail_on_error 0|1[0,1,...,0|1]] [-residence storage_unit_label
[,stunit_copy2, ...]] [-pool volume_pool_label [,pool_copy2, ...]] [-sg
share_group [,share_copy2, ...]] [-0..6 start duration] [-res_is_stl
0 | 1] [-reason "string"] [-slpwindow] [-checksum_change_detection
0|1]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd

DESCRIPTION

bpplschedrep changes the attributes of a NetBackup schedule for a defined policy. The schedule and policy that bpplschedrep names should already exist when this command is run. If the -M option is used, bpplschedrep changes the schedule on each of the listed master servers.

The -slpwindow option lets you set up a schedule for a storage lifecycle policy (SLP) that is based on a time window and only supports start time and end time. You must use the predefined policy name SLP_Internal_Policy, and the schedule type must be UBAK (User Backup).

Any authorized user can initiate this command.

For more about NetBackup authorization, see the NetBackup Security and Encryption Guide.
Note:

It is not recommended that users modify or delete automanaged policies.

If the user modifies the policy, they must make sure that the policy continues to meet the service level objective as defined by the protection plan.

If the user deletes the policy, they must make sure that the asset is added to another protection plan that meets the service level objective.

OPTIONS

-(0..6) start duration

Specifies the window during which NetBackup can run the backups for this schedule. This window applies to a specific day of the week. 0 corresponds to Sunday, 1 to Monday, and so on.

start is the time at which the backup window opens for this schedule. This time is the number of seconds since midnight. It is an integer between 0 and 86400 (the number of seconds in a day).

duration is the length of time that the window remains open. The time unit is seconds. This unit is a non-negative integer.

-cal 0|1|2

Indicates whether bpplschedrep follows a calendar-based schedule or a frequency-based schedule.

0 = frequency-based schedule
1 = calendar-based schedule with no retries after run day
2 = calendar-based schedule with retries after run day

-checksum_change_detection 0|1

Enables or disables Accelerator Force Rescan in the policy schedule.

0 = disable
1 = enable

-dayomonth 1-31 [1-31]... | 1

Specifies the day or days of every month to run the schedule. Enter l (lowercase L) to run the last day of every month, whether the month contains 28, 29, 30, or 31 days.

For example, to run the policy backup on the 14th day and the 28th day of every month, enter the following:

-dayomonth 14 28
To run the last day of every month, enter:

```
-dayomonth 1
```

```
-deldayomonth 1-31 [1-31]... | l
```

Specifies a day of every month to exclude as a run day. Enter 1 (lowercase L) to exclude the last day of every month, whether the month contains 28, 29, 30, or 31 days. This command can only remove the dates that were added by using the `-dayomonth` command.

For example, to exclude from the schedule the 20th day and 21st day of every month that you originally specified as run days, enter:

```
-deldayomonth 20 21
```

```
-delweekday day_name week [day_name week]...
```

Specifies a day of the week and the week of the month to exclude as a run day from the schedule. This command can only remove the dates that were added by using the `-weekday` command.

- The `day_name` is: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday.
- The `week` is the number of the week in the month. A week begins on Sunday and ends on Saturday. Valid values are 1-5.

For example, to delete the second Monday of the month that you originally specified as a run day, enter:

```
-delweekday Monday 2
```

```
-excl mm/dd/yyyy
```

Indicates to exclude this single date.

```
-delincl mm/dd/yyyy
```

Indicates to delete this single date. This command can only remove the dates that were added by using the `-incl` command.

```
-delexcl mm/dd/yyyy
```

Indicates to delete this single date.

```
-ci
```

Clear all specific include dates.

```
-ce
```

Clear all specific exclude dates.

```
-cw
```

Clear all week days.
-cd
  Clear all days of a month.

-fail_on_error 0|1[,0|1,...,0|1]
  Specifies whether to fail all other copies if one copy fails. If no parameter is
  specified, 0 is default for all copies. Specify a value for each copy.
  0 - Do not fail the other copies
  1 - Fail other copies

-freq backup_frequency
  The backup frequency controls how much time can elapse between successful
  automatic backups for clients on this schedule. Frequency does not apply to
  user schedules because the user can perform a backup or archive any time
  the backup window is open. This value is a positive integer that represents the
  number of seconds between successful automatic backups for this schedule.

-help
  Prints a command-line usage message when -help is the only option on
  the command line.

-generation generation
  Ensures that the command acts on a specific generation or version of a policy.
  The generation value increments each time a policy is saved. Use bpplinfo
  or bpplist to list the current generation value. If no generation is indicated,
  the command acts on the current version.

-incl mm/dd/yyyy
  Indicates to include this single date.

-M master_server,...
  A list of alternative master servers. This list is a comma-separated list of host
  names. If this option is present, each master server in the list runs the
  bpplschedrep command. Each master server in the list must allow access by
  the system that issued the bpplschedrep command. If an error occurs for any
  master server, the process terminates at that point.
  The schedule attributes are modified on all the master servers in this list.

-mpxmax mpx_factor
  The maximum multiplexing factor for this schedule. Multiplexing sends
  concurrent, multiple backups from one or several clients to a single drive.
  The multiplexing factor can range from 1 through 8 for the NetBackup Server
  and 1 through 32 for the NetBackup Enterprise Server. A value of 1 specifies
  no multiplexing and a value greater than one means that NetBackup should
create multiplexed images on the destination media. The multiplexing factor should be less than or equal to the multiplexing factor for the storage unit.

For more about multiplexing, see the *NetBackup Administrator’s Guide, Volume I*.

-number_copies number

Specify the number of simultaneous backup copies. The valid value range is 1-4. The default is 1.

-policy_name

The name of the policy that contains the schedule. This policy has been previously created.

-pool volume_pool_label[,pool-copy2,...]

Specifies the volume pool(s) for the schedule. Do not use this option if a disk storage unit is the residence for the schedule. If "*NULL*" is specified, the volume pool for the schedule is the volume pool of the policy that contains this schedule.

Specify a pool for each copy.

To display the configured volume pools, run the following command:

UNIX systems:

/usr/openv/volmgr/bin/vmpool -listall

Windows systems:

install_path\Volmgr\bin\vmpool -listall

-reason "string"

Indicates the reason why you choose this command action. The reason text string that you enter is captured and appears in the audit report. Enclose this string with double quotes ("..."). The string must not exceed 512 characters. It cannot begin with a dash character (-) nor contain a single quotation mark (').

-res_is_stl 0 | 1

Specify this flag only when the name of the storage unit and the name of the storage lifecycle policy are the same. In all other cases this flag is ignored. The possible values are as follows:

0 - the residence is a non-storage life cycle policy
1 - the residence is a storage lifecycle policy

-residence storage_unit_label[,stunit-copy2,...]

Specifies the label(s) of the storage unit to be used for storing the backups that were created according to this schedule. If "*NULL*" is specified, the residence
for the schedule defaults to the residence of the policy that contains this schedule. If the residence value is a storage unit label, the residence for the schedule becomes that storage unit and overrides the residence for the policy.

Specify a storage unit for each copy.

Run `bpstulist` to display the set of defined storage units.

```
-rl retention_level[,ri-copy2,...]
```

Specifies how long NetBackup retains the backups that it creates by using this schedule. Valid retention levels and their corresponding default retention times are listed later in this description.

Specify a retention level for each copy.

---

**Caution:** You can change the retention period that is associated with each level by using the NetBackup administration interface. Therefore, your configuration may have different values for each level than those shown here. Use the NetBackup administration interface to determine the actual retention periods before you make any changes with this command.

Otherwise, backups can expire sooner than you expect, which results in loss of data.

- 0 (one week)
- 1 (2 weeks)
- 2 (3 weeks)
- 3 (1 month)
- 4 (2 months)
- 5 (3 months)
- 6 (6 months)
- 7 (9 months)
- 8 (1 year)
- 9-100 (infinite, except 25 which is expire immediately)

**Note:** If you run this command on a pre-NetBackup 8.0 media server, you can only specify a retention level between 0 and 24.

NetBackup keeps the information about the backups for the specified time. Then it deletes information about them. When the information is deleted, the
files in the backups are unavailable for restores. When all the backups on a
to be reassigned.

\textbf{sched\_label}

Specifies the name of the schedule to be changed. This schedule has been
previously created.

\textbf{-sg \ share\_group [,,share\_copy2,...]}

Specifies the share group(s) for the schedule. Do not use this option if the
schedule resides on a disk storage unit. If \text{*NONE*} is specified, the writing
media server owns the media that this policy writes. If \text{*ANY*} is specified, EMM
chooses the media owner. \text{*ANY*} is the default value. Otherwise, the named
share group owns the media. Specify a share group for each copy to display
the configured share groups. Enter the following:

\textbf{UNIX systems:}

\texttt{/usr/openv/netbackup/bin/admincmd/nbsvrgrp}
\begin{verbatim}
   -list -summary
\end{verbatim}

\textbf{Windows systems:}

\texttt{install_path\NetBackup\bin\admincmd\nbsvrgrp}
\begin{verbatim}
   -list -summary
\end{verbatim}

\textbf{-slpwindow}

Adds or deletes time windows for an SLP\_internal\_policy.

\textbf{-st \ sched\_type}

Specifies the type of backup this schedule performs. Schedule types fall into
either an automatic category or user category. Automatic schedules define the
windows during which the NetBackup scheduler can initiate a backup for this
policy.

User schedules define the windows during which a user can initiate a backup
or archive.

The values for schedule type are as follows:

- \textbf{FULL} - full backup
- \textbf{INCR} - differential incremental backup
- \textbf{CINC} - cumulative incremental backup
- \textbf{TLOG} - transaction log
- \textbf{UBAK} - user backup
- \textbf{UARC} - user archive
- Pre-check - Runs the NetBackup preinstall environment checker. You can only use this option with the Deployment policy type.

- StagePackage - Moves a package to the client, but does not install it. Also performs the precheck operation. You can only use this option with the Deployment policy type.

- InstallPackage - Installs the specified package. Also performs the precheck and stagepackage operations. If you already performed the stagepackage operation, the installpackage command does not move the package again. You can only use this option with the Deployment policy type.

- weekday day_name week [day_name week]...
  Specifies a day of the week and a week of the month as a run day in the schedule.
  - The day_name is: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday.
  - The week is the number of the week in the month. A week begins on Sunday and ends on Saturday. Valid values are 1-5.

  For example, to instruct the policy to run every Sunday of the month, enter:

  - weekday Sunday 1 Sunday 2 Sunday 3 Sunday 4 Sunday 5

- v
  Selects the verbose mode. This option causes bpplschedrep to log additional information for debugging purposes. The information goes into the NetBackup administration daily debug log. This option is meaningful only when NetBackup enables the debug log function (that is, when the following directory is defined):

  UNIX systems:

  /usr/openv/netbackup/logs/admin

  Windows systems:

  install_path\NetBackup\logs\admin

- xdayomonth 1-31 [1-31]... | l
  Specifies the day or days of the month that you want to exclude as run days in the schedule. Use l (lowercase L) to indicate the last day of the month.

  For example, to instruct the policy to not run the backup on the 6th of the month, enter:

  -xdayomonth 6
Specifies the day of the week and week of the month, to exclude as a run day in the schedule.

- The day_name is: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday.
- The week is the number of the week in the month. Valid values are 1-5.

For example, to instruct the policy to not run on the third Monday and Wednesday of the month, enter:

-xweekday Monday 3 Wednesday 3

EXAMPLES

Example 1 - Set the frequency for a schedule.

# bpplschedrep mkbpolicy incr -freq 604800

This sets to one (1) week the frequency with which automatic backups are performed for the schedule incr in policy mkbpolicy.

Example 2 - For Saturday and Sunday of each week, have the window for schedule in policy mkbpolicy open at 10 P.M. instead of 11 P.M. Also, set the window duration to two (2) hours instead full of one (1) hour. bpplschedrep resets the windows, and bppl scheduled lists the new schedule values.

# bpplschedrep newpolicy full -0 79200 7200 -6 79200 7200
# bppl scheduled newpolicy -U -label full

Schedule: full
Type: Full Backup
Frequency: every 7 days
Retention Level: 1 (2 weeks)
Maximum MPX: 1
Residence: (specific storage unit not required)
Volume Pool: (same as policy volume pool)

Daily Windows:
Sunday 22:00:00 --> Sunday 24:00:00
Monday 23:00:00 --> Monday 24:00:00
Tuesday 23:00:00 --> Tuesday 24:00:00
Wednesday 23:00:00 --> Wednesday 24:00:00
Thursday 23:00:00 --> Thursday 24:00:00
Friday 23:00:00 --> Friday 24:00:00
Saturday 22:00:00 --> Saturday 24:00:00
Example 3 - Change the open window of SLP schedule `dup_tape1` to 6 A.M. to 10 A.M. Use the predefined policy name `SLP_internal_policy` and the UBAK schedule type. This window has no properties.

```
# bpplschedrep SLP_internal_policy -add dup_tape1 -window 21600 14400 -st UBAK -slpwindow
```

**FILES**

**UNIX systems:**

```
/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/db/policy/policy_name/schedule
```

**Windows systems:**

```
install_path\NetBackup\logs\admin/*
install_path\NetBackup\db\policy\policy_name\schedule
```

**SEE ALSO**

See `bpplsched` on page 332.
bpplschedwin

bpplschedwin — used to add or modify schedule windows.

SYNOPSIS

bpplschedwin policy_name sched_label [-verbose] [-M master_server,...] [-generation generation] [-reason string] [-0..6 seconds_past_midnight duration_seconds]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/
On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

Use the bpplschedwin command add new schedule windows or modifies the current schedule windows. Use the bpplsched command to list the schedule information and determine if the change was successful.

OPTIONS

-0..6 seconds_past_midnight duration_seconds

Use this combination of three numbers to define the day, start time, and duration of the schedule window.

The first number indicates the day of the week: -0 is Sunday, -1 is Monday, -2 is Tuesday, -3 is Wednesday, -4 is Thursday, -5 is Friday, and -6 is Saturday.

The seconds_past_midnight number indicates the start time. It is specified as the number of seconds after midnight. For example, 5:00 A.M. is 18000 seconds past midnight.

The duration_seconds value is the number of seconds past the start of the window. So 3600 is one hour. The minimum duration value for a deployment schedule is 300 seconds. You cannot specify a duration value larger than 8553600 seconds for a deployment schedule.
-generation generation
   Ensures that the command acts on a specific generation or version of a policy. The generation value increments each time a policy is saved. Use the `bpplinfo` command or the `bppllist` command to list the current generation value. If no generation is indicated, the command acts on the current version.

-M master_server,...
   This comma-separated list of host names specifies alternative master servers. If this option is included, each master server in the list runs the `bpplschedwin` command. Each master server in the list must allow access by the system that issues the `bpplschedwin` command. If this option is used, the command is run on each master server in the list. If an error occurs for any master server, the process terminates at that point.

policy_name
   The name of the policy that contains the schedule you want to add or modify. The policy must exist before you run this command. This option must be the first one on the command line.

-reason "string"
   If this option is specified, it indicates why the schedule was added or modified. The text string that is entered is captured and appears in the audit report. This string must be enclosed in double quotes ("..."). The string cannot exceed 512 characters. It cannot begin with a dash character (-) or contain a single quotation mark (‘).

sched_label
   The name of the schedule that contains the window being added or modified. The schedule must exist before you run this command. This option is required and must follow the `policy_name` option in the command line.

-verbose
   Selects the verbose mode. This option is only useful if debug logging is enabled. This option causes `bpplschedwin` to log additional information into the NetBackup administration debug log. The NetBackup administration debug log is found at `install_path\NetBackup\logs\admin` on Windows and `/usr/openv/netbackup/logs/admin` on UNIX and Linux.

EXAMPLES

Example 1: Modify sched3 deployment schedule in the dpol1 policy to start on 5/30/2018 at 5:00 A.M. and end on 6/2/2018 5:00 A.M.

# bpplschedwin dpol1 sched3 -0 0 0 -1 0 0 -2 0 0 -3 18000 259200
   -4 0 0 -5 0 0 -6 0 0
# bpplsched dpoll -label sched3
SCHED sched3 6 1 604800 1 0 0 0 *NULL* 0 1 0 0 0 0 -1 0 0
SCHEDCALENDAR
SCHEDCALIDATES 1528223400 1528309800 1528396200
SCHEDWIN 0 0 0 0 0 0 18000 259200 0 0 0 0 0 0
SCHEDRES *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL*
   *NULL* *NULL*
SCHEDPOOL *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL*
    *NULL* *NULL*
SCHEDRL 1 1 1 1 1 1 1 1 1
SCHEDFOE 0 0 0 0 0 0 0 0 0
SCHEDSG *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL*
    *NULL* *NULL*

SEE ALSO

See bpplinfo on page 297.
See bppllist on page 324.
See bpplsched on page 332.
bppolicynew

bppolicynew – create, copy, or rename a NetBackup policy

SYNOPSIS

bppolicynew policy_name [-verbose] [-M master_server,...] [-reason "string"]

bppolicynew policy_name -sameas existing_policy_name [-verbose] [-M master_server,...] [-reason "string"]

bppolicynew existing_policy_name -renameto policy_name [-verbose] [-M master_server,...] [-reason "string"]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

bppolicynew performs one of the following operations on a NetBackup policy:

- Create a new policy with default attribute values.
- Create a new policy with the same attributes as an existing policy.
- Rename an existing policy.

When bppolicynew runs without -sameas or -renameto, it creates a new NetBackup policy with default attribute values. If -M is present, the defaults that are used for the policy definition on each master server are the defaults for that master server.

bppolicynew copies a policy by adding a new policy to the NetBackup database. The clients, files, schedules, and attributes for the new policy are the same as those for the existing policy. bppolicynew does not create a policy copy with the same name as an existing policy.

If bppolicynew renames a policy, the existing association of images with the policy is lost. This means that the images that were created before the policy was renamed are not included in a list of images for the renamed policy. The command does not rename a policy with the same name as an existing policy.
bpplinfo replaces the policy-attribute defaults with new values. bpplclients, bpplineude, and bppsched define the clients, backup files, and schedules for the policy. A policy needs to have at least one client, one file specification, and one automatic schedule before it can run automatic backups.

bppolicynew sends its error messages to stderr. bppolicynew sends a log of its activity to the NetBackup admin log file for the current day.

Authorized user can initiate this command.

For more about NetBackup authorization, see the NetBackup Security and Encryption Guide.

For more about policies, see the NetBackup Administrator’s Guide, Volume I.

---

**Note:**

It is not recommended that users modify or delete automanaged policies.

If the user modifies the policy, they must make sure that the policy continues to meet the service level objective as defined by the protection plan.

If the user deletes the policy, they must make sure that the asset is added to another protection plan that meets the service level objective.

---

**OPTIONS**

**policy_name**

Specifies the name of a NetBackup policy that bppolicynew creates or the name to which bppolicynew changes an existing policy. The option has no default value.

This policy name must differ from any existing policy name. It is composed of numeric, alphabetic, plus, minus, underscore, and period characters. Do not use a minus as the first character or leave spaces between characters.

**existing_policy_name**

The name of a NetBackup policy that already exists when bppolicynew runs. The option does not have a default value.

- **-renameto**
  
  Change the name of the existing policy to the new policy name.

- **-sameas**
  
  Create a new policy by copying its characteristics from the existing policy.

- **-help**
  
  Prints a command-line usage message.
Specifies a list of comma-separated master server host names. If this option is present, the command is run on each of the master servers in this list. The servers must allow access by the system that issued the command. If an error occurs, the process stops at that point in the list. The default is the master server for the system where the command is entered.

Indicates the reason why you choose this command action. The reason text string that you enter is captured and appears in the audit report. Enclose this string with double quotes ("..."). The string must not exceed 512 characters. It cannot begin with a dash character (-) nor contain a single quotation mark (').

Select verbose mode for logging. This option is meaningful only when it runs with the debug log function (that is, when the following directory is defined):

UNIX systems:
/usr/openv/netbackup/logs/admin

Windows systems:
install_path\NetBackup\logs\admin

Specifies the name of a NetBackup policy that \texttt{bppolicynew} creates or the name to which \texttt{bppolicynew} changes an existing policy. The option has no default value.

This policy name must differ from any existing policy name. It is composed of numeric, alphabetic, plus, minus, underscore, and period characters. Do not use a minus as the first character or leave spaces between characters.

The name of a NetBackup policy that already exists when \texttt{bppolicynew} runs. The option does not have a default value.

Change the name of the existing policy to the new policy name.

Create a new policy by copying its characteristics from the existing policy.

Prints a command-line usage message.
-M master_server,...

Specifies a list of comma-separated master server host names. If this option is present, the command is run on each of the master servers in this list. The servers must allow access by the system that issued the command. If an error occurs, the process stops at that point in the list. The default is the master server for the system where the command is entered.

-verbose

Select verbose mode for logging. This option is meaningful only when it runs with the debug log function (that is, when the following directory is defined):

UNIX systems:

/usr/openv/netbackup/logs/admin

Windows systems:

install_path\NetBackup\logs\admin

EXAMPLES

Note that references to Follow NFS Mounts in these examples apply only to NetBackup Enterprise Server.

Example 1 - Create a policy with default attribute values on the master server plim:

# bppolicynew ishkabibble -M plim
# bpplist ishkabibble -U -M plim

<table>
<thead>
<tr>
<th>Policy Name:</th>
<th>ishkabibble</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Type:</td>
<td>Standard</td>
</tr>
<tr>
<td>Active:</td>
<td>yes</td>
</tr>
<tr>
<td>Client Compress:</td>
<td>no</td>
</tr>
<tr>
<td>Follow NFS Mounts:</td>
<td>no</td>
</tr>
<tr>
<td>Cross Mount Points:</td>
<td>no</td>
</tr>
<tr>
<td>Collect TIR info:</td>
<td>no</td>
</tr>
<tr>
<td>Block Incremental:</td>
<td>no</td>
</tr>
<tr>
<td>Mult. Data Streams:</td>
<td>no</td>
</tr>
<tr>
<td>Client Encrypt:</td>
<td>no</td>
</tr>
<tr>
<td>Policy Priority:</td>
<td>0</td>
</tr>
<tr>
<td>Max Jobs/Policy:</td>
<td>99</td>
</tr>
<tr>
<td>Disaster Recovery:</td>
<td>0</td>
</tr>
<tr>
<td>Residence:</td>
<td>(specific storage unit not required)</td>
</tr>
<tr>
<td>Volume Pool:</td>
<td>NetBackup</td>
</tr>
<tr>
<td>Keyword:</td>
<td>(none specified)</td>
</tr>
</tbody>
</table>
Example 2 - Create new policy mypolicy_copy from the existing policy mypolicy. bpplist shows that mypolicy_copy has the same attributes as mypolicy. For brevity, most of the schedule information is omitted here:

```bash
# bppolicynew mypolicy_copy -sameas mypolicy
# bppllist mypolicy_copy -U
```

Policy Name: mypolicy_copy
Policy Type: Standard
Active: yes
Client Compress: no
Follow NFS Mounts: no
Cross Mount Points: no
Collect TIR info: no
Block Incremental: no
Mult. Data Streams: no
Client Encrypt: no
Policy Priority: 0
Max Jobs/Policy: 99
Disaster Recovery: 0
Residence: myunit
Volume Pool: NetBackup
Keyword: (none specified)

HW/OS/Client: Linux RedHat zippity

Include: /tmp/my

Schedule: full
Type: Full Backup
Frequency: every 7 days
Maximum MPX: 1
Retention Level: 0 (1 week)
Residence: (specific storage unit not required)
Volume Pool: (same as policy volume pool)
Daily Windows:
  Sunday 00:00:00 --> Sunday 08:00:00
  Monday 00:00:00 --> Monday 08:00:00
Tuesday 00:00:00 --| Tuesday 08:00:00
Wednesday 00:00:00 --| Wednesday 08:00:00
Thursday 00:00:00 --| Thursday 08:00:00
Friday 00:00:00 --| Friday 08:00:00
Saturday 00:00:00 --| Saturday 08:00:00

Schedule: incr
Type: Differential Incremental Backup

# bppolicynew mypolicy_copy -sameas mypolicy
# bpplist mypolicy -U

------------------------------------------------------------
Policy Name: mypolicy
Policy Type: Standard
Active: yes
Client Compress: no
Follow NFS Mounts: no
Cross Mount Points: no
Collect TIR info: no
Block Incremental: no
Mult. Data Streams: no
Client Encrypt: no
Policy Priority: 0
Max Jobs/Policy: 99
Disaster Recovery: 0
Residence: myunit
Volume Pool: NetBackup
Keyword: (none specified)

HW/OS/Client: Linux RedHat zippity
Include: /tmp/my

Schedule: full
Type: Full Backup
Frequency: every 7 days
Maximum MPX: 1
Retention Level: 0 (1 week)
Residence: (specific storage unit not required)
Volume Pool: (same as policy volume pool)
Daily Windows:
  Sunday 00:00:00 --| Sunday 08:00:00
  Monday 00:00:00 --| Monday 08:00:00
Tuesday 00:00:00 --> Tuesday 08:00:00
Wednesday 00:00:00 --> Wednesday 08:00:00
Thursday 00:00:00 --> Thursday 08:00:00
Friday 00:00:00 --> Friday 08:00:00
Saturday 00:00:00 --> Saturday 08:00:00

Schedule: incr
Type: Differential Incremental Backup

# bpplist mypolicy_copy -U

Policy Name: mypolicy_copy
Policy Type: Standard
Active: yes
Client Compress: no
Follow NFS Mounts: no
Cross Mount Points: no
Collect TIR info: no
Block Incremental: no
Mult. Data Streams: no
Client Encrypt: no
Policy Priority: 0
Max Jobs/Policy: 99
Disaster Recovery: 0
Residence: myunit
Volume Pool: NetBackup
Keyword: (none specified)

HW/OS/Client: Linux RedHat zippity

Include: /tmp/my

Schedule: full
Type: Full Backup
Frequency: every 7 days
Maximum MPX: 1
Retention Level: 0 (1 week)
Residence: (specific storage unit not required)
Volume Pool: (same as policy volume pool)
Daily Windows:
  Sunday 00:00:00 --> Sunday 08:00:00
  Monday 00:00:00 --> Monday 08:00:00
  Tuesday 00:00:00 --> Tuesday 08:00:00
Wednesday 00:00:00 --> Wednesday 08:00:00
Thursday 00:00:00 --> Thursday 08:00:00
Friday 00:00:00 --> Friday 08:00:00
Saturday 00:00:00 --> Saturday 08:00:00

Schedule: incr
Type: Differential Incremental Backup

Example 3 - Rename a policy from policy_old to policy_new. Before and after the renaming, `bppllist` shows the policies in the NetBackup configuration database:

```bash
bppllist
mypolicy
policy_old
test
bpplnew policy_old -renameto policy_new
bppllist
mypolicy
policy_new
test
```

RETURN VALUES

An exit status of zero (0) means that the command ran successfully.
Any exit status other than zero (0) means that an error occurred.
If the administrative log function is enabled, `bppllist` logs the exit status in the administrative daily log under the log directory:

UNIX systems:

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

Windows systems:

```
install_path\NetBackup\logs\admin
```

It has the following form:

```
bpplnew: EXIT status = exit status
```

If an error occurred, a diagnostic precedes this message.

FILES

UNIX systems:
/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/db/policy/policy_name

Windows systems:

install_path\NetBackup\logs\admin/*
install_path\NetBackup\db\policy\policy_name

SEE ALSO

See bpplclients on page 276.
See bpplinfo on page 297.
See bpplsched on page 332.
See bppldelete on page 287.
See bppllist on page 324.
bpps

bpps – list process statistics for the processes that run on your system. Be aware this command operates differently on Windows systems than it does on UNIX systems.

SYNOPSIS

bpps [-a | -x | [ [{-n}[-3}] [-f] ]] 
bpps [-l | -s | -S] [-t sample_time[m]] [-i | -x process_group] ... [host_name] ... 
install_path\NetBackup\bin\bpps -? [process_group ...]

For UNIX systems, the directory path for this command is /usr/openv/netbackup/bin/

For Windows, the directory path to this command is install_path\NetBackup\bin\bpps

DESCRIPTION

This command operates differently on Windows systems than it does on UNIX systems.

The bpps command lists the process statistics for all processes that run on your system. This command enables you to list a specific process group. It also enables you to specify a sample time in seconds (or milliseconds) before it lists the processes.

Note: The command options that bpps uses on Windows are unrelated to the options that the UNIX bpps command uses.

OPTIONS: UNIX and Linux

-3 Display all processes running from programs resident outside the NetBackup installation directories but using libraries, open files, or current working directory within the NetBackup installation directories. This option includes any currently running notify scripts.

-a Includes the Media Manager processes in the listing.
-f Display the NetBackup files and directories in use by the NetBackup (-n) or third-party (-3) processes. This option includes files either mapped into the process or currently open by the process. The option also includes any directories which are the current working directory for the process.

-n Display all processes running from programs resident within the NetBackup installation directories. Excludes notify scripts because they contain third-party commands.

-x Includes Media Manager processes and the extra shared processes such as pbx_exchange in the listing.

OPTIONS: Windows

host_name
The name of the host computer on which you list group process statistics.

-? Print the help screen. If you specify process_group here, it displays the list of processes that are included or excluded when you specify process_group with -i or -x options.

-i process_group
Include the specified process group in the listing (default NB_ALL).

-l Output a long listing.

-s Output a short listing (default).

-S Output a short listing without the header (for example, host name, date, and column headings).

-t sample_time[m]
Specify the sample time (default 1 second). The sample time is specified in seconds unless followed by \( m \), which specifies the sample time in milliseconds.

-x process_group
Exclude the specified process group from the listing.

NOTES

The following is a list of all of the valid process groups and a brief description of each:
MM_ALL
  All Media Manager processes.

MM_CLIS
  Media Manager command line programs.

MM_CORE
  Media Manager core processes.

MM_GUIS
  Media Manager GUI programs.

MM_SERVICES
  Media Manager services.

MM_UIS
  Media Manager user interface programs.

MM_WORKERS
  Media Manager worker processes.

NB_ALL
  All NetBackup, Media Manager, and ARO processes.

NB_ALL_CLIS
  All NetBackup and Media Manager command line programs.

NB_ALL_CORE
  All NetBackup, Media Manager, and ARO core processes.

NB_ALL_GUIS
  All NetBackup and Media Manager GUI programs.

NB_ALL_SERVICES
  All NetBackup and Media Manager Services.

NB_ALL_UIS
  All NetBackup and Media Manager user interface programs.

NB_ALL_WORKERS
  All NetBackup and Media Manager worker processes.

NB_CLIENT_ALL
  All NetBackup client processes.

NB_CLIENT_CLIS
  NetBackup client command line programs.

NB_CLIENT_CORE
  NetBackup client core processes.
NB_CLIENT_GUIs
    NetBackup client GUI programs.

NB_CLIENT_SERVICES
    NetBackup client services.

NB_CLIENT_UIS
    NetBackup client user interface programs.

NB_CLIENT_WORKERS
    NetBackup client worker processes.

NB_SERVER_ALL
    All NetBackup server processes.

NB_SERVER_CLIS
    NetBackup server command line programs.

NB_SERVER_CORE
    NetBackup server core processes.

NB_SERVER_GUIs
    NetBackup server GUI programs.

NB_SERVER_SERVICES
    NetBackup server services.

NB_SERVER_UIS
    NetBackup server user interface programs.

NB_SERVER_WORKERS
    NetBackup server worker processes.

NBDB_SERVICES
    NetBackup Database services.

NBDB_CLIS
    NetBackup Database command line programs.

NBDB_ALL
    All NetBackup Database processes.

VLT_CORE
    Core Vault processes.

VLT_GUIs
    Vault GUI programs.

VLT_CLIS
    Vault command line programs.
VLT_UIS

Vault user interface programs.

VLT_ALL

All Vault processes.

OTHER_PROCESSES

All processes that are not included in NB_ALL.

FILES

install_path\NetBackup\bin\bp.conf
bprd

bprd – initiate NetBackup request daemon

SYNOPSIS

bprd [-verbose]

The directory path to this command is /usr/openv/netbackup/bin/

DESCRIPTION

This command operates only on UNIX systems.

bprd is responsible for starting automatic client backups and for responding to client requests for file restores and user backups and archives. bprd runs only on the master server and can be started only by the administrator.

The following steps occur in the order listed when bprd starts:

■ After it disassociates itself from the terminal, the daemon does the following:
  ■ Logs a message that indicates it started.
  ■ Starts bpdbm (NetBackup database manager).
  ■ Verifies that no other instance of bprd is running. If another instance of bprd is found, the program terminates.
  ■ The program reads the NetBackup configuration attributes and recycles older error and debug log files. Activity and error logs are also recycled on a daily basis.
  ■ bprd determines its port number by checking the services file for an entry with a service name of bprd and a protocol name of tcp. For example:

    bprd 13720/tcp

■ After it binds to its port, the program performs the following tasks: It schedules automatic client backups, accepts requests from client computers for file restores or user backups or archives, and accepts administrative requests from the server.

You can use bprdreq -terminate to terminate bprd. If you terminate bprd, it does not terminate bpdbm.
OPTIONS

-verbose
   Specifies that the bprd command writes additional information in its daily debug log for debugging purposes.

FILES

/usr/openv/netbackup/db/*
/usr/openv/netbackup/bp.conf
/usr/openv/netbackup/logs/bprd/*
/usr/openv/netbackup/bin/initbprd
/usr/openv/netbackup/bin/initbpdbm

SEE ALSO

See bpdbm on page 115.
bprecover

bprecover – recover selected NetBackup related catalogs

SYNOPSIS

bprecover -wizard [-copy number]
bprecover -r -nbdb [-priority number] [-copy number] [-L output_file]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The bprecover command initiates the NetBackup utility for restoring the NetBackup catalogs. It recovers the catalogs that were backed up by using the procedures that are described in the NetBackup Administrator’s Guide, Volume I. Use bprecover only if catalogs were destroyed on disk.

bprecover has three modes:

- -wizard lets you recover the entire NetBackup catalog or the catalog image and configuration files by using a recovery wizard.

- NBDB recovery (-r -nbdb) lets you recover the NetBackup relational database and the BMR database, if BMR is configured.

In Windows, the NetBackup catalog backup does not back up registry entries. If you reinstall NetBackup but do not provide media server names during installation, the master server is unaware of the media servers. The bprecover command returns media servers, related storage servers, and disk pools. Because these entries are not in the registry, the backup fails. Therefore, you must provide the media server names during reinstallation, or add them manually to the registry after the reinstallation.

You must have administrator privileges to run this command.
OPTIONS

-copy number
    Specifies the number of the copy of the catalog backup image to be used for
    the recovery operation. This option restores from a non-primary copy of the
    catalog backup image.

-L output_file
    Reports the results of the recovery in the specified output file.

-nbdb
    Used with the -r option during catalog recovery to recover and resynchronize
    the NetBackup relational databases (NBDBs) and the BMR database (BMRDB),
    if BMR is configured.

    For complete catalog recovery procedures, see the NetBackup Troubleshooting
    Guide.

-priority number
    Recovers the NetBackup relational database when used with -nbdb.

-r
    Recovers the images from the specified policy name.

-wizard
    Enables a user to perform the same functions from a command line that are
    present on the recovery wizard. For example, a user can specify the full
    pathname to the catalog disaster recovery file or recover the entire NetBackup
    catalog. The wizard prompts you for the catalog disaster recovery file.

    The -copy option lets you select the number of the copy

---

Note: The operator must be logged on locally to the master server that is to be recovered.

EXEMPLES

Example 1 - Recover the entire NetBackup catalog or the catalog image and
configuration files. On Windows, a series of screens takes you through the recovery
process. On UNIX, a series of prompts takes you through the recovery process.

    # bprecover -wizard

    The disaster recovery information in the NetBackup Troubleshooting Guide describes
each step of the recovery process.
Example 2 - Recover the NetBackup relational databases and reports the results of the recovery in the `recovery.rpt` file.

```bash
# bprecover -r -nbdb -L recovery.rpt
```

**ERRORS**

If any errors occur during the recover operation, NetBackup writes error messages to one of the following: `stderr` (UNIX systems) or the MS-DOS command window when you run the `bprecover` command (Windows systems).

Also, debug logs are accumulated in the following directory path:

- **On Windows**, `install_path\NetBackup\logs\admin`
- **On UNIX**, `/usr/openv/netbackup/logs/admin`

**SEE ALSO**

*NetBackup Troubleshooting Guide* for information on disaster recovery.
bprestore

bprestore – restore files from NetBackup Server

SYNOPSIS


On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\n
DESCRIPTION

bprestore lets users restore a backed up or archived file or list of files. You can also name directories to restore. If you include a directory name, bprestore restores all files and subdirectories of that directory. You can exclude a file or a directory path that was previously included in the restore by placing an exclamation mark (!) in front of the file or the directory path (does not apply to NDMP restores). For example, the exclude capability is useful if you want to exclude part of a directory from the restore.

Note: If a policy or date range is not specified, bprestore starts with the most recent full backup image. It includes all subsequent incremental and differential backup images. The most recent copy of a file is restored from these images.
By default, you are returned to the system prompt after `bprestore` is successfully submitted. The command works in the background and does not return completion status directly to you. The `-w` option lets you change this behavior so `bprestore` works in the foreground and then returns completion status after a specified time period.

The `bprestore` command restores the file from the most recent backups within the time period you specify, except for a true-image restore. (See the `-T` option description.)

`bprestore` overwrites any file of the same name that already exists on the local client disk, unless you include the `-K` option. You also can restore the files that were backed up or archived on another client (`-C` option). To restore from other clients, the NetBackup administrator must validate you.

`bprestore` writes informative and error messages to a progress log file if you do the following: create the file before you run the `bprestore` command and then specify the file with the `-L progress_log` option. If `bprestore` cannot restore the requested files or directories, you can use the progress log to find the reason for the failure.

For detailed troubleshooting information, create a directory that is named `/usr/openv/netbackup/logs/bprestore` (UNIX systems) or `install_path\NetBackup\logs\bprestore` (Windows systems) with public-write access. `bprestore` then creates a debug log file in this directory.

For UNIX systems, if a nonroot user specifies `USEMAIL = mail_address` in the `$HOME/bp.conf` file, the following occurs: NetBackup sends mail on the restore completion status to `mail_address`. This message is sent when the restore process is complete.

The following restrictions apply to `bprestore`:

- You can restore the files and the directories that you own and those owned by other users if you have read access. You need write access to another user’s directories and files to restore that user’s files to their original location.

- The operating system restricts the number of files and directories that you can specify on a single `bprestore` command line. If this restriction is a problem, use the `-f` option to restore the files.

- When you use `bprestore` on a Windows computer, if the file names contain non-ASCII characters, the acceptable format for the file names depends on the policy type. For the policy types listed, you must give the file list in the Windows code page format:

  ```
  DB2
  MS-Exchange-Server
  ```
Informix
Lotus-Notes
Oracle
SAP
MS-SQL-Server
Sybase
TeraData
MS-Windows
Standard

For all other policy types, the file list must be given in UTF-8 format. The rule applies for the file lists that are given on the command line and file lists that are provided in a file with the \-f option.

Use the bplist command to display information on the files and directories that were backed up or archived.

**Note:** If you restore catalog files directly by using `bprestore` on a Solaris system, use the following path: `/opt/openv/netbackup/bin/bprestore`.

## OPTIONS

---

**\-A | \-B | \-rb**

Specifies if data is to be restored from archives (\-A), backups (\-B), or snapshot rollbacks (\-rb). The default is \-B.

**Note:** The rollback (\-rb) operation always occurs from copy 1. If copy 1 is expired, the rollback fails.

---

**\-BR portal_name | teamsite_name | Exchange_2010_redirected_path**

Specifies a portal name, team site name, or Exchange 2010 redirected path name where the selected portal or team site is to be redirected in a SharePoint farm. A user should specify the redirected portal or team site as http://portalname | http://teamsitename, and should already exist in a farm.

---

**\-C client**

Specifies a client name to use for finding backups or archives from which to restore files. This name must be as it appears in the NetBackup catalog. The default is the current client name.
Note: The destination client does not default to the source client. See the description for -D client option.

-cm
Enables the restore operation to play through log files and roll back any incompleted transactions. Use this option if your selection contains the last backup to be restored. If this option is not selected, the database is left in an intermediate state and is not yet usable.

-copy copy_number
Specifies the copy number to restore from. The user is able to restore from a different copy than the primary copy. For example, -copy 3 restores copy 3 of a file or list of files.

Alternatively, you may specify the copy from which to restore at a global level (for all restore operations). Put the copy number into the file ALT_RESTORE_COPY_NUMBER.

Refer to "Restoring from a specific backup copy" of the NetBackup Backup, Archive, and Restore online Help for a complete description.

-D client
Specifies a destination client. The default is the current client name.

On UNIX systems, the master server root user can use this option to do the following: Direct restored files to a computer other than the client that the -C option specifies.

On Windows systems, the master server administrator can use this option to do the following: Direct restored files to a computer other than the client that the -C option specifies.

-disk_media_server media_server
Identifies the disk media server to be used for the restore operation. The default server is the one currently being used.

-drs
Restores the files without access-control attributes. By default, access-control attributes are restored along with file and directory data. Option -drs is available only to NetBackup administrators.

-ev_migrated_data
Restores the migrated data from Enterprise Vault. bprestore -ev_migrated_data does not support the restoration of migrated data from a non-Enterprise Vault source. Use the other bprestore parameters as required.
The following example restores migrated data from Vault1 to master server ms1 using an NDMP policy type. The files to be restored are listed in file restorefiles.

```
# bprestore -S ms1 -C Vault1 -t 19 -ev_migrated_data restorefiles
```

`-f listfile`

Specifies a file (listfile) that contains a list of files to be restored and can be used instead of the filenames option. In listfile, list each file path must be on a separate line.

The required format for the file list depends on whether the files have spaces or newlines in the names.

To restore the files that do not have spaces or newlines in the names, use this format:

```
filepath
```

Where `filepath` is the path to the file that you restore. For example:

**Note:** For Windows systems, use upper case for the drive letter. For example, C:\NetBackup\Log1.

UNIX systems:

```
/home
/etc
/var
```

Windows systems:

```
C:\programs
C:\winnt
C:\documents\old_memos
```

To restore the files that have spaces or newlines in the names, use one of the following formats:

```
filepathlen filepath
filepathlen filepath start_date_time end_date_time
filepathlen filepath -s datetime -e datetime
```

The `filepath` is the path to the file you restore.

The `filepathlen` is the total number of characters in the file path.
The `start_date_time` and `end_date_time` are the decimal number of seconds since 01/01/1970 00:00:00.

`datetime` is the same as the command line (`mm/dd/yy [hh:mm:ss]`). The command uses the start date, end date, and time from the command line unless a line in `listfile` overrides it. The dates may change from line to line.

The required date and time values format in NetBackup commands varies according to your locale. The `/usr/openv/msg/.conf` file (UNIX) and the `install_path\VERITAS\msg\LC.CONF` file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

See "About specifying the locale of the NetBackup installation" in the *NetBackup Administrator's Guide, Volume II*.

To exclude a file or a directory path that was previously included in the restore, place an exclamation mark (!) in front of the file or the directory path. NDMP and FlashBackup restores do not support the exclude option.

The following is an example that uses `filepathlenfilepath`:

**UNIX systems:**

5 /home
4 /etc
4 /var
19 /home/abc/test file
12 !/etc/passwd

**Windows systems:**

11 C:\programs
8 C:\winnt
22 C:\documents\old memos
17 !C:\programs\test

- `-f filenames`

Names one or more files to be restored and can be used instead of the `-f` option.

Any files that you specify must be listed at the end of the command line after all other options. You must use absolute file paths.

To exclude a file or a directory path that was previously included in the restore, place an exclamation mark (!) in front of the file or the directory path. NDMP and FlashBackup restores do not support the exclude option.
For Windows systems, use upper case for the drive letter. For example, 
C:\NetBackup\log1.

- **F** file_options
  Allows NetBackup files to be restored.

- **granular_restore**
  Enables the restore of the objects and attributes in the Active Directory. If this 
  option is not specified, the restore still runs, but the backup cannot produce 
  granular restores.

- **J**
  If specified, newer snapshots on the volume may be lost. This option is used 
  only with the rollback restore (-rb) option.

- **K**
  Causes bprestore to keep existing files rather than overwrite them when it 
  restores files with the same name. The default condition is to overwrite existing 
  files.

  When you use -K with the rollback (-rb) option, it means to not perform 
  verification before the rollback. Files that are added on the volume after the 
  snapshot is taken would be lost.

- **k "keyword_phrase"**
  Specifies a keyword phrase for NetBackup to use when it searches for backups 
  or archives from which to restore files. The phrase must match the one that 
  was previously associated with backup or archive by the -k option of the 
  bpbackup or the bparchive command.

  Use this option in place of or in combination with the other restore options to 
  more easily restore your backups and archives. The meta-characters that follow 
  simplify the match of keywords or parts of keywords in the phrase:

  * matches any string of characters.

  The "?" character matches any single character.

  [ ] matches one of the sequence of characters that is specified within the 
  brackets.

  [ - ] matches one of the range of characters that the ",-" separates.

  The keyword phrase can be up to 128 characters in length. All printable 
  characters are permitted including space (" ") and period (".").

  The phrase must be enclosed in double quotes ("...") or single quotes (‘...’).

  The default keyword phrase is the null (empty) string.
-L progress_log [-en]
  Specifies the name of an existing file in which to write progress information.
  For example:

  **UNIX systems**: netbackup/logs/user_ops/proglog

  **Windows systems**: NetBackup\logs\user_ops\proglog

  The default is not to use a progress log.

  Include the **-en** option to generate a log entry in English. The name of the log
  contains the string _en. This option is useful to support any personnel that
  assist in a distributed environment where different locales may create logs of
  various languages.

  Only default paths are allowed for this option and Veritas recommends to use
  the default paths. If you cannot use the NetBackup default path in your setup,
  you should add custom paths to the NetBackup configuration.

  For more information on how to add a custom path, see the
  “BPCD_WHITELIST_PATH option for NetBackup servers and clients” topic in
  the NetBackup Administrator’s Guide, Volume I.

-1 | -H | -y

  **Note**: The -1 | -H | -y options apply only when you restore UNIX files to a
  UNIX system.

  Specify -l to rename the targets of UNIX links by using the -R rename_file
  option in the same way as when you rename files.

  Specify -H to rename UNIX hard links by using the -R rename_file option in
  the same way as when you rename files. Soft links are unchanged.

  Specify -y to rename UNIX soft links by using the -R rename_file option in
  the same way as when you rename files. Hard links are unchanged.

  See Example 5 in the EXAMPLES section.

-M
  Enables the client job to be monitored.

-md
  Mounts the database so that it is available to users. This option is only available
  if **Commit after restore completes** is selected.

-optimized_backup 0 | 1
  Specifies if the restore operation is done from an optimized backup.
-p policy
  Specifies the policy for which the backups or archives were performed.

-print_jobid
  Display to the stdout the job ID of the restore job that the bprestore command initiates.

-r
  Specify this option to restore raw partitions (UNIX systems) or disk images (Windows systems) instead of file systems.

-R rename_file
  Specifies the name of a file with name changes for alternate-path restores.

  For example: bprestore -R /C/renamefile /C/origfile

  Where /C/rename_file is the file with the name change and /C/origfile is the file to be renamed. The pathname that you enter must be an absolute path.

  Use the following form for entries in the rename file:

  change backup_filepath to restore_filepath

  The file paths must start with / (slash)

  The first backup_filepath that is matched is replaced with the restore_filepath string.

  The default is to restore by using the original path.

  On UNIX systems: For example, the following entry renames /usr/fred to /usr/fred2:

  change /usr/fred to /usr/fred2

  On Windows systems: For example, the following entry renames C:\users\fred to C:\users\fred2:

  change /C/users/fred to /C/users/fred2

  Use all upper case for the drive letter and end the entry with a return.

  When you restore to a Windows client, you can also use the following method for specifying entries in the rename file. (Do not use this method for other clients.)

  rename bulength backup_filepath reslength restore_filepath

  Where:
bulength is the number of ASCII characters in the backup path.
reslength is the number of ASCII characters in the restore path.
The first backup_filepath that is matched is replaced with the restore_filepath string.
For example, the following entry renames C:\fred.txt to C:\fred2.txt:

rename 11 /C/fred.txt 12 /C/fred2.txt
(Be sure to end the entry with a return.)

Only default paths are allowed for this option and Veritas recommends to use the default paths. If you cannot use the NetBackup default path in your setup, you should add custom paths to the NetBackup configuration.

For more information on how to add a custom path, see the “BPCD_WHITELIST_PATH option for NetBackup servers and clients” topic in the NetBackup Administrator's Guide, Volume I.

-s date, -e date
Specifies the start and the end date range for the listing. The bprestore command restores only files from backups or the archives that occurred within the specified start and end date range.

-s specifies a start date and time for the restore window. bprestore restores files only from the backups or the archives that occurred at or after the specified date and time.

Note: To restore multistreamed images, first run bplist -1 to get the modification time of the desired files during the last backup that contained the files. Specify that date as the -s when you run the bprestore command. If you specify no start or no end date for the files that have been backed using multiple data streams, errors may result.

The required date and time values format in NetBackup commands varies according to your locale. The /usr/openv/msg/.conf file (UNIX) and the install_path\VERITAS\msg\LC.CONF file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

More information is available about the locale of your system.

See "About specifying the locale of the NetBackup installation" in the NetBackup Administrator's Guide, Volume II.
The valid range of dates is from 01/01/1970 00:00:00 to 01/19/2038 03:14:07. The default start date is 01/01/1970 00:00:00.

The default is to return the most recent image. For backups, this image is the most recent full backup if a full backup exists. If a full backup does not exist, then the most recent incremental or user-directed backup is restored.

--e specifies an end date and time for the restore window. bprestore restores only files in the backups or the archives that occurred at or before the specified date and time. Use the same format as for the start date and time.

The end backup date and time do not need to be exact, except for a true-image restore (see the –T option description). bprestore restores the file that has the specified backup date and time. Or it restores the file that precedes the end date and time, which is the most recent backup. The default is the current date and time.

-S master_server

Specifies the name of the NetBackup server.

On UNIX systems, the default is the first server found in the /usr/openv/netbackup/bp.conf file.

On Windows systems, the default is the server designated as current on the Servers tab of the Specify NetBackup Machines dialog box. To display this dialog box, start the Backup, Archive, and Restore user interface on the client. Then click Specify NetBackup Machines on the File menu.

-spscurver

For SharePoint operation, -spscurver restores only the most recent version of an item.

-spsignorelock

For SharePoint operation, -spsignorelock releases the lock on the SharePoint farm topology, if it is set.

-spspreserveiis

For SharePoint operation, -spspreserveiis preserves the existing Internet Information Services (IIS) website and application pool.

-sparedir_server hostname

For SharePoint operation, this option specifies the web server on which the redirected portal or team site resides in a SharePoint farm. The redirected web server should be specified as hostname.

-spsrestoresecurity

For SharePoint operation, -spsrestoresecurity includes security information in the restore operation.
-spsverkeep 0 | 1 | 2
   For SharePoint operation, -spsverkeep specifies if versioning is enabled on the restore destination.

-t policy_type
   Specifies one of the following numbers that corresponds to the policy type. The default is 0 for all clients except Windows, where the default is 13.
   0 = Standard
   8 = MS-SharePoint
   13 = MS-Windows
   16 = MS-Exchange-Server
   19 = NDMP
   20 = FlashBackup
   21 = Split-Mirror
   25 = Lotus-Notes
   29 = FlashBackup-Windows
   30 = Vault
   35 = NBU-Catalog
   38 = PureDisk-Export
   39 = Enterprise-Vault
   40 = VMware
   41 = Hyper-V
   44 = BigData

-T
   Specifies a true-image restore, where only the files and the directories that existed in the last true-image backup are restored. This option is useful only if true-image backups were performed. If this option is not specified, all files and directories that meet the specified criteria are restored, even if they were deleted.

   When the -T option is specified, the image that is requested must be uniquely identified. Unique identification is accomplished by using the -e option with seconds granularity. The -s option (if any) is ignored. The seconds granularity of an image can be retrieved by using the bplist command with the -l and -Listseconds options.
-td temp_dir
   This option provides a location where the associated log and any patch files are to be kept until the database is restored. If storage groups are restored, a subdirectory in temp_dir is created for each storage group. The log and patch files for each storage group are kept in the corresponding subdirectory.
   
   On UNIX systems, the default location is /temp.
   On Windows systems, the default location is C: \temp.

-vhd_dof 0 | 1
   For Hyper-V operation, -vhd_dof specifies whether or not to delete on any failure. Possible values are 1 (delete on failure) and 0 (do not delete on failure).

-vhd_dsize VHD_disk_size
   For Hyper-V operation, -vhd_dsize specifies the size of the VHD file to be recovered.

-vhd_fn VHD_filename
   For Hyper-V operation, -vhd_fn specifies the name of the VHD file to be recovered.

-vhd_type 0 | 1
   For Hyper-V operation, -vhd_type specifies the type of the VHD file. Possible values for this option are the following:
   1 - Fixed.
   2 - Dynamic.

-w [hh:mm:ss]
   Causes NetBackup to wait for a completion status from the server before it returns you to the system prompt.

   The required date and time values format in NetBackup commands varies according to your locale. The /usr/openv/msg/.conf file (UNIX) and the install_path\VERITAS\msg\LC.CONF file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

   More information is available about the locale of your system.

   See "About specifying the locale of the NetBackup installation" in the NetBackup Administrator's Guide, Volume II.

   You can optionally specify a wait time in hours, minutes, and seconds. The maximum wait time you can specify is 23:59:59. If the wait time expires before the restore is complete, the command exits with a timeout status. The restore, however, still completes on the server.
If you specify 0 or do not specify a time, the wait time is indefinite for the completion status.

EXAMPLES

Example 1 - Restore files from backups of file1 that were performed between 04/01/2010 06:00:00 and 04/10/2010 18:00:00. Enter the following:

UNIX systems:

# bprestore -s 04/01/2010 06:00:00 -e 04/10/2010 18:00:00 /usr/user1/file1

Windows systems:

# bprestore -s 04/01/2010 06:00:00 -e 04/10/2010 18:00:00 C:\user1\file1

Example 2 - Restore the files that are listed in a file named restore_list by using the most recent backups, enter the following:

UNIX systems:

# bprestore -f restore_list

Windows systems:

# bprestore -f c:\restore_list

Example 3

UNIX systems:

Restore directory /home/kwc from the backups that are associated with a keyword phrase that contains "My Home Directory". Use a progress log named /usr/openv/netbackup/logs/user_op/bkup.log. Enter the following on one line:

# bprestore -k "*My Home Directory*" -L /usr/openv/netbackup/logs/user_op/bkup.log /home/kwc

Windows systems:

Restore directory C:\kwc from the backups that are associated with a keyword phrase that contains "My Home Directory". Use a progress log named c:\Program Files\Veritas\NetBackup\logs\user_ops\bkup.log. Enter the following on one line:

# bprestore -k "*My Home Directory*" -L c:\Program Files\Veritas\NetBackup\logs\user_ops\bkup.log C:\kwc
Example 4 - Restore the D drive on the Windows client slater from the backups that are associated with a keyword phrase that contains "My Home Dir". Use a progress log named bkup.log. Enter the following all on one line or use the backslash continuation character:

UNIX systems:

```
# bprestore -k "*My Home Dir*" -C slater
-D slater -t 13
-L /usr/openv/netbackup/logs/user_op/bkup.log /D
```

Windows systems:

```
# bprestore -k "*My Home Dir*" -C slater -D slater 
-t 13
-L c:\Program Files\Veritas\NetBackup\logs\user_ops\bkup.log D:
```

Example 5 - Assume that you have a rename file named /usr/openv/netbackup/logs/user_ops/rename on a UNIX client and it contains the following:

```
change /home/kwc/linkback to /home/kwc/linkback_alt
```

To restore the hard link that is named /home/kwc/linkback to alternate path /home/kwc/linkback_alt on that client, run the following command:

```
# bprestore -H -R
/usr/openv/netbackup/logs/user_ops/rename
/home/kwc/linkback
```

Example 6 - Assume that you want to restore files from backups of the file user1. The backups were performed between 04/01/12 06:00:00 and 04/10/12 18:00:00. You also want to exclude all files with a .pdf extension, except for the file named final_doc.pdf. To perform this operation, run the following (on one line):

UNIX systems:

```
# bprestore -s 04/01/12 06:00:00 -e 04/10/12 18:00:00
/home/user1 !/home/user1/*.pdf /home/user1/final_doc.pdf
```

Windows systems:

```
# bprestore -s 04/01/12 06:00:00 -e 04/10/12 18:00:00
C:\user1 \ !C:\user1\*.pdf C:\user1\final_doc.pdf
```
FILES

UNIX systems:

$HOME/bp.conf
/usr/openv/netbackup/logs/bprestore/log.mmddyy

Windows systems:

install_path\NetBackup\logs\bprestore\*.*.log

SEE ALSO

See bp on page 49.
See bparestore on page 51.
See bplist on page 215.
bpretlevel

bpretlevel – display or change the values of the retention levels on the master server

SYNOPSIS

bpretlevel [-s | -l | -L | -U] [-M master_server,...]

bpretlevel (-r level period) | -d [-M master_server,...]

On UNIX and Linux systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

bpretlevel sets or changes time periods for each of the 100 retention levels and lists the current settings for levels. The time period can be specified in hours, days, weeks, months, or years. Retention levels 9 and 25 cannot be edited by the user.

The default periods for the retention values are as follows:

- 0 (1 week)
- 1 (2 weeks)
- 2 (3 weeks)
- 3 (1 month)
- 4 (2 months)
- 5 (3 months)
- 6 (6 months)
- 7 (9 months)
- 8 (1 year)
- 9-100 (infinite, except 25 which is expire immediately)

Note: If you run this command on a pre-NetBackup 8.0 media server, you can only specify a retention level between 0 and 24.
OPTIONS

-s | -l | -L | -U

Specifies what information is listed and how the information is formatted in the output. The possible values are the following:

- **-s** is the short listing which contains the retention level, retention period, and equivalent days. **-s** is the default value.
- **-l** is the condensed listing which contains the retention level, number of seconds, and period with no headings or formatting.
- **-L** is the long listing which contains the retention level, equivalent days, retention in seconds, and retention period.
- **-U** is the user listing which contains the level, number of days, and label of the retention period.

master_server

Specifies the master server whose job retention levels are to be reported or changed.

-d

Restores default retention periods for all retention levels. See the default values listed in the Description.

-r level period

Changes the retention period for a specified retention level. You can edit all retention levels (**level**) except 9 and 25. Levels 9-100 are set to infinity, except 25 which is set to expire immediately. The retention period (**period**) can be specified in days, weeks, months, years, or infinity (no limit). Include a space between the value and the units. For example, 3 d.

**Note:** If you run this command on a pre-NetBackup 8.0 media server, you can only specify a retention level between 0 and 24.

Enter the retention period in any of the following ways:

- **#hours:** hour | hours | h
  
  For example, four hours can be represented by 4 h.

- **#days:** day | days | d

  For example, four days can be represented by 4 d.

- **#weeks:** week | weeks | w

  For example, eight weeks can be represented by 8 week.

- **#months:** month | months | m
For example, one month can be represented by 1 m.

- **#years**: year | years | y
  For example, one year can be represented by 1 years.

- **infinite**: infinity | i

**EXAMPLE**

Example - Change the retention period of retention level 2 from its default value of three (3) weeks to five (5) weeks.

```
orbitervm1 # bpretlevel -r 2 5 w
```

**SEE ALSO**

See **bpduplicate** on page 121.
See **bpimagelist** on page 171.
See **bpimmedia** on page 180.
See **bpmedialist** on page 227.
See **bpplsched** on page 332.
See **bpplschedrep** on page 350.
See **nbstl** on page 845.
bpschedule

bpschedule – add, delete, or list disk staging storage unit (DSSU) schedules

SYNOPSIS

```
bpschedule [-v] [-M master_server,...] -add sched_label [-freq frequency] [-stage_priority number] [-altreadhost hostname] [-number_copies number] [-residence storage_unit_label [,stunit-copy2,...]] [-pool volume_pool_label [,pool-copy2,...]] [-fail_on_error 0|1[,...0|1] [-window start_duration]] [-cal 0|1|2] [-ut] [-incl mm/dd/yyyy] [-excl mm/dd/yyyy] [-weekday day_name week [day_name week]...] [-dayomonth 1-31 [1-31]... | 1] [-xweekday day_name week [day_name week]...] [-xdayomonth 1-31 [1-31]... | 1]
```

```
bpschedule [-v] [-M master_server,...] -delete sched_label...
```

```
bpschedule [-v] [-M master_server,...] -deleteall
```

```
bpschedule [-v] [-M master_server,...] [-L | -l | -U] [-label sched_label]
```

On UNIX systems, the directory path to this command is `/usr/openv/netbackup/bin/admincmd/`

On Windows systems, the directory path to this command is `install_path\NetBackup\bin\admincmd`

DESCRIPTION

The bpschedule command does the following:

- Adds a new disk staging storage unit (DSSU) schedule.
- Deletes one or more DSSU schedules.
- Deletes all the DSSU schedules.
- Lists one or all DSSU schedules (default is list all DSSU schedules).

For the -add and -delete options, bpschedule returns to the system prompt immediately after it submits the DSSU schedule change request to NetBackup. To determine whether the change was successful, run bpschedule again to list the updated schedule information.
The list option displays a single entry for each schedule, even if the -M option is used. The -l form lists the information for each schedule on several lines. -l does not identify the attributes by name; these are as follows (where the names are not described, they are reserved for internal NetBackup use):

Line 1: SCHED, schedule name, type, max_mpx, frequency, retention level, u_wind/o/d, two internal attributes, maximum fragment size, calendar, number of copies, and fail on error. Note that u_wind/o/d is a field reserved for future use. The u_wind entry in the -L display is also reserved for future use.

Line 2: SCHEDWIN, seven pairs of the form start,duration, expresses the start and duration of the window for each day of the week. The week starts with Sunday.

Line 3: SCHEDRES, residence (a value for each copy).

Line 4: SCHEDPOOL, pool (a value for each copy).

Line 5: SCHEDRL, retention level (a value for each copy).

Line 6: SCHEDFOE, fail on error (a value for each copy).

If the -M option is used, bpschedule performs the operation on each of the listed master servers. For instance, if bpschedule adds a schedule, bpschedule adds the schedule to the policy on each of the listed master servers for -M. If -M is used on a listing request, the listing is composed of the returned information from all the master servers in the -M list. If the command fails for any of the master servers, activity stops at that point.

To modify an existing NetBackup schedule, use the NetBackup command bpschedulerep.

Any authorized user can initiate this command.

For more about NetBackup authorization, see the NetBackup Security and Encryption Guide.

OPTIONS

These options are common to all forms of bpschedule:

-M master_server,...

Specifies a list of alternative master servers. This list is a comma-separated list of host names. If this option is present, each master server in the list runs the bpschedule command. Each master server in the list must allow access by the system that issues the bpschedule command.

If this option is present, the command is run on each master server in the list. If an error occurs for any master server, the process terminates at that point.
If `bpschedule` produces a listing, the listing is the composite of the returned information from all the master servers in this list.

If `bpschedule` adds or deletes a schedule, all master servers in this list receive the change.

`-v`

Selects the verbose mode where `bpschedule` logs additional information for debugging purposes. The information goes into the NetBackup administration debug log. This option is meaningful only when NetBackup enables the debug log function (that is, when the following directory is defined):

UNIX systems:

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

Windows systems:

```
install_path\NetBackup\logs\admin
```

The remaining options depend on the form of `bpschedule`. The first form of `bpschedule` adds a schedule to the specified storage unit name. The following options apply to this form of `bpschedule`:

```
-add sched_label [suboptions]
```

Adds a single schedule to the specified storage unit name. The following describes the suboptions for the `-add` option. These are attributes of the schedule being added.

```
-cal 0|1|2
```

Indicates whether `bpschedule` follows a calendar-based schedule or a frequency-based schedule.

0 = frequency-based schedule

1 = calendar-based schedule with no retries after run day

2 = calendar-based schedule with retries after run day

```
-dayomonth 1-31 [1-31]... | l
```

Specifies the day or days of every month to run the schedule. Enter l (lowercase L) to run the last day of every month, whether the month contains 28, 29, 30, or 31 days.

For example, to run the policy backup on the 14th day and the 28th day of every month, enter the following:

```
-dayomonth 14 28
```

To run the last day of every month, enter:
-dayomonth 1

-excl mm/dd/yyyy
   Indicates to exclude this single date.

-fail_on_error 0|1[,0|1,...,0|1]
   Specifies whether to fail all other copies if one copy fails. If no parameter is
   specified, 0 is default for all copies. Specify a value for each copy.
   
   0 = Do not fail the other copies
   1 = Fail other copies

-freq frequency
   Determines how often backups run. Represents the number of seconds between
   the backups that are initiated according to this schedule. Valid range for this
   option is 0 through 2419200 (number of seconds in four weeks). When this
   value is omitted on the command line, the default value is 604800 (duration of
   one week in seconds).

-incl mm/dd/yyyy
   Indicates to include this single date.

-number_copies number
   Specify the number of simultaneous backup copies. The valid value range is
   1-4. The default is 1.

-pool volume_pool_label[,,pool-copy2,...]
   The name of the volume pool. This choice overrides the policy-level volume
   pool. The value "*NULL*" causes NetBackup to use the volume pool that is
   specified at the policy level. The default is to use the volume pool that is
   specified at the policy level. The volume pool label cannot be None. If you do
   not specify a volume pool at either the schedule level or the policy level,
   NetBackup uses a default value of NetBackup.

   When you specify -number_copies greater than 1, specify a pool for each
   copy.

-residence storage_unit_label [,stunit-copy2,...]
   The name of the storage unit, which specifies the location of the backup images.
   The value "*NULL*" causes NetBackup to use the storage unit that is specified
   at the policy level. The default is for NetBackup to use the storage unit that is
   specified at the policy level. If you do not specify a storage unit at either the
   schedule level or the policy level, NetBackup uses the next storage unit
   available.

   When you specify -number_copies greater than 1, specify a residence for
   each copy.
-stage_priority number
The order in which storage units are to be selected within a storage unit group:
1 = Use the storage units in the order that appears in the storage unit group
dialog box (default).
2 = Use the storage unit least recently used. (The storage units take turns.)
3 = Use the first storage unit in the list that is not full or down. If the storage
unit is only busy, the policy waits to write to it.

-altreadhost hostname
The server to be used to read a backup image that a different media server
originally wrote.

-ut
If any of the date or the time arguments follow -ut, they are accepted as UNIX
time, instead of the standard time format. The -ut option is used primarily for
Java.

-weekday day_name week [day_name week]...
Specifies a day of the week, and the week of the month, as a run day in the
schedule.
- The day_name is: Sunday, Monday, Tuesday, Wednesday, Thursday,
  Friday, or Saturday.
- The week is the number of the week in the month. A week begins on Sunday
  and ends on Saturday. Valid values are 1-5.

For example, to instruct the policy to run every Sunday of the month, enter:

-weekday Sunday 1 Sunday 2 Sunday 3 Sunday 4 Sunday 5

-window start_duration
Specifies when NetBackup can run the backups for this schedule. Every day
of the week has the same window.

- start is the time at which the backup window opens for this schedule. This
  number is the number of seconds since midnight. This number is an integer
  between 0 and 86399 (86400 seconds in a day).

- duration is the length of time that the window remains open. The time unit is
  seconds. This number is a non-negative integer.

-xdayomonth 1-31 [1-31]... | l
Specifies the day or days of the month that you want to exclude as run days
in the schedule. Use l (lowercase L) to indicate the last day of the month.
For example, to instruct the policy to not run on the 14th and 15th of the month, enter:

-xdayomonth 14 15

-xweekday day_name week [day_name week]...

Specifies the day of the week and week of the month, to exclude as a run day in the schedule.

- The day_name is: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday.
- The week is the number of the week in the month.
- Use 1 to indicate the last week of the month. The week of the month starts on Sunday and ends on Monday. Valid values are 1-5.

For example, to instruct the policy to not run on the first and third Mondays of the month, enter:

-xweekday Monday 1 Monday 3

The second form of bpschedule deletes one or more schedules from the named policy. The following option applies to this form of bpschedule:

-delete sched_label

Deletes the listed schedules from the named policy. Separate the elements of the sched_label list with spaces. There can be up to 25 labels in the list.

The third form of bpschedule deletes all schedule from the named policy. The following option applies to this form of bpschedule:

-deleteall

Deletes all schedules from the named policy.

The fourth form of bpschedule produces a listing of information about the schedules for the named policy. The following options apply to this form of bpschedule:

-l

The list type is short. This list is the default list type. This option produces a terse listing that includes all attributes for the schedule. Each schedule occupies one line of the listing. Most attribute values are expressed numerically. This option is useful for scripts or the programs that rework the listing contents into a customized report format.

-L

The list type is long. This listing includes all attributes for the schedule. Some attribute values are descriptive terms, rather than numbers.
-label sched_label

List the attributes for this schedule in the named policy. The default is to list information for all schedules for the named policy.

-U The list type is user. This listing is similar to the long-type list, but it has fewer entries. Most attribute values are descriptive terms, rather than numbers.

EXAMPLE

List the information for schedule test in long form.

# bpschedule -L -label test

Schedule: test
Type: FULL (0)
Frequency: 7day(s) (604800 seconds)
Retention Level: 1 (2 weeks)
u-wind/o/d: 0 0
Incr Type: DELTA (0)
Incr Depends: (none defined)
Max Frag Size: 0 MB (1048576 MB)
Maximum MPX: 1
Number copies: 1
Fail on Error: 0
Residence: (specific storage unit not required)
Volume Pool: (same as policy volume pool)
Daily Windows:

<table>
<thead>
<tr>
<th>Day</th>
<th>Open</th>
<th>Close</th>
<th>W-Open</th>
<th>W-Close</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sunday</td>
<td>00:00:00</td>
<td>00:00:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monday</td>
<td>00:00:00</td>
<td>00:00:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tuesday</td>
<td>00:00:00</td>
<td>00:00:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wednesday</td>
<td>00:00:00</td>
<td>00:00:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thursday</td>
<td>00:00:00</td>
<td>00:00:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Friday</td>
<td>00:00:00</td>
<td>00:00:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Saturday</td>
<td>00:00:00</td>
<td>00:00:00</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

FILES

UNIX systems:

/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/db/sched/schedule name

Windows systems:
install_path\NetBackup\logs\admin\*
install_path\NetBackup\db\sched\schedule name

SEE ALSO

See bpschedulerep on page 409.
bpschedulerep

bpschedulerep – modify attributes of disk staging storage unit (DSSU) schedule

SYNOPSIS

bpschedulerep sched_label [ -M master_server,...] [-v] [-freq backup_frequency] [-stage_priority number] [-altreadhost hostname] [-cal 0|1|2] [-incl mm/dd/yyyy] [-excl mm/dd/yyyy] [-delincl mm/dd/yyyy] [-delexcl mm/dd/yyyy] [-weekday day_name week [day_name week]...] [-dayomonth 1-31 [1-31]... | 1] [-xweekday day_name week [day_name week]...] [-xdayomonth 1-31 [1-31]... | 1] [-deldayomonth 1-31 [1-31]... | 1] [-delweekday day_name week [day_name week]...] [-ci] [-ce] [-cw] [-cd] [-number_copies number] [-fail_on_error 0|1[,0|1,...,0|1]] [-residence storage_unit_label [,stunit-copy2,...]] [-pool volume_pool_label [,pool-copy2,...]] [-(0..6) start duration]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

bpschedulerep changes the attributes of a NetBackup disk staging storage unit (DSSU) schedule. The schedule that bpschedulerep named should already exist when this command is run. bpschedulerep changes the schedule on each of the master servers that are listed, if the -M option is used.

Any authorized user can initiate this command.

For more about NetBackup authorization, see the NetBackup Security and Encryption Guide.

OPTIONS

-(0..6) start duration

Specifies the window during which NetBackup can run the backups for this schedule. This window applies to a specific day of the week. 0 corresponds to Sunday, 1 to Monday, and so on.
start is the time at which the backup window opens for this schedule. This number is the number of seconds since midnight. It is an integer between 0 and 86400 (the number of seconds in a day).

duration is the length of time that the window remains open. The time unit is seconds. It is a non-negative integer.

-cal 0|1|2
Indicates whether bpschedulerep follows a calendar-based schedule or a frequency-based schedule.

0 = frequency-based schedule
1 = calendar-based schedule with no retries after run day
2 = calendar-based schedule with retries after run day

dayomonth 1-31 [1-31]... | 1
Specifies the day or days of every month to run the schedule. Enter 1 (lowercase L) to run the last day of every month, whether the month contains 28, 29, 30, or 31 days.

For example, to run the policy backup on the 14th day and the 28th day of every month, enter the following:

-dayomonth 14 28

To run the last day of every month, enter:

-dayomonth 1

deldayomonth 1-31 [1-31]... | 1
Specifies a day of every month to exclude as a run day. Enter 1 (lowercase L) to exclude the last day of every month, whether the month contains 28, 29, 30, or 31 days. This command can only remove the dates that were added by using the -dayomonth command.

For example, to exclude from the schedule the 20th day and 21st day of every month that you originally specified as run days, enter:

-deldayomonth 20 21

delweekday day_name week [day_name week]...
Specifies a day of the week and the week of the month to exclude as a run day from the schedule. This command can only remove the dates that were added by using the -weekday command.

- The day_name is: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday.
- The week is the number of the week in the month. A week begins on Sunday and ends on Saturday. Valid values are 1-5.

For example, to delete the second Monday of the month that you originally specified as a run day, enter:

- delweekday Monday 2

-excl mm/dd/yyyy
Indicates to exclude this single date.

-delincl mm/dd/yyyy
Indicates to delete this single date.

-delexcl mm/dd/yyyy
Indicates to delete this single date.

-ci
Clears all specific include dates.

-ce
Clears all specific exclude dates.

-cw
Clears all week days.

-cd
Clears all days of a month.

-fail_on_error 0|1[,0|1,...,0|1]
Specifies whether to fail all other copies if one copy fails. If no parameter is specified, 0 is default for all copies. Specify a value for each copy.

0  = Do not fail the other copies
1  = Fail other copies

-freq backup_frequency
Specifies how much time can elapse between successful automatic backups for clients on this schedule. Frequency does not apply to user schedules because the user can perform a backup or archive any time the backup window is open. This value is a positive integer that represents the number of seconds between successful automatic backups for this schedule.

-help
Prints a command-line usage message.

-incl mm/dd/yyyy
Indicates to include this single date.
-M master_server,...

A list of alternative master servers. This list is a comma-separated list of host names. If this option is present, each master server in the list runs the bpschedulerep command. Each master server in the list must allow access by the system that issued the bpschedulerep command. If an error occurs for any master server, the process terminates at that point.

The schedule attributes are modified on all the master servers in this list.

-number_copies number

Specify the number of simultaneous backup copies. The valid value range is 1-4. The default is 1.

-pool volume_pool_label[ , pool-copy2,...]

Specifies the volume pool(s) for the schedule. Do not use this option if a disk storage unit is the residence for the schedule. If "*NULL*" is specified, the volume pool for the schedule is the volume pool of the policy that contains this schedule.

Specify a pool for each copy.

To display the configured volume pools, run the following command:

UNIX systems:

/usr/openv/volmgr/bin/vmpool -listall

Windows systems:

install_path\Volmgr\bin\vmpool -listall

-residence storage_unit_label[ , stunit-copy2,...]

Specifies the label(s) of the storage unit to be used for storing the backups that were created according to this schedule. If "*NULL*" is specified, the residence for the schedule defaults to the residence of the policy that contains this schedule. If the residence value is a storage unit label, the residence for the schedule becomes that storage unit; it overrides the residence for the policy.

Specify a storage unit for each copy.

Run bpstulist to display the set of defined storage units.

-stage priority number

The order in which storage units are to be selected within a storage unit group:

1 = Use the storage units in the order that appears in the storage unit group dialog box (default).

2 = Use the storage unit least recently used. (The storage units take turns.)
3 = Use the first storage unit in the list that is not full or down. If the storage unit is only busy, the policy waits to write to it.

-altreadhost hostname

The server to be used to read a backup image that a different media server originally wrote.

sched_label

The name of the previously created schedule to be changed.

-weekday day_name week [day_name week]...

Specifies a day of the week and a week of the month as a run day in the schedule.

- The day_name is: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday.
- The week is the number of the week in the month. A week begins on Sunday and ends on Saturday. Valid values are 1-5.

For example, to instruct the policy to run every Sunday of the month, enter:

-weekday Sunday 1 Sunday 2 Sunday 3 Sunday 4 Sunday 5

-v

Selects the verbose mode. This option causes bpschedulerep to log additional information for debugging purposes. The information goes into the NetBackup administration daily debug log. This option is meaningful only when NetBackup enables the debug log function (that is, when the following directory is defined):

UNIX systems:

/usr/openv/netbackup/logs/admin

Windows systems:

install_path\NetBackup\logs\admin

-xdayomonth 1-31 [1-31]... | l

Specifies the day or days of the month that you want to exclude as run days in the schedule. Use l (lowercase L) to indicate the last day of the month.

For example, to instruct the policy to not run the backup on the 6th of the month, enter:

-xdayomonth 6
-xweekday day_name week [day_name week]...

Specifies the day of the week and week of the month, to exclude as a run day in the schedule.

- The *day_name* is: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday.
- The *week* is the number of the week in the month.
- Use 1 to indicate the last week of the month. The week of the month starts on Sunday and ends on Monday. Valid values are 1-5.

For example, to instruct the policy to not run on the third Monday and Wednesday of the month, enter:

- -xweekday Monday 3 Wednesday 3

EXAMPLES

Example 1 - Change and schedule named test.

# bpschedulerep test -cal 2

The following is received after the change and a bpschedule -label test listing.

SCHED test 0 1 604800 1 0 0 0 *NULL* 0 2 0 0 0
SCHEDWIN 0 0 0 0 0 0 0 0 0 0 0 0 0
SCHEDRES *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL*
SCHEDPOOL *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL*
SCHEDRL 1 1 1 1 1 1 1
SCHEDFOE 0 0 0 0 0 0 0

Example 2 - For Saturday and Sunday of each week, have the window for schedule test open at 10 p.m. instead of 11 p.m. Also, set the window duration to two (2) hours instead of one (1) hour. bpschedulerep resets the windows, and bpschedule lists the new schedule values.

# bpschedulerep test -0 79200 7200 -6 79200 7200
bpschedule -U -label test
Schedule: test
Type: Full Backup
Frequency: every 7 days
Retention Level: 1 (2 weeks)
Maximum MPX: 1
Residence: (specific storage unit not required)
Volume Pool: (same as policy volume pool)
Daily Windows:
Sunday  22:00:00 --> Sunday  24:00:00  
Monday  23:00:00 --> Monday  24:00:00  
Tuesday 23:00:00 --> Tuesday 24:00:00  
Wednesday 23:00:00 --> Wednesday 24:00:00  
Thursday 23:00:00 --> Thursday 24:00:00  
Friday  23:00:00 --> Friday  24:00:00  
Saturday 22:00:00 --> Saturday 24:00:00

FILES

UNIX systems:

/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/db/sched/schedule name

Windows systems:

install_path\NetBackup\logs\admin/*
install_path\NetBackup\db\sched\schedule name

SEE ALSO

See bpschedule on page 401.
bpsetconfig

bpsetconfig – update a NetBackup configuration

SYNOPSIS

bpsetconfig [-h host] [-u user] [filename,...] [-r "reason"]

UNIX only: bpsetconfig -i | -e filename [-c class [-s schedule]]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\

DESCRIPTION

The bpsetconfig command is used as a stand-alone program, or as a helper program with the backuptrace and the restoretrace commands, to update a configuration. This command is available for all NetBackup server platforms. You must have administrator privileges to run this command.

OPTIONS

-e filename [-c class [-s schedule]]

  Writes the exclude_list file to /usr/openv/netbackup/exclude_list on client client. The class (policy) and schedule qualifiers allow the exclude_list.class file and the exclude_list.class.schedule to be written. The files in the exclude list are excluded from being backed up.

  This option applies only to UNIX.

filename,...

  Specifies the file or files where the updates are listed. If not specified, standard input is read.

-h host

  Specifies the host name of the server or client whose configuration is updated.
-i filename [-c class [-s schedule]]

Writes the include_list file to /usr/openv/netbackup/include_list on client class. The class (policy) and schedule qualifiers allow the include_list.class file and the include_list.class.schedule to be written. The files in the include list are the exceptions to the exclude list. They are therefore included in a backup operation.

This option applies only to UNIX.

-r "reason"

Indicates the reason why you choose this command action. The reason text string that you enter is captured and appears in the audit report. Enclose this string with double quotes ("..."). The string must not exceed 512 characters. It cannot begin with a dash character (-) nor contain a single quotation mark (').

-u user

Specifies the user whose configuration is updated.

EXAMPLE

Example 1 - Set a NetBackup configuration on a different system.

bpsetconfig -h orange.colors.org
SERVER = yellow.colors.org
SERVER = orange.colors.org

UNIX systems: Ctl+D
Windows systems: Ctl+Z

Sets the NetBackup configuration on the system orange.colors.org to the designated server that follows. That is, yellow.colors.org is the master server for the client orange.colors.org:

SERVER = yellow.colors.org
SERVER = orange.colors.org

Example 2 - Write the file /usr/openv/netbackup/lists/sun01_excl_list.fullb to /usr/openv/netbackup/excl_list.fullb on the client sun01.

# bpsetconfig -e /usr/openv/netbackup/lists/sun01_excl_list.fullb / -h sun01 -c fullbck

SEE ALSO

See bpgetconfig on page 158.
See `nbgetconfig` on page 714.

See `nbsetconfig` on page 831.
bpstsinfo

bpstsinfo – display information on storage servers, LSUs, images, and plugins

SYNOPSIS

bpstsinfo -comparedbandstu | -cdas -servername | -sn server_name | -storage_server storage_server -serverprefix server_prefix | -stype server_type [ -lsuname lsu_name],... -oldservervolume old_sts_server:old_volume [ -oldservervolume old_sts_server:old_volume ...
bpstsinfo -deleteimage | -di -servername | -sn server_name -serverprefix server_prefix -lsuname lsu_name -imagename image_name -imagedate image_date [ -remote remote_server...]
bpstsinfo -deleteimagegroup | -dig -servername | -sn server_name | -storage_server storage_server -serverprefix server_prefix -lsuname lsu_name -imagename image_name -imagedate image_date [ -remote remote_server...]
bpstsinfo -diskspaceinfo | -dsi -stype storage_type

bpstsinfo -imagegrouplist | -igl [-servername | -sn server_name] [-serverprefix server_prefix] [-lsuname lsu_name,...] [ -imagename image_name] [[-imagedatetostart image_date] [ -imagedateend image_date]] [-imagetype STS_FULL_ONLY | STS_INCR_ONLY ] [ -remote remote_server...]

bpstsinfo -imageinfo | -ii [-servername | -sn server_name] [-serverprefix server_prefix] [-lsuname lsu_name,...] [ -imagename image_name] [-imagedate image_date] [ [-imagedatetostart image_date] [-imagedateend image_date]] [-imagetype STS_FULL_ONLY | STS_INCR_ONLY ] [ -remote remote_server...]

bpstsinfo -lsuinfo | -li [-servername | -sn server_name] [-serverprefix server_prefix] [-lsuname lsu_name,...] [-filteronimagemodetype [STS_SA_IMAGE | STS_SA_OPAQUEF | STS_SA_CLEARF] [ -remote remote_server...]

bpstsinfo -plugininfo | -pi [-serverprefix server_prefix] [-stype server_type] [ -remote remote_server...]

bpstsinfo -servercap | -sc [-stype server_type] -storage_server storage_server [ -remote remote_server...]
bpstsinfo -serverinfo | -si [-servername | -sn server_name]
[-serverprefix server_prefix] [-remote remote_server...]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\

DESCRIPTION

The bpstsinfo command displays the attributes for plugins, storage servers, logical
storage units (LSUs), and the images that reside on disk. The command also
compares images old and current servers and volumes, displays all image IDs for
an image group, and deletes a specified image. A log of the command activity is
sent to the NetBackup admin log file for the current day. All errors for this command
go to stderr.

Only authorized users can run this command.

For more about NetBackup authorization, see the NetBackup Security and
Encryption Guide.

OPTIONS

Only one of the following options can be specified on a single command line.

-comparebandstu | -cdas
Creates a report of the compares of OpenStorage.

-deleteimage | -di
Deletes the specified image.

-deleteimagegroup | -dig
Deletes the specified image group.

-diskspaceinfo | -dsi
Prints the aggregated space for a specified disk type.

-imagegrouplist | -igl
For a given image and image group type, print all associate image IDs
-imageinfo | -ii
  Prints the image information.

-lsuinfo | -li
  Prints the LSU information.

-plugininfo | -pi
  Prints the plugin information for internal and external plugins on the system. When you use -plugininfo with no sub-options, all plugins are printed. Use with -serverprefix to restrict the printout to only the plugin with the specified prefix. Use -stype to restrict the printout to only plugins of the specified storage server type.

-serverinfo | -si
  Prints the storage server information.

-servercap | -sc
  Prints the storage server capabilities.

SUB-OPTIONS

-filteronimagemodetype [STS_SA_IMAGE | STS_SA_OPAQUE | STS_SA_CLEAR]
  Limits the LSUs to be printed on the system to the specified image mode type.

-imagedate image_date
  Specifies a single image. The following are acceptable formats:
  03/08/2009 09:41:22
  1110296416
  This option can be used with -imageinfo only; it cannot be used with -imagedateend or -imagedatestart.

-imagedateend image_date
  Optional filter argument. By default, all images are used. Specify MM/DD/YYYY hh:mm:ss to the images to something that is equal to or newer than the image_date.

-imagedatestart image_date
  Optional filter argument. By default, all images are used. Specify MM/DD/YYYY hh:mm:ss to limit the images to something that is equal to or newer than the image_date.

-imagename image_name
  Optional filter argument. By default, all images are used. Specify image_name to limit to only the images that match.
Optional filter argument. By default, both the full and the incremental images are used. STS_FULLONLY or STS_INCRONLY to limit to only images from a full backup or an incremental backup.

Optional filter argument. By default, all LSUs are used. Specify -lsuname to limit to one LSU for each -lsuname supplied.

Specifies the name of a remote server to query for disk information. The remote server performs the bpstsinfo operation instead of the host on which the bpstsinfo command is executed. You can specify multiple remote servers, one for each -remote supplied.

Specifies the hostname of the STS server. If -servername is not specified, the hostname of the local host is used.

Limits server prefixes to the one that server_prefix specifies. Optional filter argument. By default, all server prefixes are used. This option can be used with -serverinfo, -lsuinfo, and -imageinfo. The following are valid prefixes:

- ntap:
- STSBasicDisk:
- PureDisk:

Specifies a string that identifies the storage server type. The server_type value can originate from one of the following sources:

- Veritas provided storage. Possible values are AdvancedDisk and PureDisk.
- Third-party disk appliances. The vendor supplies the server_type string.
- Cloud storage. Use the cconfig cldprovider -1 command to determine the possible stype values. The cloud stype values reflect the cloud storage provider. Cloud storage stype values can also incorporate a suffix (for example, amazon_crypt). Possible suffixes are:
  - _raw: The NetBackup backup image is sent to the cloud in raw format. Use this option if you do not want to compress or encrypt data before sending to cloud storage.
  - _rawc: Compresses the data before it is written to the cloud storage.
- _crypt: Encrypt the data using AES-256 encryption before writing the data to cloud storage. You must have KMS configured in NetBackup to use this option.

- _cryptc: Compress and encrypt the data before writing to cloud storage.

The storage server type is case sensitive.

When used with the -diskspaceinfo option, -stype specifies the disk type that is to display the aggregated space. An example of the output display:

```
Disktype: AdvancedDisk TotalCapacity: 100000000 TotalUsed: 10000000
```

Licensing is based on the TotalCapacity and TotalUsed values.

EXAMPLES

Example 1 - List the attributes of the LSU SnapMirrorA1 on storage server apricot:

```
# bpstsinfo -lsuinfo -serverprefix "ntap:" -servername apricot /vol/dsu1
LsuInfo:
  Server Name: ntapdfm
  LSU Name: SnapMirrorA1
  Allocation: STS_LSU_AT_STATIC
  Storage: STS_LSU_ST_NONE
  Description:
  Configuration:
    Media: (STS_LSUF_DISK | STS_LSUF_REP_ENABLED)
    Save As: (STS_SA_SNAPSHOT | STS_SA_MIRROR)
  Replication Sources: 1 (simdisk:ntapdfm:SnapVaultA)
  Replication Targets: 0 ( )
  Maximum Transfer: 0
  Block Size: 4096
  Allocation Size: 0
  Size: 171798691840
  Bytes Used: 8895016960
  Physical Bytes Used: 0
  Resident Images: 0
```

Example 2 - List all capabilities for storage server sigt32.

```
# bpstsinfo -sc -stype Network_MWS -storage_server sigt32
Network_MWS:sigt32
```
STS_SRVC_ASYNC_WAIT
STS_SRVC_CLAIM
STS_SRVC_CLOSE_IMAGE
STS_SRVC_CLOSE_IMAGE_LIST
STS_SRVC_CLOSE_LSU_LIST
STS_SRVC_CLOSE_SERVER
STS_SRVC_COPY_IMAGE
...
STS_SRVC_NAMED_ASYNC_ROLLBACK_SNAP
STS_SRVC_NAMED_ASYNC_VALIDATE_SNAP_BYNAME
STS_SRVC_NAMED_ASYNC_WAIT_SNAP
STS_SRVC_OPEN_SNAP_LIST
STS_SRVC_VALIDATE_ROLLBACK
STS_SRVC_VALIDATE_SNAP_BYNAME

SEE ALSO

See `bpstuadd` on page 425.
See `bpstudel` on page 435.
See `bpstulist` on page 438.
See `bpsturep` on page 446.
bpstuadd

bpstuadd – create NetBackup storage unit or storage group

SYNOPSIS

bpstuadd -label storage_unit_label -path path_name [-dt disk_type]
| -dp disk_pool [-dt disk_type] | -density density_type [-rt
robot_type -rn robot_number] [-host host_name] [-cj max_jobs] [-odo
on_demand_only_flag] [-flags flags] [-cf clearfiles] [-tt
transfer_throttle] [-hwm high_water_mark] [-lwm low_water_mark] [-okrt
ok_on_root] [-mfs max_fragment_size] [-maxmpx mpx_factor] [-nh
NDMP_attach_host] [-nodevhost] [-verbose] [-hostlist host_name...]
[-M master_server,...] [-reason "string"] [-uw 1|0]

bpstuadd -group storage_unit_group storage_unit_label ... [-sm
selection_method]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The bpstuadd command creates a NetBackup storage unit or storage unit group. When you create a single storage unit, make sure that you include a label for the new storage unit: either the -density the -path, or the -dp option. bpstuadd cannot create the storage unit if the master server has already created the maximum number of storage units that its NetBackup configuration allows. The command does not create a storage unit that specifies the same destination medium as an existing storage unit.

Note: This command does not enable you to change a disk storage unit (DSU) or a tape storage unit to a disk staging storage unit (DSSU). In addition, you cannot change a DSSU to a DSU or a tape storage unit.

NetBackup has several types of storage units. The storage-unit type affects how NetBackup stores the data. The options on the bpstuadd command line determine one of the following:
- Disk. The storage destination is a disk file system directory, a disk pool, or both.
- Disk Staging. A disk staging storage unit (DSSU) addresses the automatic (or scheduled sweeping) of images from the DSSU to the final storage unit.
- Media Manager. The storage destination is a tape device managed by the Media Manager.
- NDMP. An NDMP is a storage unit that Media Manager controls. The NetBackup for NDMP option must be installed. In this command description, references to Media Manager storage-unit types also apply to the NDMP storage-unit type except where specifically mentioned. The media for an NDMP storage unit always attach directly to an NDMP host and cannot be used to store data for other NetBackup clients. To define an NDMP storage unit, run the `bpstuadd` command on the master server.

For more about how to add NDMP storage units, see the *NetBackup for NDMP Administrator’s Guide*.

Errors go to `stderr`. A log of the command activity goes to the NetBackup admin log file for the current day.

For more about storage units, see the *NetBackup Administrator’s Guide*, *Volume II*.

Only authorized users can run this command.

For more about NetBackup authorization, see the *NetBackup Security and Encryption Guide*.

## OPTIONS

`-cf clearfiles`

Enables the NetBackup media to perform data translation operations on backup data. Typically, OpenStorage plugins use metadata to perform the block-level deduplication operations that reduce the total amount of disk space being used. This value is valid only for disk storage units that are configured with OST disk pools.

The `clearfiles` variable can be one of the following values:

- 0 - Disables all data translation operations.
- 1 - Enables detailed translation operation. The metadata describes all of the attributes of the files that are backed up. These files are called clear files.
- 2 - Enables simple translation operation. The metadata identifies only the name, size, and byte offset location of the files that are backed up. They are called opaque files.
-cj max_jobs
   Specifies the maximum number of concurrent jobs that are permitted for this
   storage unit. max_jobs is a non-negative integer. The appropriate value depends
   on your server’s ability to run multiple backup processes comfortably and the
   available space on the storage media.

   For more about maximum jobs per client, see the NetBackup Administrator’s
   Guide, Volume I.

   The max_jobs option that is set to zero (0) means that this storage unit is never
   selected when a job is scheduled. The default is 1.

-density density_type
   Specifies the density type of the media. If this option is present, the storage
   unit type is Media Manager. This option has no default. Either -density, -path,
   or -dp must be on the command line. If you have specified the robot type on
   the command line, the value for density should be consistent with the robot
   type. The -density, -path, and -dp options can only be used independently.

   Valid values for density_type are:

   dlt - DLT Cartridge
   dlt2 - DLT Cartridge alternate
   8mm - 8mm Cartridge
   4mm - 4mm Cartridge
   qscsi - 1/4 Inch Cartridge

   Note: NetBackup supports the following densities on NetBackup Enterprise
   Servers.

   hcart - 1/2-inch cartridge
   hcart2 - 1/2-inch cartridge alternate
   dtf - DTF Cartridge

   -dp disk_pool
   Specifies the name of the disk pool, which is the data storage area for this
   storage unit. The disk pool must already exist.

   -dt disk_type
   Enables the user to specify a disk type. The following are the valid values for
   disk_type:

   1 - BasicDisk
3 - SnapVault
6 - DiskPool

-flags flags
   Specifies the storage unit to be a staging storage unit, which allows for a quick
   restore. Valid values for flags are: NONE and STAGE_DATA. Currently valid
   for only disk storage units.

-group storage_unit_group storage_unit_label...
   Adds a storage unit group and specifies the group name and the storage unit(s)
   that comprise the group. Add multiple storage units to the storage unit group
   by separating the names with a space. The maximum length of a storage unit
   group label is 128 characters.

-host host_name
   Indicates a single specific media server that is associated with the storage unit.
   Only this media server can be selected as the system to read or write from the
   storage. The default is the host name of the local system.

---

**Note:** NetBackup Server does not support remote media servers.

The host you select must be either your NetBackup master server or a remote
media server (if you configure remote media servers). The host name must be
the network name for the server as known by all NetBackup servers and clients.

If host_name is a valid network name, but was not configured previously in
NetBackup, it is added to NetBackup’s configuration as a media server. On
UNIX, this server shows up as a SERVER entry in the bp.conf file; on Windows,
Host Properties specifies the server in the Servers list. If host_name is not a
valid network name, you must configure it manually.

-hostlist host_name...
   Indicates that a subset of the media servers with access to the storage should
   be used. Use this option if multiple media servers share a disk pool. You want
to dedicate one set of media servers to service a set of policies and clients.
Then you want a different set to service other policies and clients (or for a
specific role such as duplication jobs).

-hwm high_water_mark
   Specifies a percentage of a disk storage unit at which it is considered full. This
option is a user-configurable threshold. The valid range for the High Water
Mark is 0 to 100 (percentage), and the default setting is 98(%). When the High
Water Mark is reached, NetBackup becomes proactive in the following two
different scenarios:
When you run a job and the total capacity is used, the DSU is considered to be Full. If you choose a storage unit in a Storage Unit Group, the following occurs: The media and the device selection (MDS) does not assign a new job to a storage unit whose used capacity exceeds the High Water Mark. Instead, it looks for another storage unit in the group to assign to the job.

During a job, if the Staging attribute is set and the total capacity is used, staging expires images to free space on the DSU. This action accommodates more backup data.

-`-label storage_unit_label`
  Specifies the name of the storage unit. This option is required unless you use `-group`. The maximum length of a storage-unit label is 128 characters.

-`-lwm low_water_mark`
  This option is a user-configurable threshold that the disk storage units that do disk staging use. The valid range for the Low Water Mark is 0 to 100 (percent). The default setting is 80 (percent).

  When the High Water Mark is reached, do one of the following:
  - Migrate images to other storage units until the Low Water Mark is reached.
  - Free disk space by expiring disk images for the oldest staged images until the Low Water Mark is reached.

  If you want to save most of your data, configure the Low Water Mark to be near the High Water Mark.

-`-M master_server,...`
  A list of master servers. This list is a comma-separated list of host names. If this option is present, the command is run on each of the master servers in this list. The servers must allow access by the system that issues the command. If an error occurs for any master server, the process stops at that point. The default is the master server for the system where the command is entered.

-`-maxmpx mpx_factor`
  The maximum multiplexing factor. Multiplexing sends concurrent, multiple backups from one or several clients to a single drive.

  For more about multiplexing (MPX), see the *NetBackup Administrator's Guide, Volume I*.

  The multiplexing factor can range from 1 to 32. The default is 1, which means no multiplexing. A value greater than one (1) means that NetBackup can create multiplexed images on the destination medium. The license determines the effective subset of the 1 to 32 range for the local NetBackup installation.
-mfs max_fragment_size
   Specifies the maximum fragment size in megabytes, or how large a fragment a NetBackup image can be. NetBackup supports a maximum fragment size of 1,000,000 megabytes (one terabyte).
   For removable media, this value is zero or any integer between 50 (megabytes) and 1,048,576 (megabytes) (1024 GB) inclusive. The default value is 0, which means the maximum of 1,048,576 MB.
   For a Disk storage unit, this value ranges from 20 MB to 524,288 MB (512 GB). The default value is 524,288 MB.

-nh NDMP_attach_host
   Specifies the host name of the NDMP server. If this option is present, the storage unit type is set to NDMP. The default is no NDMP server.

-nodevhost
   Indicates that no media server is associated with this storage unit. You can select any media server that can access the storage to move the data (such as backup, duplicate, restore).

-odo on_demand_only_flag
   The On-Demand-Only flag controls the condition under which NetBackup uses the storage unit:
   ■ To make the storage unit available only to the policies or the schedules that request it, set the flag to 1 (enabled).
   ■ To make the storage unit available to any policy or schedule, set the flag to 0 (disabled).
   If the storage unit type is Disk, the default is 1; NetBackup uses the storage unit only when explicitly requested. Otherwise, the default is 0.
   DSSUs are on demand only. They have to be chosen explicitly as a backup target.

-okrt ok_on_root
   If this flag is not set, neither backups nor directory creation occur on the root file system. If the ok_on_root flag is set, then backups and directory creations occur normally.
   The default value for this flag is 0. Backups and directory creations to a disk storage unit (BasicDisk) do not occur if the path is on the root file system.

-path path_name
   Specifies the path to a disk file system that expressed as an absolute pathname, which is the data storage area for this storage unit. When this option is present, the storage unit type is Disk. This option has no default. Either -path, -dp, or
-density must be on the command line. The -density, -path, and -dp options can only be used independently.

In general when this option is used, enable the On-Demand-Only flag (see -odo). Otherwise, if you have any NetBackup policies that do not require specific storage units, they can fill the disk file system path_name. This action can cause serious system problems. For example, if the system swap area happens to be on the same file system, new processes may fail.

-reason "string"
Indicates the reason why you choose this command action. The reason text string that you enter is captured and appears in the audit report. Enclose this string with double quotes ("..."). The string must not exceed 512 characters. It cannot begin with a dash character (-) nor contain a single quotation mark (').

-rn robot_number
Specifies the robot number for this storage unit. It must be greater than or equal to 0. The robot number can be obtained from the Media and Device Management of the Administration Console. This option is ignored unless the -rt option is present. This option has no default.

For more about rules that concern the use of the robot number, see the NetBackup Administrator's Guide, Volume II.

-rt robot_type
The robot type for this storage unit. For non-robotic (stand-alone) devices select NONE or omit this option. The default value is NONE (Not Robotic). The value for density should be consistent with the robot type.

If this option is set to any value other than NONE, the -rn option is required. Available robot type codes are:

NONE - Not Robotic
TLD - Tape Library DLT
ACS - Automated Cartridge System

-sm selection_method
Selects the method in which a storage unit group is chosen. This option is valid only for storage unit groups. The possible values for selection_method are:

Prioritized = 1 (default)
Least Recently Selected = 2
Failover = 3
Load Balance = 4
Option 1: Prioritized, selects the first storage unit in the list until the unit is down, is full, or its max-concurrent-jobs setting is reached. Then the next storage unit in the list is examined and so on until an available one is found.

Option 2: Least Recently Selected, selects the least-recently selected storage unit.

Option 3: Failover is the same as Prioritized except MDS queues a job to wait for the first storage unit if the max-concurrent-jobs is reached. MDS moves on to the next storage unit in the list only if the first unit is down or full.

Option 4: Load Balance. If the user selects this option and has installed the capacity management license, Media Device Selection (MDS) balances the job load. It balances the job load by considering if a media server meets the following conditions:

- Enough disk volume free space available to accommodate the estimated job size.
- Enough CPU and memory resources available to accommodate another job.
- Least amount of estimated job size data being processed compared to other media servers of the same class or rank.

If the user does not have the capacity management license, then Load Balance reverts to option 2, the least-recently selected storage unit.

-\texttt{tt} transfer\_throttle

The Transfer Throttle setting appears for SnapVault storage units only.

The setting indicates the maximum SnapVault data transfer bandwidth. A setting of zero (default) indicates an unlimited bandwidth and data transfer would occur at the full network bandwidth. (Range: 0 (default) to 9999999.)

-\texttt{-uw} 1|0

This option is used to define a storage unit as write once, read many (WORM). If this option is set, the images that are written to the storage until are WORM locked. The default value for this option is 0. Once -\texttt{-uw} is set to 1, defining the storage unit for WORM, it cannot be reverted. You must delete the storage unit and create it again with -\texttt{-uw} 0.

-\texttt{-verbose}

Select verbose mode for logging. This option is meaningful only when it runs with debug log function on (that is, when the following directory is defined):

UNIX systems: /usr/openv/netbackup/logs/admin

Windows systems: install_path\NetBackup\logs\admin
EXAMPLES

Example 1 - Create a new storage unit, named *hatunit*. Its storage unit type is Disk.

On UNIX systems, the path for the storage unit is `/tmp/hatdisk`.

On Windows systems, the path for the storage unit is `C:\tmp\hatdisk`.

UNIX systems:

```
# bpstuadd -label hatunit -path /tmp/hatdisk -verbose
```

Windows systems:

```
# bpstuadd -label hatunit -path C:\tmp\hatdisk -verbose
```

<2>bpstuadd: INITIATING: NetBackup 8.0 created: 0
<2>bpstuadd: EXIT status = 0.

Example 2 - Create a storage unit by using a UNIX server, which has not been configured previously in NetBackup:

```
# bpstuadd -label parrot_stu -host parrot -density dlt -rt TLD -rn 2

Remote media server parrot was added to the *bp.conf* file.

You must also install NetBackup and Media Manager on parrot and run the
*add_media_server_on_clients* executable on the master server.

```
% grep parrot /usr/openv/netbackup/bp.conf
SERVER = parrot
```

RETURN VALUES

An exit status of zero (0) means that the command ran successfully.

Any exit status other than zero (0) means that an error occurred.

If the administrative log function is enabled, *bpstuadd* logs the exit status in the administrative daily log under the log directory:

UNIX systems:

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

Windows systems:
install_path\NetBackup\logs\admin

It has the following form:

```bash
# bpstuaddnew: EXIT status = exit status
```

If an error occurred, a diagnostic precedes this message.

**FILES**

UNIX systems:

```bash
/usr/openv/netbackup/logs/admin/*
```

Windows systems:

```bash
install_path\NetBackup\logs\admin/*
```

EMM database

**SEE ALSO**

- See [bpstsinfo](#) on page 419.
- See [bpstudel](#) on page 435.
- See [bpstulist](#) on page 438.
- See [bpsturep](#) on page 446.
bpstudel

bpstudel – delete NetBackup storage unit or storage unit group

SYNOPSIS

bpstudel -label storage_unit_label [-verbose] [-M master_server [, ...]] [-reason "string"
bpstudel -group storage_unit_group [-M master_server [, ...]]

On UNIX systems, the directory path to this command is 
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The bpstudel command deletes a NetBackup storage unit or storage unit group. The
command must include either a label name for the storage unit or a group name for the storage unit group, but not both.

If bpstudel cannot delete the storage unit (for example, the storage unit label is
mistyped), it does not return an error message. You can run bpstulist to verify
that the storage unit was deleted.

Errors are sent to stderr. A log of the command’s activity is sent to the NetBackup
admin log file for the current day.

For more about storage units, see the NetBackup Administrator’s Guide, Volume II.

Any authorized user can run this command.

For more about NetBackup authorization, see the NetBackup Security and
Encryption Guide.

OPTIONS

-label storage_unit_label

The name of the storage unit. This option is required. The maximum length for
a storage-unit label is 128 characters.
-group storage_unit_group
Deletes the specified storage unit group the name. If this option is present, the named storage unit group is deleted.

-M master_server [, ...]
Runs this command on each of the master servers in this list. This list is a comma-separated list of master servers. The master servers must allow access by the system that issued the command. If an error occurs for any master server, the process stops at that point. The default is the master server for the system where the command is entered.

-reason "string"
Indicates the reason why you choose this command action. The reason text string that you enter is captured and appears in the audit report. Enclose this string with double quotes ("..."). The string must not exceed 512 characters. It cannot begin with a dash character (-) nor contain a single quotation mark (').

-verbose
Selects the verbose mode for logging. This mode is meaningful only when you run with the debug log function on (that is, when the following directory is defined):

UNIX systems:
/usr/openv/netbackup/logs/admin

Windows systems:
install_path\NetBackup\logs\admin

EXAMPLE

Delete the storage unit named tst.dsk and list the existing storage units before and after the deletion:

# bpstulist

UNIX systems:

stuunit 0 mango 0 -1 -1 1 0 /tmp/stuunit 1 1 2000 *NULL*
tst.dsk 0 mango 0 -1 -1 3 0 /hsm3/dsk 1 1 2000 *NULL*

Windows systems:

stuunit 0 mango 0 -1 -1 1 0 C:\tmp\stuunit 1 1 2000 *NULL*
tst.dsk 0 mango 0 -1 -1 3 0 C:\hsm3\dsk/ 1 1 2000 *NULL*
# bpstudel -label tst.dsk

# bpstulist

UNIX systems:

stuunit 0 mango 0 -1 -1 1 0 /tmp/stuunit 1 1 2000 *NULL*

Windows systems:

stuunit 0 mango 0 -1 -1 1 0 C:\tmp\stuunit 1 1 2000 *NULL*

FILES

UNIX systems:

/usr/openv/netbackup/logs/admin/*

Windows systems:

install_path\NetBackup\logs\admin/*

SEE ALSO

See bpstsinfo on page 419.
See bpstuadd on page 425.
See bpstulist on page 438.
See bpsturep on page 446.
bpstulist

bpstulist – display NetBackup storage units or storage unit groups

SYNOPSIS

bpstulist -label storage_unit_label [...] [-L | -l | -U | -show_available | -lsa ] [ -g | -go ] [-verbose] [-M master_server [...] [ -reason "string"]

bpstulist -group storage_unit_group [-verbose] [-M master_server [...] [,...]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The bpstulist command displays the attributes for a NetBackup storage unit or storage unit group. If no storage label or storage unit group name is specified, bpstulist displays the attributes for all NetBackup storage units or storage unit groups. In addition, this command accepts a comma-separated list of storage unit labels and displays the information for each of the storage units. The -show_available and -lsa flags enable you to list all of the configured media servers for a particular storage unit.

Errors are sent to stderr. A log of the command’s activity is sent to the NetBackup admin log file for the current day.

For more about storage units, see the NetBackup Administrator’s Guide, Volume I.

Any authorized user can run this command.

For more about NetBackup authorization, see the NetBackup Security and Encryption Guide.

OPTIONS

List-type options:
The list type is long. This option produces a listing with one storage unit attribute per line, in the format `storage-unit attribute: value`. Some attribute values are expressed in both interpreted form and raw form.

For a disk storage unit, a long listing has these attributes for each storage unit:

- Label
- Storage Unit Type (For example, Disk (0))
- Media Subtype (For example, BasicDisk (1))
- Host Connection
- Concurrent Jobs
- On Demand Only
- Max MPX
- Max Fragment Size
- Block Sharing
- OK On Root

A long listing has these attributes for each DiskPool disk storage unit:

- Label
- Storage Unit Type
- Media Subtype (DiskPool (6))
- Host Connection (one host per line)
- Concurrent Jobs
- On Demand Only
- Max Fragment Size
- Max MPX
- Block sharing
- Use WORM
- File System Export
- Disk Pool
- Snapshots
- Replication Primary
- Replication Source
Replication Target
Mirror

A long listing has these attributes for each Media Manager storage unit:

- Label
- Storage Unit Type (For example, Tape (0))
- Host Connection
- Concurrent Jobs
- On Demand Only
- Robot Type
- Max Fragment Size
- Max MPX/drive

The list type is short, which produces a terse listing. This option is useful for the scripts or the programs that rework the listing contents into a customized report format. This option is the default list type.

A single line contains the information for a storage unit, with all attribute values expressed in raw form. The fields on this line are:

- label
- storage unit type
- host
- density
- concurrent_jobs
- initial_mpx
- path
- on_demand_only
- max_mpx
- maxfrag_size
- ndmp_attach_host
- throttle (SnapVault only)
- subtype
- disk_flags
- high_water_mark
The list type is user. This option produces a listing with one storage-unit attribute per line, in the format `storage-unit attribute: value`. Attribute values are expressed in interpreted form.

For a disk storage unit, a user-type list has these attributes for each storage unit:

- Label
- Storage Unit Type (the storage-unit type)
- Storage Unit Subtype
- Host Connection
- Concurrent Jobs
- On Demand Only
- Max MPX
- Path
- Max Fragment Size
- Stage data
- High Water Mark
- Ok On Root

For a DiskPool disk storage unit, a user-type list has these attributes for each storage unit:

- Label
- Storage Unit Type
- Host Connection (one host per line)
- Concurrent Jobs
- On Demand Only
- Max Fragment Size
- Max MPX
- Use WORM
-g This list type causes the storage unit list to include the storage unit groups. The format of this option produces a listing with one storage unit group per line, in the format group_name: group_members. This option also includes the Selection Method value at the beginning of the Storage Unit Group List.

-go

This list type causes the storage unit list to include only information on the storage unit groups.

-label storage_unit_label1 [,storage_unit_label2...] Specifies the name of the storage unit. This list is a comma-separated list of storage unit labels. If this option is not present, the listing is for all storage units. The maximum length for a storage-unit label is 128 characters.

-group storage_unit_group

Specifies a list of defined storage units and storage unit groups. For the list of storage units, the list type is short, which produces a terse listing. The list of storage unit groups is in the format group_name: group_members.

-1sa

Lists all storage units in the database including any available media servers on the media server list.

-M master_server1 [,master_server2...] Specifies a comma-separated list of master servers. If this option is present, the command is run on each of the master servers in this list. The master servers must allow access by the system that issued the command. If an error
occurs for any master server, the process stops at that point in the list. The default is the master server for the system where the command is entered.

-reason "string"
Indicates the reason why you choose this command action. The reason text string that you enter is captured and appears in the audit report. Enclose this string with double quotes ("..."). The string must not exceed 512 characters. It cannot begin with a dash character (-) nor contain a single quotation mark (').

-show_available
Lists all storage units in the database including any available media servers on the media server list.

-verbose
Select verbose mode for logging. This mode is meaningful when only you run with the debug log function on (that is, when the following directory is defined):

UNIX systems:
/usr/openv/netbackup/logs/admin

Windows systems:
install_path\NetBackup\logs\admin

EXAMPLES

Example 1 - List the storage units that are defined on the master server apricot by using the -u display option:

# bpstulist -U -M apricot

Label: redtest
Storage Unit Type: Disk
Host Connection: apricot
Concurrent Jobs: 1
On Demand Only: yes
Max MPX: 4
Max Fragment Size: 512000 MB
Block Sharing: yes
OK On Root: no
Use WORM: no
Disk Pool: simSnapVaultA
Snapshots: yes
Replication Primary: no
Replication Source: yes
Replication Target: yes
Mirror: no
WORM Capable: no

Example 2 - The following output is realized by using the following `bpstuadd` command to create a regular disk staging storage unit:

```sh
# bpstuadd -label pear -path /tmp/pear -flags STAGE_DATA
```

Short output:

```
pear 0 felix.example.com 0 -1 -1 1 0 "/tmp/pear" 1 1 2000
*NULL* 0 1 0 98 80 1 pear felix.example.com
```

Long output:

```
Label: pear
Media Type: Disk (0)
Host Connection: felix.example.com
Concurrent Jobs: 1
On Demand Only: yes
Path: "/tmp/pear"
Robot Type: (not robotic)
Max Fragment Size: 512000
Max MPX: 1
Stage data: no
Block Sharing: no
File System Export: no
High Water Mark: 98
Low Water Mark: 80
OK On Root: no
```

**FILES**

**UNIX systems:**

```
/usr/openv/netbackup/logs/admin/*
```

**Windows systems:**

```
install_path\NetBackup\logs\admin\*
```

**EMM database**
SEE ALSO

See `bpstinfo` on page 419.
See `bpstuadd` on page 425.
See `bpstudel` on page 435.
See `bpsturep` on page 446.
bpsturep

bpsturep – replace selected NetBackup storage unit attributes

SYNOPSIS


bpsturep -group storage_unit_group [-addstu | -delstu] storage_unit_label [-M master_server ,...] [-sm selection_method]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\

DESCRIPTION

The bpsturep command modifies an existing NetBackup storage unit by replacing selected storage-unit or storage-unit-group attributes in the NetBackup catalog. The command line must include a label for the storage unit or a group name for the storage unit group. The label or the group name is the only storage-unit attribute that bpsturep cannot modify.

Note: This command does not enable you to change a disk storage unit (DSU) or a tape storage unit to a disk staging storage unit (DSSU). In addition, you cannot change a DSSU to a DSU or a tape storage unit.

Use the bpsturep command with care. The changes to the storage unit or storage unit group must be compatible with existing attributes. Make sure that resulting attribute combinations are valid, especially for the following attributes:
robot_type
robot_number
density_type
max_fragment_size
path_type
NDMP_attach_host

The safest way to modify these attributes is to run `bpsturep` one time for each attribute to be replaced.

`bpsturep` makes the changes by modifying the storage unit with the specified attribute changes. Run `bpstulist` after `bpsturep` to determine whether the intended changes were applied.

Errors go to `stderr`. A log of the command's activity goes to the NetBackup administrative log file for the current day.

For more about storage units, see the *NetBackup Administrator's Guide, Volume I*.

Any authorized user can run this command.

For more about NetBackup authorization, see the *NetBackup Security and Encryption Guide*.

**OPTIONS**

- **-cf clearfiles**
  Enables the NBU media to perform data translation operations on backup data. Typically, OpenStorage plugins use metadata to perform the block-level deduplication operations that reduce the total amount of disk space that is used. This value is valid only for disk storage units that are configured with OST disk pools.

  The `clearfiles` variable can be one of the following values:
  - 0 - Disables all data translation operations.
  - 1 - Enables detailed translation operation. The metadata describes all of the attributes of the files that are backed up. These files are called clear files.
  - 2 - Enables simple translation operation. The metadata identifies only the name, size, and byte offset location of the files that are backed up. They are called opaque files.

- **-cj max_jobs**
  The maximum number of concurrent jobs that are permitted for this storage unit. `max_jobs` is a non-negative integer. The appropriate value depends on
your server's ability to run multiple backup processes comfortably and the available space on the storage media.

For more about maximum jobs per policy, see the *NetBackup Administrator's Guide, Volume I.*

Zero (0) means that this storage unit is never selected when a job is scheduled. The default is 1.

-density density_type

If this option is present, the storage unit type is Media Manager. This option does not have a default. If the command line includes a robot type, the value for density should be consistent with the robot type. The -density, -path, and -dp options can only be used independently.

Valid density types are:

- dlt - DLT cartridge
- dlt2 - DLT cartridge alternate
- 8mm - 8mm cartridge
- 4mm - 4mm cartridge
- qscsi - 1/4-inch cartridge

**Note:** The following densities apply only to NetBackup Enterprise Servers.

- hcart - 1/2 Inch Cartridge
- hcart2 - 1/2 Inch Cartridge alternate
- dtf - DTF Cartridge

-dp disk_pool

Specifies the name of the disk pool, which is the data storage area for this storage unit. This option can be used only when the disk type is 6 (DiskPool). The disk pool must already exist.

-dt disk_type

Enables the user to specify a disk type. The following are the valid values for disk_type:

- 1 - BasicDisk
- 3 - SnapVault
- 6 - DiskPool
-flags flags

Specifies the storage unit to be a staging storage unit, which allows for a quick restore. Valid values for flags are: NONE and STAGE_DATA. Currently valid for only disk storage units.

-group storage_unit_group

The name of a storage unit group. This group is the storage unit whose members bpsturep adds or deletes. Use -addstu storage_unit to add storage units to the group. Use -delstu storage_unit to remove storage units from the group.

-host host_name

Note: NetBackup Server does not support remote media servers.

The NetBackup host to which the destination media is attached. The default is the host name of the local system.

The host you select must be either your NetBackup master server or a media server (if you configure media servers). The host name must be the network name for the server as known by all NetBackup servers and clients.

If host_name is a valid network name and is not yet configured, the value host_name is added to NetBackup’s configuration as a media server. On UNIX, this value shows up in bp.conf; on Windows, this value shows up in the Configuration window for Servers. If host_name is not a valid network name, you must configure it manually.

-hwm high_water_mark

This option is a user-configurable threshold. The default setting for the high water mark is 98%. When the high water mark is reached, NetBackup becomes proactive, under two different circumstances:

- When it initiates a job and the total capacity is used, the DSU is considered to be Full. If it selects from multiple storage units in a storage unit group, the following occurs: The media and the device selection (MDS) do not assign new jobs to units that are at or over the high water mark. It looks for another storage unit in the group, to assign to the job.

- During a job, if the Staging attribute is set and the total capacity is used, staging expires images to free space on the DSU. This action occurs to accommodate more backup data.
-label storage_unit_label
   The name of a storage unit. This unit is the storage unit whose attributes
   bpsturep replaces. This option is required. The maximum length of a
   storage-unit label is 128 characters.

-lwm low_water_mark
   This option is a user-configurable threshold, which disk storage units that do
   disk staging use. The default setting for the Low Water Mark is 80%.

   When the High Water Mark is reached, you should do one of the following:
   - Migrate images to other storage units, until the "Low Water Mark" is reached.
   - Free disk space by expiring disk images for the oldest staged images, until
     the "Low Water Mark" is reached.

   **Note**: If you want to save most of your available data, configure the Low Water
   Mark setting near the High Water Mark. In addition, the Low Water Mark must
   be less than High Water Mark. They cannot be equal settings.

-mfs max_fragment_size
   The maximum fragment size in megabytes that is specified (how large a
   fragment for a NetBackup image can be). NetBackup supports a maximum
   fragment size of 1,000,000 megabytes (one terabyte).

   For a Media Manager storage unit, this value is either zero. Or it is any integer
   greater than or equal to 50 megabytes (MB) and less than or equal to 1,048,576
   megabytes (MB) or (1024 GB). The default value is 0, which is equivalent to
   the largest value that is allowed, 1024 GB.

   For a Disk storage unit, this value ranges from 20 megabytes to 2000
   megabytes (2 gigabytes). The default value is 524288 (512 GB).

-maxmpx mpx_factor
   The maximum multiplexing factor. Multiplexing sends concurrent, multiple
   backups from one or several clients to a single drive.

   For more about multiplexing (MPX), see the *NetBackup Administrator’s Guide,
   Volume I*.

   The multiplexing factor can range from 1 to 32, where one (1) means no
   multiplexing. A value greater than one (1) means that NetBackup can create
   multiplexed images on the destination medium. Because of how the local
   NetBackup installation may be licensed, you may not be able to assign
   multiplexing factors in the entire range 1-32. The default is 1.
-M master_server [, ...]

Specifies a list of master servers. This list is a comma-separated list of host names. If this option is present, the command is run on each of the master servers in this list. The master servers must allow access by the system that issued the command. If an error occurs for any master server, the process stops at that point in the list. The default is the master server for the system where the command is entered.

-nh NDMP_attach_host

Specifies the host name of the NDMP server. If this option is present, the storage unit type is set to NDMP. The default is no NDMP server.

-nodevhost

Indicates that no media server is to be associated with this storage unit.

-odo on_demand_only_flag

The on-demand-only flag controls whether the storage unit is used only for the backups that explicitly request (demand) the storage unit:

To make the storage unit available only to the policies or the schedules that request it, set the flag to 1 (enabled).

To make the storage unit available to any policy or schedule, set the flag to 0 (disabled).

If the storage unit's type is Disk, the default is 1; NetBackup uses the storage unit only when explicitly requested. Otherwise, the default is 0.

-okrt ok_on_root

If this flag is not set, neither backups nor directory creation occurs on the root file system. If the ok_on_root flag is set, then backups and directory creations happen normally.

The default value for this flag is 0. Backups and directory creations to a disk storage unit (BasicDisk) do not occur if the path is on the root file system.

On UNIX systems, root is "/".

On Windows, root is the Volume where the windows\system directory resides.

-path path_name

The path to a disk file system, expressed as an absolute pathname, the data storage area for this storage unit. When this option is present, the storage unit type is Disk. This option does not have a default. The -density, -path, and -dp options can only be used independently.

In general when this option is used, enable the on-demand-only flag (see -odo). Otherwise, if you have any NetBackup policies that do not require a specific storage unit, they can fill the disk file system path_name. This action can cause
serious system problems. For instance, if the system swap area happens to be on the same file system, new processes may fail.

If the path name is defined as a disk staging storage unit (DSSU), use this option to change the path name a different DSSU. It cannot be used to change a DSSU to a different type of storage unit.

-\texttt{rn} \texttt{robot\_number}

The robot number for this storage unit. The robot number must be greater than or equal to 0. The robot number can be obtained from the Media and Device Management of the Administration Console. This option is ignored unless the -rt option is present. This option does not have a default.

For more about rules regarding the use of the robot number, see the \textit{NetBackup Administrator's Guide, Volume II}.

-\texttt{rt} \texttt{robot\_type}

The robot type for this storage unit. For non-robotic (stand-alone) devices select \texttt{NONE} or omit this option. The default value is \texttt{NONE} (Not Robotic). The value for density should be consistent with the robot type.

If this option is set to any value other than \texttt{NONE}, the -rn option is required.

Available robot type codes are:

\- \texttt{NONE} - Not Robotic
\- \texttt{TLD} - Tape Library DLT
\- \texttt{ACS} - Automated Cartridge System

-\texttt{sm} \texttt{selection\_method}

Selects the method in which a storage unit group is chosen. This option is valid only for storage unit groups. The following are its possible values:

Prioritized = 1 (DEFAULT)
Least Recently Selected = 2
Failover = 3
Load Balance = 4 (appears if the capacity management license is installed)

Option 1: Prioritized is the default condition. It selects the first storage unit in the list until either the unit is down or full, or its max-concurrent-jobs setting is reached. Then the next storage unit in the list is examined and so on until an available one is found.

Option 2: Least Recently Selected selects the least-recently selected storage unit.
Option 3: Failover is the same as Prioritized except MDS queues a job to wait for the first storage unit if the max-concurrent-jobs is reached. MDS moves to the next storage unit in the list only if the first unit is down or full.

Option 4: Load Balance. For this option to appear, make sure that you have installed the capacity management license. If the user selects this option, Media Device Selection (MDS) balances the job load by considering if a media server meets these conditions:

- Enough disk volume free space available to accommodate the estimated job size.
- Enough CPU and memory resources available to accommodate another job.
- Least amount of estimated job size data being processed compared to other media servers of the same class or rank.

If the license expires, then Load Balance reverts to Option 2 behavior. It selects the least-recently selected storage unit.

```
-transfer_throttle
```

The Transfer Throttle setting appears for SnapVault storage units only. The setting indicates the maximum SnapVault data transfer bandwidth. A setting of zero (default) indicates an unlimited bandwidth and data transfer would occur at the full network bandwidth. (Range: 0 (default) to 9999999.)

```
-worm
```

This option is used to define a storage unit as write once, read many (WORM). If this option is set, the images that are written to the storage until are WORM locked. The default value for this option is 0. Once -uw is set to 1, defining the storage unit for WORM, it cannot be reverted. You must delete the storage unit and create it again with -uw 0.

```
-verbose
```

Select verbose mode for logging. This mode is meaningful only when it runs with the debug log function on (when the following directory is defined):

UNIX systems:

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

Windows systems:

```
install_path\NetBackup\logs\admin
```
EXAMPLE

UNIX systems:
Change the path of disk storage unit \textit{mkbunit}. The path is changed from 
/tmp/mkbunit to /tmp/mkbunit2:

```bash
# bpstulist
mkbunit 0 beaver 0 -1 -1 1 0 /tmp/mkbunit 1 1 2000 *NULL*
# bpsturep -label mkbunit -path /tmp/mkbunit2
# bpstulist
mkbunit 0 beaver 0 -1 -1 1 0 /tmp/mkbunit2 1 1 2000 *NULL*
```

Windows systems:
Change the path of disk storage unit \textit{mkbunit}. The path is changed from 
C:/tmp/mkbunit to C:/tmp/mkbunit2:

```bash
# bpstulist
mkbunit 0 beaver 0 -1 -1 1 0 C:/tmp/mkbunit 1 1 2000 *NULL*
# bpsturep -label mkbunit -path C:/tmp/mkbunit2
# bpstulist
mkbunit 0 beaver 0 -1 -1 1 0 C:/tmp/mkbunit2/ 1 1 2000 *NULL*
```

FILES

UNIX systems:

/usr/openv/netbackup/logs/admin/*

Windows systems:

\textit{install\_path}/NetBackup/logs/admin/*

EMM database

SEE ALSO

See \texttt{bpstinfo} on page 419.
See \texttt{bpstuadd} on page 425.
See \texttt{bpstudel} on page 435.
See \texttt{bpstulist} on page 438.
bptestbpcd

bptestbpcd — test bpcd connections and verify connect options

SYNOPSIS

bptestbpcd [-host hostname] [-client client_name] [-M server] [-connect_options 0|1|2 0|1|2 0|1|2|3] [-connect_timeout seconds] [-wait_to_close seconds] [-verbose]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\

DESCRIPTION

The bptestbpcd command tries to establish a connection from a NetBackup server to the bpcd daemon on a NetBackup host or client. If successful, it reports information about the sockets that are established.

The first line of output consists of three digits that represent the effective connect options. These digits are only relevant when you connect to bpcd on the local host.

- The first digit is 0 if reserved source port is used and 1 if non-reserved port is used.
- The second digit is 0 if you use legacy (random port) callback and 1 if you use vnetd callback.
- The third digit is 1 if the connection is initiated to the PBX or vnetd port number. The third digit is 2 if the connection is initiated to the legacy bpcd port number.

The other output lines display the items shown:

- The NetBackup server IP address and port number.
- The connection direction.
- The bpcd IP address and port number.
- Whether the communication was encrypted by a local connection to the secure proxy process.
OPTIONS

-connect_options 0|1|2 0|1|2|3 0|1|2|3

The first setting indicates the type of source port to use when you connect to `bpcd` on the host or client. If you use the traditional callback method, this setting also designates the type of server port on which to listen for the inbound connection.

Note: This option is only useful when you test connectivity to `bpcd` on the local host.

0 = Use a reserved port number.
1 = Use a nonreserved port number.
2 = Use the value in the DEFAULT_CONNECT_OPTIONS configuration entry on the server.

The second setting indicates the `bpcd` call-back method to use to connect to the client:

0 = Use the traditional call-back method.
1 = Use the `vnetd` no call-back method.
2 = Use the value that the DEFAULT_CONNECT_OPTIONS configuration entry on the server defines.

The third setting indicates the connection method to use to connect the host or client:

0 = Connect to the host or client through the PBX port (1556). If unsuccessful, connect through the `vnetd` port (13724). If still unsuccessful, connect through the daemon port (13782).
1 = Connect to the host or client through the PBX port (1556). If unsuccessful, connect through the `vnetd` port (13724). If still unsuccessful, fail the connection attempt.
2 = Connect to the host or client through the daemon port (13782).
3 = Use the value that the DEFAULT_CONNECT_OPTIONS configuration entry on the server defines.

If `-connect_options` is not specified for `-client`, any CONNECT_OPTIONS configured in the Client Attributes for `clientname` are used. Otherwise, any CONNECT_OPTIONS for `clientname` are used. Otherwise, the DEFAULT_CONNECT_OPTIONS are used.
-client client_name
  The client name of the system to connect to. This option creates the same
  legacy connections to bpcd that would normally be used when you connect to
  a NetBackup client for a multiplex backup. If neither -host nor -client is
  specified, the host name of the local system is used.

-connect_timeout seconds
  Specifies the number of seconds to wait for a connection attempt from the
  server to the host or client to fail. If not specified, the default is the
  CLIENT_CONNECT_TIMEOUT that is configured on the server that tries to
  make the connection.

-host hostname
  Specifies the host name of the system to connect to. Typically, hostname
  is the host name of a NetBackup server. This option creates the same legacy
  connections to bpcd that would normally be used when you connect to a
  NetBackup server. If neither -host nor -client is specified, the host name of
  the local system is used.

-M server
  Specifies the host name of the NetBackup server that initiates the connections
  to the target host or client. If this option is not specified, the local host makes
  the connections. If it is specified, the local host connects to bpcd on the specified
  server, which then connects to bpcd on the target host or client.

-wait_to_close seconds
  Specifies the number of seconds that the server waits before it closes the
  connections to bpcd on the target host or client. The default is 0 (no waiting).

-verbose
  After successfully connecting to bpcd on the target host or client, request and
  display key configuration information from the remote host. This information
  can include: The host name, client name, master server, peer name for the
  connecting server, operating system, NetBackup version, and the host id
  certificate information used each host for the connection.

EXAMPLES

Example 1 - Try to connect from the local system to server fred using secure
connections:

# bp test bpcd -host fred
1 1 1
127.0.0.1:49613 -> 127.0.0.1:51195 PROXY 10.0.0.32:38828 -> 10.0.0.59:1556
127.0.0.1:53454 -> 127.0.0.1:52214 PROXY 10.0.0.32:54869 -> 10.0.0.59:1556
Example 2 - Request the server fred to connect to the insecure back-level (pre-8.1) host wilma as a client by using the daemon port and no-call-back method. If successful, display the key configuration from wilma. Notice that the daemon connect options are ignored, connections are by PBX or vnetd:

```
$ bptestbpcd -M fred -client wilma -connect_options 1 1 2 -verbose
PEER_NAME = fred
HOST_NAME = wilma
CLIENT_NAME = wilma
VERSION = 0x07730000
PLATFORM = solaris10
PATCH_VERSION = 7.7.3.0
SERVER_PATCH_VERSION = 7.7.3.0
MASTER_SERVER = wilma
EMM_SERVER = wilma
NB_MACHINE_TYPE = MASTER_SERVER
```

Example 3 – Request the server valbl8 to connect to the server host valbl7. Notice that the connect options that are user requested are ignored for communication between secure capable hosts. The connections are by a local host connection to the secure proxy process. The secure proxy process then secures the communication with the remote host. The connection to the remote host is made through the PBX or vnetd ports. Some key fields from the certificates, used to secure the connection, are included in the output.

```
# bptestbpcd -host valbl7 -verbose -connect_options 1 1 2
LOCAL_CERT_ISSUER_NAME = /CN=broker/OU=root@valbl8.min.veritas.com/O=vx
LOCAL_CERT_SUBJECT_COMMON_NAME = 59a8584a-2f88-4a21-8d91-62ceebc40c29
PEER_CERT_ISSUER_NAME = /CN=broker/OU=root@valbl8.min.veritas.com/O=vx
PEER_CERT_SUBJECT_COMMON_NAME = 4f0f2f15-1cde-4acd-9c82-9bd212741970
PEER_NAME = 10.0.91.128
HOST_NAME = valbl7
CLIENT_NAME = valbl7
VERSION = 0x08100000
PLATFORM = solaris_x86_10_64
PATCH_VERSION = 8.1
SERVER_PATCH_VERSION = 8.1
```
MASTER_SERVER = valb18
EMM_SERVER = valb18
NB_MACHINE_TYPE = MEDIA_SERVER
bptestnetconn

bptestnetconn – test and analyze various configurations and connections

SYNOPSIS

bptestnetconn [-v] -h | -b | -l
bptestnetconn [-v] [-i | -frap] [-s | -H hostname]
bptestnetconn [-v] [-c[service_name] [-o time_value] [-t time_value]]
[ -H hostname | -s ] [-x]
bptestnetconn -6 [-u]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\

DESCRIPTION

The bptestnetconn command performs several tasks that help you analyze DNS and connectivity problems with any specified list of hosts, including 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. The command can also perform and report the responsiveness of the NetBackup Web Service. The command also shows the connection direction, whether the communication was encrypted by a connection to the secure proxy process or not.

Logs for the bptestnetconn command are located in
/usr/openv/netbackup/logs/bptestnetconn/*.log for UNIX and Linux, and in
install_path\netbackup\logs\bptestnetconn\*.log for Windows.

OPTIONS

-6 or --afcheck

Checks the configuration for IP_ADDRESS_FAMILY requirements.
-a or --all
Reports all times. This option has the same effect as -fr. This condition is the default.

-b or --confchecker
Verifies that bp.conf (UNIX) or the NetBackup registry entry (Windows) exists.

-c or --connect service_name
Reports the connectToObject times to service. Some CORBA service examples are EMM/EMMServer, NBFSMCLIENT/FSM.ClientClusterMgr, nbrmms/DiskPollingService.DPS nbrmms/STSEventService, and nbsvcmcn/NBSvcMon (default). Type this option with no spaces between -c and service_name.

-e or --retrycount retry_count
Specifies the number of retries that are performed in case of web service connection failures. The default value of this parameter is 5.

-f or --flkup
Reports all forward DNS lookup times for the specified host or hosts.

-h or --help
Displays this help message.

-H hostname
Specifies a single host name of the system, IPv4 address, or name of a file containing a list of such names, one per line.

-i or --ipservers
Lists the IP addresses of all servers in the NetBackup configuration.

-l or --listservers
Lists all servers in the NetBackup configuration.

-O or --port port_number
Specifies the web service port to which the command connects. The default web service port is the PBX port, port number 1556.

-o or --objconntimeout time_value
Specifies the timeout in seconds for NetBackup level retries in case of CORBA errors.

-p or --prefnet
Includes how PREFERRED_NETWORK affects connections to the specified hosts or servers in the output display.

-r or --rlkup
Reports all reverse DNS lookup times for the specified host or hosts.
-s or --servers
Looks up all NetBackup servers in the configuration.

-T or --wsconntimeout time_value
Specifies the web service connection timeout in seconds. The
CLIENT_CONNECT_TIMEOUT specified in the NetBackup configuration is used
by default.

-t or --orbconntimeout time_value
Specifies the TCP timeout, the socket level time out for establishing the TCP/IP
connection. Specify -t larger than -o to distinguish between TCP/IP and
CORBA errors. Otherwise, all failures time out after retries_timeout seconds
(-o time_value).

-u or --update
Updates the bp.conf (UNIX) or the Host Properties (Windows) based on the
action of the --afcheck operation. This option is used only as part of installation.

-v or --verbose
Reports in verbose mode. The reverse lookup report shows which servers are
media servers, EMMSERVER (if not local), and if any server is also the
PREFERRED_NETWORK or CLUSTERNAME.

-w or --web webappname
Reports the web service responsiveness. The supported names for the
webappname value are the default nbwmc/netbackup and nbwmc/security.
Type this option with no spaces between -w and webappname.

-x or --skipproxyinfo
Skip displaying information about the secure CORBA connection via proxy.

EXAMPLES

Example 1 - List all the servers in the NetBackup configuration.

# bptestnetconn -l
knothead.example.com
www.google.com
r2d2.starwars.galaxy.com
whoknows.what.com
zebra
lawndartsvm2
lawndartsvm1

Example 2 - List all the non-default settings.
# bptestnetconn -b

CLIENT_PORT_WINDOW (min) = 2024 [0]
CLIENT_PORT_WINDOW (max) = 4048 [0]
CLIENT_CONNECT_TIMEOUT = 30 [300]
SERVER_CONNECT_TIMEOUT = 10 [30]
DEFAULT_CONNECT_OPTIONS (daemon port) = vnetd [Automatic]
CONNECT_OPTIONS = [configured]
PREFERRED_NETWORK = knothead [NULL]
FIREWALL_IN = [configured]
REVERSE_NAME_LOOKUP = PROHIBITED [ALLOWED]

Example 3 - Report all forward DNS lookup times for all NetBackup servers in the configuration.

# bptestnetconn -f -s

----------------------------------------------------------------------
FL: knothead.example.com -> 10.80.73.101 : 0 ms [local]
FL: www.google.com -> 74.125.19.106 : 0 ms
FL: r2d2.starwars.galaxy.com -> 0.0.0.0 : 4 ms
FL: whoknows.what.com -> 209.139.193.224 : 0 ms [cluster/ri]
FL: zebra -> 10.80.120.103 : 0 ms
FL: lawndartsvm2 -> 10.80.74.153 : 0 ms
FL: lawndartsvm1 -> 10.80.74.154 : 0 ms
----------------------------------------------------------------------

Slow (>5 sec) or/and failed forward lookups:

r2d2.starwars.galaxy.com : 0 sec [FAILED]

----------------------------------------------------------------------

Total elapsed time: 0 sec

Example 4 - Report all reverse DNS lookup times for all NetBackup servers in the configuration.

# bptestnetconn -r -s

----------------------------------------------------------------------
RL: 10.80.73.101 -> knothead.example.com : 0 ms
RL: 74.125.19.106 -> nuq04s01-in-f106.1e100.net : 156 ms MISMATCH
RL: **LKUP FAIL** -> r2d2.starwars.galaxy.com : 0 ms
RL: 209.139.193.224 -> **LKUP FAIL** : 739 ms
RL: 10.80.120.103 -> zebra.example.com : 0 ms
RL: 10.80.74.153 -> lawndartsvm2.example.com : 0 ms
RL: 10.80.74.154 -> lawndartsvm1.example.com : 0 ms
----------------------------------------------------------------------

Slow (>5 sec) or/and failed/mismatched reverse lookups:

www.google.com : 0 sec [MISMATCH] -> nuq04s01-in-f106.1e100.net
Example 5 - Report all reverse DNS lookup times for all NetBackup servers in the configuration.

```bash
# bptestnetconn -s -c -t 10 -o 5
```

---

Total elapsed time: 1 sec

---

Example 6 - Report NetBackup Web Service responsiveness for all NetBackup servers in the configuration.

```bash
# bptestnetconn -s -w -T 30 -e 2
```

```
nbwmc/netbackup web service test for host: server.domain.com : 450 ms [SUCCESS]
nbwmc/netbackup web service test for host: sample.server2.domain2.com : 800 ms [FAIL]
nbwmc/netbackup web service test for host: testvm2 : 550 ms [SUCCESS]
```

---

Example 7 - Report NetBackup Web Service responsiveness for the security webapp on a specified NetBackup master server.

```bash
# bptestnetconn -wnbwmc/security -T 30 -H server.domain.com
```

```
nbwmc/security web service test for host: server.domain.com : 450 ms [SUCCESS]
```

---

Example 8: Reports the Secure CORBA connection via proxy by connecting `nbsl` service on the `example.server.domain.com`

```bash
# bptestnetconn.exe -cnbsl/HSFactory -H example.server.domain.com -v
```

```
adding hostname = example.server.domain.com
```

Connecting to 'nbsl/HSFactory'

```
CN: example.server.domain.com : 91 ms [SUCCESS] PBX: No VNETD: No
Certificate Information:
local_cert_info: {
  "certificate_subject_common_name": "08a1395f-81fe-40c6-af59-2631988ca076",
```
Example 9: Skip secure CORBA connection information via proxy for host example.server.domain.com

# bptestnetconn -cnbsl/HSFactory -t 10 -o 5 -H example.server.domain.com -x
adding hostname = example.server.domain.com

Connecting to 'nbsl/HSFactory'
CN: example.server.domain.com : 126 ms [SUCCESS] PBX: No VNETD: No

Total elapsed time: 1 sec
bptpcinfo

bptpcinfo – discover SAN devices and creates 3pc.conf file

SYNOPSIS


The directory path to this command is /usr/openv/netbackup/bin/

DESCRIPTION

This command operates only on UNIX systems.

The bptpcinfo command discovers all the disk and the tape devices on Fibre Channel and SCSI connections. It provides information about each device (one line per device). By default, this command writes the information to the following file:

/usr/openv/volmgr/database/3pc.conf

Note: For off-host backup (Third-Party Copy Device or NetBackup media server backup methods), a 3pc.conf file must exist at /usr/openv/volmgr/database.

At the start of a backup, using the Third-Party Copy Device or NetBackup media server method, NetBackup automatically runs this command to create the 3pc.conf file if the file does not already exist. This file is complete and you do not need to rerun this command if any of the following is true:

- The backup uses the NetBackup media server backup method.
- You use the Third-Party Copy Device backup method and all required devices (such as disks, tapes, and third-party copy devices) support identification descriptors.

If any of the devices does not support identification descriptors, run the bptpcinfo command manually to create the 3pc.conf file. Then edit the file as explained in the SAN Configuration chapter of the NetBackup Snapshot Client Administrator’s Guide.
OPTIONS

-a

-c
Checks for syntax errors in an already existing 3pc.conf file (in /usr/openv/volmgr/database). If the 3pc.conf file does not exist, a message states that it cannot open the file. In that case, use other command options to create the file. Note that if -c is specified, any other options are ignored.

The -c option checks for syntax errors such as the following: missing spaces between entries, missing keywords (such as a worldwide name without "w="), or a worldwide name that is not 16 digits in length. Any such errors can cause the backup to fail.

-h
Displays the bptpcinfo usage statement.

-u
DisCOVERS ALL THE DISK DEVICES AND THE TAPE DEVICES ON THE FIBRE CHANNEL AND SCSI CONNECTIONS. IT ALSO ADDS ENTRIES IN THE 3pc.conf FILE (OR ALTERNATE THE OUTPUT FILE THAT IS SPECIFIED WITH THE -o OPTION) FOR NEW DEVICES THAT ARE FOUND. IF THE 3pc.conf FILE DOES NOT EXIST, THE -u OPTION FAILS (USE -a INSTEAD).

Note: To remove obsolete entries, use -r instead of -u. (The -u and -r options cannot be used together.)

-r
Removes any obsolete entries in the 3pc.conf file (or the alternate output file that is specified with the -o option). An obsolete entry is one that no longer corresponds to any devices on the Fibre Channel or SCSI connections.

Note: The -r option does not add entries to the 3pc.conf file for new or reconfigured devices. To add entries, use the -u option. (The -u and -r options cannot be used together.)
-v
*Specifies the verbose mode, which causes `bptpcinfo` to list information on its discovery progress. The information is written to the screen, not to the `3pc.conf` file.*

You can select the `-v` option to track problems in device discovery.

-d disk_device_directory
*Discovers all disks in the specified directory (usually `/dev/rdsk` on Solaris or Hewlett Packard Enterprise, and `/dev` on AIX) and creates new entries in the `3pc.conf` file. Or, it creates new entries in the alternate output file that is specified with the `-o` option by overwriting any current entries.*

To avoid overwriting the `3pc.conf` file, use the `-d` option with the `-u` option. When `-d` and `-u` are combined, the new disk entries are added to the existing entries.

-t tape_device_directory
*Discovers all tape drives in the specified directory (usually `/dev/rmt` on Solaris or Hewlett Packard Enterprise, and `/dev` on AIX) and creates new entries in the `3pc.conf` file. Or, it creates new entries in the alternate output file that is specified with the `-o` option by overwriting any current entries.*

To avoid overwriting the `3pc.conf` file, use the `-t` option with the `-u` option. When `-t` and `-u` are combined, the new tape entries are added to the existing entries.

-p physical_device
*Creates an entry for a physical device in the `3pc.conf` file, if the specified device is discovered. Or, it creates new entries in the alternate output file that is specified with the `-o` option by overwriting any current entries.*

To avoid overwriting the `3pc.conf` file, use the `-p` option with the `-u` option. When `-p` and `-u` are combined, the new entry is added to the existing entries.

-o output_file_name
*-o specifies an alternate (usually temporary) path for the `bptpcinfo` command output. If this option is not specified, the default is `/usr/openv/volmgr/database/3pc.conf`.*

-o -
*Sends the output to the screen. Note the space before the second hyphen.*
EXAMPLES

Example 1 - Discover all the source and the destination devices on the SAN and create the required 3pc.conf file in /usr/openv/volmgr/database.

```
# bptpcinfo -a
```

Example 2 - Discover all the source and the destination devices on the SAN, and send the output to the screen.

```
# bptpcinfo -a -o -
```

Sample output:

devid [p=devpath] [s=sn] [n=npid] [l=lun] [w=wwpn] [i=iddesc]
1 p=/dev/rdsk/c1t11d3s2 s=SEAGATE:ST19171N:LAE82305 l=3
2 p=/dev/rdsk/c1t13d4s2 s=SEAGATE:ST19101W:NH022724 l=4
3 p=/dev/rdsk/c1t20d0s2 s=HITACHI:OPEN-9:60159003900 l=0
4 p=/dev/rdsk/c1t20d1s2 s=HITACHI:OPEN-9:60159000000 l=1
5 p=/dev/rdsk/c1t20d2s2 s=HITACHI:OPEN-9:60159000100 l=2
6 p=/dev/rdsk/c1t20d3s2 s=HITACHI:OPEN-9-CM:60159001C00 l=3
7 p=/dev/rdsk/c1t20d4s2 s=HITACHI:OPEN-9:60159002B00 l=4
8 p=/dev/rdsk/c1t20d5s2 s=HITACHI:OPEN-9:60159002C00 l=5

Example 3 - Discover the devices in the /dev/rmt directory (/dev on AIX) and send the output to the screen:

On Solaris or Hewlett Packard Enterprise:

```
# bptpcinfo -t /dev/rmt -o -
```

Sample output:

```
devid [p=devpath] [s=sn] [n=npid] [l=lun] [w=wwpn] [i=iddesc]
0 p=/dev/rmt/0cbn s=QUANTUM:DLT8000:CX949P0164 l=1 i=10200E09E600000868
1 p=/dev/rmt/1cbn s=QUANTUM:DLT8000:CX949P1208 l=2 i=10200E09E600001381
2 p=/dev/rmt/4cbn s=QUANTUM:DLT8000:CX940P2790 l=2 i=1031000005013E000D3
3 p=/dev/rmt/7cbn s=QUANTUM:DLT7000:TNA48S0267 l=1
4 p=/dev/rmt/19cbn s=QUANTUM:DLT8000:PKB02P0989 l=1 i=10200E09E6000030C36
5 p=/dev/rmt/20cbn s=QUANTUM:DLT8000:PKB02P0841 l=2 i=10200E09E6000030DC5
```

On AIX:

```
# bptpcinfo -t /dev -o -
```

Sample output:
Example 4 - Create a `3pc.conf` file that describes all devices on the SAN, and send the output to an alternate file:

```bash
# bptpcinfo -a -o /usr/openv/volmgr/database/3pc_alt1.conf
```

**NOTES**

Note the following items when you use the `bptpcinfo` command:

- Run the `bptpcinfo` command when no backups are in progress. If a backup operation uses or reserves a device, `bptpcinfo` may be unable to obtain information on it. It omits such a device from the output.
- If you do not want to overwrite the existing `3pc.conf` file, include the `-o` option and specify the wanted location.
- If you have a host that runs Veritas SANPoint Control, do the following: Use the `bpSALinfo` command to add the worldwide name and LUN values for each device in the `3pc.conf` file. If you do not have SANPoint Control, you must edit the new entries in the `3pc.conf` file. To edit, manually add the worldwide name (WWPN) and LUNs for each device.
  
  For more about SAN Configuration, see the NetBackup Snapshot Client Administrator's Guide.

**FILES**

```
/usr/openv/volmgr/database/3pc.conf
```
bpup

bpup – start NetBackup services on Windows systems

SYNOPSIS

install_path\NetBackup\bin\bpup [-S|v] [-f] [-a] [-c] [-d] [-m] [-n] [-s]

DESCRIPTION

This command operates only on Windows systems.

The bpup command is used to start NetBackup services including the NetBackup databases, Media Manager, and clients.

OPTIONS

-\hs\ -s Enables you to select Silent Mode. With this option, no listing is generated and no confirmation is requested.
-\hv\ -v Selects the verbose mode and generates a detailed listing.
-\hf\ -f Forces the startup of the NetBackup services without prompting the user for a confirmation.
-\hc\ -c Starts the client.
-\hd\ -d Starts the NetBackup database.
-\hm\ -m Starts Media Manager.
-\hn\ -n Starts the NetBackup services.
-\hs\ -s Starts the server and not the client (NetBackup Media Manager).

SEE ALSO

See bpdown on page 120.
bpverify

bpverify – verify the backups that NetBackup creates

SYNOPSIS

[-sl sched_label] [-L output_file [-en]] [-policy name] [-s date]
[-e date] [-M master_server] [-Bidfile file_name] [-pt policy_type]
[-hoursago hours] [ [-cn copy number] | [-primary]] [-backupid
backup_id] [ [-id media_id or path] | [-stype server_type] [-dp
disk_pool_name [-dv disk_volume]]] [-priority number]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

bpverify verifies the contents of one or more backups by reading the backup
volume and by comparing its contents to the NetBackup catalog. This operation
does not compare the data on the volume with the contents of the client disk.
However, it does read each block in the image, which verifies that the volume is
readable. NetBackup verifies only one backup at a time and tries to minimize media
mounts and position time.

If either -Bidfile or -backupid is specified, bpverify uses this option as the sole
criterion for selecting the set of backups it verifies. If the command line does not
contain -Bidfile or -backupid, then bpverify selects the backups that satisfy all
the selection options. For example, if the command line looks like the following:

bpverify -pt Standard -hoursago 10

then bpverify verifies the set of backups with policy type Standard that run in the
past 10 hours.

If -p or -pb is specified, bpverify previews the set of backups that meet the
selection criteria. It displays the backup IDs, but does not perform the verification.

bpverify sends its error messages to stderr. It sends a log of its activity for the
current day to the NetBackup admin log file in the following directory:
UNIX systems:

/usr/openv/netbackup/logs/admin

Windows systems:

install_path\NetBackup\Logs\admin

Any authorized user can run this command.

For more about NetBackup authorization, see the *NetBackup Security and Encryption Guide*.

**OPTIONS**

-backupid backup_id
   Specifies the backup ID of a single backup to verify. This option takes precedence over any other selection criteria except -Bidfile. The default is any backup.

-Bidfile file_name
   Specifies a file that contains a list of backup IDs to be verified. This file is removed during the activation of the command line interface (CLI). This file is removed because the NetBackup GUIs commonly use this parameter. The GUIs expect the command-line interface to remove the temporary file that was used for the -Bidfile option upon completion. Direct command-line interface users can also use the option, however it removes the file.

   The file contains one backup ID per line. If this option is specified, other selection criteria are ignored. The default is no file of backup IDs, which means any backup can be verified.

-client name
   Specifies the name of the client that produced the original backup. The default is any client.

-cn copy_number | -primary
   Determines the copy number of the backup ID to verify. Valid values are 1 through the setting that the `bpconfig -max_copies` setting indicates, up to 10. The default is 1.

   -primary indicates that the primary copy should be verified rather than the copy.

(dp disk_pool_name | -dv disk_volume)
   Specifies the name of the disk pool, which is the data storage area for this storage unit. Optionally, `bpverify` verifies the images that reside on the
specified disk volume only. This option must be used with the -stype option. The disk pool must already exist.

-hoursago hours
Specifies the number of hours before the current time to search for backups. This number is equivalent to the specification of a start time (-s) of the current time minus hours. Do not use both this option and the -s option.

The hours value is a non-negative integer. The default starting time is 24 hours ago.

-id media_id | path
Search the image catalog for backups to verify that they are on this media ID or pathname. If a backup has some fragments on this media ID and some another media ID, the following occurs: NetBackup verifies a spanning image as long as the backup begins on the media of the media ID that is provided.

For the images that are stored on disk rather than removable media, specify an absolute pathname instead of media_id. The default is any media ID or pathname. BasicDisk uses this option.

-L output_file [-en]
Specifies the name of a file in which to write progress information. The default is not to use a progress file, in which case the progress information is written to stderr. For more information, see DISPLAY FORMATS later in this command description.

Example path for UNIX systems, /usr/openv/netbackup/logs/user_ops
Example path for Windows systems, c:\Program Files\Veritas\NetBackup\logs\user_ops

Include the -en option to generate a log entry in English. The name of the log contains the string _en. This option is useful to the support personnel that assist in a distributed environment where different locales may create logs of various languages.

Only default paths are allowed for this option and It is recommended to use the default paths. If you cannot use the NetBackup default path in your setup, you should add custom paths to the NetBackup configuration.

For more information on how to add a custom path, see the "BPCD_WHITELIST_PATH option for NetBackup servers and clients" topic in the NetBackup Administrator's Guide, Volume I.
-l
Specifies that the list type is long, which causes bpverify to write additional information to the progress log. The default list type is short. For additional information, see DISPLAY FORMATS later in this command description.

-local
If you initiate bpverify from a host other than the master server and do not use -local (default), the following occurs: bpverify starts a remote copy of the command on the master server.

The remote copy allows the command to be terminated from the Activity Monitor.

Use -local to prevent the creation of a remote copy on the master server and to run bpverify only from the host where it initiated.

If the -local option is used, bpverify cannot be canceled from the Activity Monitor.

-M master_server
Specifies the master server that provides the bpverify image data. The master server must allow access by the system that issued the bpverify command. The default is the master server for the system where bpverify is entered:

For NetBackup Server:
The default is always the master server where the command is entered.

For NetBackup Enterprise Server:
If the command is entered on a master server, then that server is the default.
If the command is entered on a remote media server, then the master for that media server is the default.

-p
Previews the verification, but does not perform the verification. For additional information, see DISPLAY FORMATS later in this command description.

-pb
Previews the verification but does not perform the verification. This option is similar to -p, but -pb does not display information about the individual backups. For additional information, see DISPLAY FORMATS later in this command description.

-policy name
Search for backups to verify in the specified policy. The default is any policy.

-priority number
Specifies a new priority for the verification job that overrides the default job priority.
-pt policy_type
    Specifies the policy type for selecting backups to verify. The default is any policy type.
    
    The valid policy types are the following:

    BigData
    DataStore
    DataTools-SQL-BackTrack
    DB2
    Enterprise-Vault
    FlashBackup
    Hyper-V
    Informix-On-BAR
    Lotus-Notes
    MS-Exchange-Server
    MS-SharePoint
    MS-SQL-Server
    MS-Windows
    NBU-Catalog
    NDMP
    Oracle
    PureDisk-Export
    SAP
    Split-Mirror
    Standard
    Sybase
    Vault
    VMware

-s date, -e date
    Specifies the start of the range of dates and times that include all backups to verify. The -e option specifies the end of the range.
    
    The required date and time values format in NetBackup commands varies according to your locale. The /usr/openv/msg/.conf file (UNIX) and the install_path\VERITAS\msg\LC.CONF file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.
    
    See "About specifying the locale of the NetBackup installation" in the NetBackup Administrator's Guide, Volume II.
    
    The valid range of dates is from 01/01/1970 00:00:00 to 01/19/2038 03:14:07. The default start time is 24 hours ago. The default ending time is the current date and time.
-sl sched_label
  Search for backups to verify that the specified schedule created. The default is all schedules.

-st sched_type
  Search for backups to verify that the specified schedule type created. The default is any schedule type.
  Valid values are:
  FULL (full backup)
  INCR (differential-incremental backup)
  CINC (cumulative-incremental backup)
  UBAK (user backup)
  UARC (user archive)
  NOT_ARCHIVE (all backups except user archive)

-stype server_type
  Specifies a string that identifies the storage server type. The server_type value can originate from one of the following sources:
  - Veritas provided storage. Possible values are AdvancedDisk and PureDisk.
  - Third-party disk appliances. The vendor supplies the server_type string.
  - Cloud storage. Use the csconfig cldprovider -l command to determine the possible server_type values. The cloud server_type values reflect the cloud storage provider. Cloud storage server_type values can also incorporate a suffix (for example, amazon_crypt). Possible suffixes are:
    - _raw: The NetBackup backup image is sent to the cloud in raw format. Use this option if you do not want to compress or encrypt data before sending to cloud storage.
    - _rawc: Compresses the data before it is written to the cloud storage.
    - _crypt: Encrypt the data using AES-256 encryption before writing the data to cloud storage. You must have KMS configured in NetBackup to use this option.
    - _cryptc: Compress and encrypt the data before writing to cloud storage.
  The storage server type is case sensitive.

-v
  Selects the verbose mode. When -v is specified, the debug logs and progress logs include more information. The default is not verbose.
DISPLAY FORMATS

Preview displays:

`bpverify` runs a preview by searching for backups and then by displaying them in one of the following ways (`bpverify` does not verify the backups):

- The `-p` display lists backup IDs that meet the criteria that the `bpverify` command-line options set. The `-p` information appears in volume order. For each volume that contains a selected backup, the media ID and server appear. The selected backup IDs that reside on that volume follow them.

- The `-pb` display is a brief version of the `-p` display. It lists the media ID and server for each volume that contains the backups that meet the selection criteria.

Verification displays:

`bpverify` creates these displays as it verifies images. If `bpverify` contains no option to set the list format, the display format is short. If the command line contains `-l`, the display format is long. If the command line contains both `-l` and `-L`, `bpverify` creates a file that contains the progress log.

The verification list appears in volume order in the following formats:

- In long format, `bpverify` displays the following information for each selected backup ID:
  - Policy, schedule, backup ID, media ID or path, and creation time
  - Files that are backed up
  - Any problems that `bpverify` detects while it verifies the image
  - Whether the image verification is successful or not

- In short format, `bpverify` does not list the files that were backed up.

EXAMPLES

Example 1 - Verify the backups that ran in the past 36 hours:

```
# bpverify -hoursago 36
Verify started Thu Feb  3 11:30:29 2012
INF - Verifying policy mkb_policy, schedule Full
(plim_0949536546), path /tmp/mkbunit, created 02/02/12 18:09:06.
INF - Verify of policy mkb_policy, schedule Full
(plim_0949536546) was successful.
INF - Status = successfully verified 1 of 1 images.
```

Example 2 - Compare the two preview displays, `-p` and `-pb`:
# bpverify -p -hoursago 200
Media id = A00002  Server = plim
Bid = plim_0949616279  Kbytes = 32800  Filenum = 1  Fragment = 1
Bid = gava_0949681647  Kbytes = 12191  Filenum = 2  Fragment = 1
Bid = gava_0949683298  Kbytes = 161  Filenum = 3  Fragment = 1
Bid = gava_0949683671  Kbytes = 11417  Filenum = 4  Fragment = 1
Bid = gava_0949684009  Kbytes = 11611  Filenum = 5  Fragment = 1
Bid = gava_0949684276  Kbytes = 806  Filenum = 6  Fragment = 1
Bid = gava_0949688704  Kbytes = 9869  Filenum = 7  Fragment = 1
Bid = gava_0949688813  Kbytes = 9869  Filenum = 8  Fragment = 1
Bid = gava_0949949336  Kbytes = 10256  Filenum = 9  Fragment = 1
Bid = plim_0949949337  Kbytes = 6080  Filenum = 9  Fragment = 1
Bid = plim_0949949337  Kbytes = 4176  Filenum = 10  Fragment = 2
Bid = gava_0949949686  Kbytes = 10256  Filenum = 11  Fragment = 1
Bid = plim_0949949687  Kbytes = 5440  Filenum = 11  Fragment = 1
Bid = plim_0949949687  Kbytes = 4816  Filenum = 12  Fragment = 2

Media id = 400032  Server = plim
Bid = toaster2_0950199621  Kbytes = 298180  Filenum = 1  Fragment = 1
Bid = toaster2_0950199901  Kbytes = 298180  Filenum = 3  Fragment = 1

# bpverify -pb -hoursago 200
Media id = A00002  Server = plim
Media id = 400032  Server = plim

**RETURN VALUES**

An exit status of 0 means that the command ran successfully. Any exit status other than 0 means that an error occurred.

If the administrative log function is enabled, bpverify logs the exit status in the administrative daily log under the log directory:

**UNIX systems:**

/usr/openv/netbackup/logs/admin

**Windows systems:**

install_path\NetBackup\logs\admin

It has the following form:

bpverify: EXIT status = exit status
If an error occurred, a diagnostic precedes this message.

**FILES**

**UNIX systems:**

/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/db/error/*
/usr/openv/netbackup/db/images/*

**Windows systems:**

install_path\NetBackup\logs\admin/*
install_path\NetBackup\db\error/*
install_path\NetBackup\db\images/*
cat_convert

cat_convert – run NetBackup catalog format conversion utility

SYNOPSIS

cat_convert -a2b [-o] [-s] [-v] source_file_directory
[target_file_directory]

cat_convert -check source_file

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

cat_convert converts NetBackup catalog .f files between version 3.4, 4.0v, or 4.5 ASCII format and 4.5 or later binary format. It automatically detects the source catalog file format and converts it to the other format.

The -dump option enables users to view the contents of the binary catalog image .f (dot-f) files. It echoes the contents of the .f file to stdout in a readable format. It also has helper options that limit the output to only certain records in the file or a subset of the output columns.

The -check option provides a consistency check on specified binary .f files.

The -decompress option allows you to decompress specified binary .f files that have been compressed using the .Z1 compression format. It also supports .Z format decompression on UNIX platforms.

If cat_convert detects inconsistencies, the utility generates up to four of the following reports that depend on the types of inconsistencies reported:

- Invalid Inode Report

  This report lists invalid inodes. The following is an example:
The following describes the column information in this report:

- **Type** - displays whether the item is a file or a directory.
- **Problem** - displays whether no data or no name is the cause of the invalid inode.
- **Additional information** - the path element name that is associated with the inode, the `filenum` field that the catalog received for the inode, or an error message.

### Invalid Directory Report
This report lists inconsistent directories. The following is an example:

<table>
<thead>
<tr>
<th>Index</th>
<th>InodeIndex</th>
<th>1stChild</th>
<th>1stDir</th>
<th>LastChild</th>
<th>NextIndex</th>
<th>NextDir</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2539</td>
<td>2230</td>
<td>5605F</td>
<td>-1</td>
<td>5605F</td>
<td>788763F</td>
<td>-1</td>
<td>JSP.cla</td>
</tr>
<tr>
<td>21281</td>
<td>2229</td>
<td>43380F</td>
<td>-1</td>
<td>1122108F</td>
<td>257809F</td>
<td>56110</td>
<td>fr.tmp</td>
</tr>
<tr>
<td>24157</td>
<td>3330</td>
<td>53103F</td>
<td>-1</td>
<td>2688747F</td>
<td>-1F</td>
<td>-1</td>
<td>UNKNOWN</td>
</tr>
<tr>
<td>36766</td>
<td>4406</td>
<td>98367F</td>
<td>-1</td>
<td>98367F</td>
<td>-1F</td>
<td>-1</td>
<td>Root</td>
</tr>
<tr>
<td>97393</td>
<td>5134</td>
<td>471040F</td>
<td>-1</td>
<td>3136322F</td>
<td>-1F</td>
<td>-1</td>
<td>udst.js</td>
</tr>
</tbody>
</table>

Total Directories: 150307
Total Files: 1137006

The following describes the column information in this report:

- **Index** - the relative position of the directory that is reported to the catalog.
- **Inode Index** - an index into the temporary file in which inode information is stored while the backup is in process.
- **1st Child** - the index to the first child (file or directory) under the listed directory. This value is -1 if there is no child. The character F follows the index if the first child is a file, or the character D follows the index if it is a directory.
- **1st Dir** - the index to the first directory under the listed directory. This value is -1 if there is no subdirectory.
- **Last Child** - the index to the last child (file or directory) under the listed directory. This value is -1 if there is no child. The character F follows the
index if the last child is a file, or the character D follows the index if it is a directory.

- **Next Index** - the index to the next sibling (file or directory) of the listed file. This value is -1 if there is no sibling. The character F follows the index if the next sibling is a file, or the character D follows the index if it is a directory.

- **Next Dir** - the index to the next sibling directory of the listed directory. This value is -1 if no sibling directory exists.

- **Name** - the short name of the directory if available, or UNKNOWN if not available.

**Invalid File Report**
This report lists inconsistent files. The following is the format of the report:

```
Index   Inode Index   Next Index   Name
2364    12180        2368F       Report.doc
39774   16642        39776D     UNKNOWN
```

The following describes the column information in this report:

- **Index** - the relative position of the file as reported to the catalog.

- **Inode Index** - an index into the temporary file in which inode information is stored while the backup is in process.

- **Next Index** - the index to the next sibling (either a file or directory) of the listed file. This value is -1 if there is no sibling. The character F follows the index if the next sibling is a file, or the character D follows the index if it is a directory.

- **Name** - the short name of the directory if available, or UNKNOWN if not available.

**Invalid Directory and File Report**
This report lists both inconsistent files and directories. The following is the format of the report:

```
Index   Inode   Type               Name
2363    11134   Directory /Documents/Directory 1
13679   10077   Directory /Documents/Directory 2
```

The following describes the column information in this report:

- **Index** - the relative position of the file as reported to the catalog.

- **Inode** - the inode number of the file or directory that is reported to the catalog.
- Type - displays whether the item is a file or a directory.
- Name - the short name of the directory if available, or UNKNOWN if not available.

Since this report traverses the directory tree, it may not list all of the files or directories that are reported in the first two reports. Since it provides the fully qualified name of the file or directory, it can be useful in problem resolution. It also provides the total number of files and directories.

These reports are not localized.

You must have administrator privileges to run this command.

OPTIONS

-a2b
Convert NetBackup 3.4, 4.0V, 4.5 ASCII format catalog .f file(s) to NetBackup 4.5 binary format .f file(s).

-check source_file
Checks the consistency of a binary .f file. source_file must be the fully qualified path. Inconsistencies may be due to faulty FlashBackup or NDMP type backups. If this utility detects no inconsistencies, it ends silently and returns a zero return code. If the utility detects any inconsistencies, it returns the number of inconsistencies and prints up to three reports depending on the types of inconsistencies reported.

-decompress compressed_file target_file_directory
Decompresses the specified compress binary .f file. compressed_file must be the fully qualified path. decompress decompresses catalog files that have been compressed using the .Zl compression format. On UNIX, it also supports .Z format decompression. target_directory is the directory where the decompress operation places the decompressed file.

-dump
Enables you to view the contents of catalog image .f files.

-erec num
Modifies the output from the cat_convert -dump. Stops the display of records at this record number.

Note: The record number is not necessarily the same as the file number in the first column of the output.
-nodata
Eliminates the data column from the output of the cat_convert -dump. The data column can result in excessively large outputs.

-noheader
Modifies the output from cat_convert -dump. An option that modifies the output from the cat_convert -dump. Eliminates the column headers.

-nopath
Modifies the output from cat_convert -dump. Eliminates the path column. The path column can result in excessively large outputs.

-o
Overwrite original catalog file content with the new format that converts. -o cannot be used with target_file_directory.

-s
Show statistic information to the console window.

-sep char
An option that modifies the output from cat_convert -dump. An option that modifies the output from the cat_convert -dump. Use char to separate the columns instead of the white-space default separation. For example, you can use this command to generate a comma-separated output.

-short
An option that modifies the output from cat_convert -dump. Limits the output to a subset of the usual columns.

-srec num
An option that modifies the output from cat_convert -dump. An option that modifies the output from the cat_convert -dump. Starts to display the records at this record number.

Note: The record number is not necessarily the same as the file number in the first column of the output.

target_file_directory
-v
Show current progress information.

Specify one of the following to convert:

- To specify a target file, the source must be a file.
- To specify a target directory, the source must be a directory.
If the source is a directory, you must use `-a2b`.

The new files that the conversion creates convert to the specified format, and the original file names are used in the target directory.

If you do not specify the target file or directory when you convert source files, the files the conversion process creates have an appended suffix. `_bin.f` or `_ascii.f`.

If the catalog `.f` file size is more than 4 megabytes, the binary catalog leaves output files separate. It puts them in the `catstore` directory.

EXAMPLES

Example 1

```bash
# cat_convert -a2b abc.f
```

If `abc.f` is in ASCII format, the `target_file_path` is `abc_bin.f`.

Example 2

```bash
# cat_convert -a2b abc.f
```

The contents of `abc.f` convert to binary.

Example 3

```bash
# cat_convert -dump -short abc.f
```

The contents of `abc.f` appear in `stdout` in a user-readable format.

SEE ALSO

See `cat_export` on page 487.

See `cat_import` on page 490.
cat_export

**cat_export** — export catalog image metadata from the NetBackup database (NBDB) to one or more flat ASCII image header files.

**SYNOPSIS**

```
cat_export -all | -client name | -backupid backupid | -mediahost hostname [-delete_source] [-replace_destination] [-export_dependents] [-export_no_dependents] [-staging [-source_master name]] [-base directory_name]
```

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\n
**DESCRIPTION**

The **cat_export** utility is used in specific scenarios to export image metadata from NBDB or a staged copy of NBDB to flat ASCII image header files in a target directory. It organizes the data into a directory hierarchy based on the hierarchy that is used in the NetBackup database.

**cat_export** is normally used in conjunction with the **cat_import** command as part of a disaster recovery scenario or to relocate image metadata information from one repository to another. More information is available on NetBackup disaster recovery.

For more about Disaster Recovery, see the **NetBackup Troubleshooting Guide**.

By default, **cat_export** exports the image metadata that is specified with the **-backupid** option as well as the image metadata that is dependent on the specified backup images.

You must have administrator privileges to run this command.

**OPTIONS**

- **-all**

  Exports the catalog image data of all the clients of the master server.
-base directory_name

Changes the target directory of the catalog metadata from the default directory netbackup/db.export to the specified directory name.

-backupid backupid

Exports the catalog image data of the specified backup ID.

-client name

Exports the catalog image data of the specified client.

-delete_source

Deletes the original image metadata in NBDB.

-export_dependents

Used with the -backupid and -client options to export VMware image metadata that is dependent on the specified backup image.

-export_no_dependents

Used with the -backupid, -client and -mediahost options to export the specified image header but not any of the dependent image metadata.

-mediahost hostname

Exports the catalog image data that has at least one fragment on the specified media host. The hostname value can be a media server or a snapshot client.

-replace_destination

Forces the new flat files to overwrite any existing flat files in the target directory.

-staging [-source_master name]

Specifies that the copy of the NBDB in the staging directory should be used as the source of the export operation instead of the NBDB. You can use this option for the following reasons:

- To export the image metadata to the legacy flat file format in the db.export (default) directory.
- To export the image metadata, so that you can import it into another copy of NBDB by using the cat_import command.

EXAMPLES

Example 1 - Export all image metadata for alfred into the /catExport/images/alfred directory:

# cat_export -base /catExport -client alfred

Example 2 - Export all NBDB image metadata to the netbackup/db.export directory:
Example 3 - Export only the image metadata related to client `hostname1` from the copy of NBDB that is located in the staging directory:

```
# cat_export -client hostname1 -staging
```

SEE ALSO

See `cat_convert` on page 481.
See `cat_import` on page 490.
cat_import

cat_import – migrate catalog image metadata from flat ASCII image header files into the NetBackup database (NBDB)

SYNOPSIS

cat_import -all | -client name | -backupid backupid [-delete_source] [-replace_destination] [-staging] [-base directory_name]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/
On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

The cat_import utility migrates catalog image metadata from flat ASCII image header files into the NetBackup database (NBDB) or a staged copy of NBDB. You can use the cat_import command line to move all image metadata or a subset of metadata based on client (-client) or backup ID (-backupid).

The cat_import utility can also be used with the cat_export command in the following ways: as part of a disaster recovery scenario or to relocate image metadata information from one repository to another. More information is available on NetBackup disaster recovery.

For more about Disaster Recovery, see the NetBackup Troubleshooting Guide.
You must have administrator privileges to run this command.

OPTIONS

-all
Imports the catalog image data of all the clients of the master server.

-base directory_name
Changes the source directory of the image metadata from the default directory netbackup/db.export to the specified directory name.

-backupid backupid
Imports the catalog image data of the specified backup ID.
-client name
  Imports the catalog image data of the specified client.

-delete_source
  Deletes the original image metadata from the source location.

-replace_destination
  Forces the utility to overwrite any pre-existing image metadata in the destination location.

-staging
  Specifies the copy of the NBDB in the staging directory to be used as the destination of the import operation instead of the NBDB itself. Use this operation in combination with the cat_export command to insert the image metadata into another copy of NBDB.

EXAMPLES

Example 1 - Import all image metadata from flat ASCII image header files:

  # cat_import -all

Example 2 - Import only the image metadata that is related to client hostname1 from associated flat ASCII image header files:

  # cat_import -client hostname1

SEE ALSO

See cat_convert on page 481.

See cat_export on page 487.
configureCerts

configureCerts – configures all the required certificates for the web server and updates the Java Key Store (JKS) with the latest certificate in the trust store.

SYNOPSIS

configureCerts [-renew_webserver_keys]
configureCerts [-update_trust_store]

On UNIX systems, the directory path to this command is /usr/openv/wmc/bin/install/

On Windows systems, the directory path to this command is install_path\NetBackup\wmc\bin\install\n
DESCRIPTION

The configureCerts command configures all the required certificates for the web server and updates the JKS with the latest certificate in the trust store. Additionally, the command is used to update the trust store of the web server configuration.

The command provides a way to regenerate the key-pairs for the web server that include:

- A key-pair for the web service user (the default web service user is nbwebsvc)
- A key-pair for the NetBackup Web Management Console (nbwmc)
- A key-pair for the web server services (that is a computer certificate)

After renewal of the key-pairs and their respective certificates, the command immediately updates the JKS file with the latest certificates that are available in trust store.

If the command is run without any option, it updates the JKS with the latest certificate that is available in the trust store.

On Windows systems, you must provide the password for the NetBackup Web Services account to successfully complete the key-pair renewal. To skip entering the password, set the WEBSVC_PASSWORD environment variable before you run the command. If you do not set this variable, the script prompts for the password three times:

- For the web service user (nbwebsvc)
- For the NetBackup Web Management Console (`nbwmc`)
- For the web server

**Note:** Be sure to stop the NetBackup Web Management Console service (`nbwmc`) before you renew the web server key-pairs.

The command logs to the `configureCerts_KeyPairRenewal.log` and `configureCerts.log` files at the location shown:

- **UNIX:** `/usr/openv/netbackup/wmc/webserver/logs`
- **Windows:** `install_path\NetBackup\wmc\webserver\logs`

**OPTIONS**

- `renew_webserver_keys`
  - Regenerates the key-pair and the respective certificates for the web server configuration.

- `update_trust_store`
  - Updates the trust store of the web server configuration. This option does not update the JKS or regenerate the key-pair of web server configuration.
configureCertsForPlugins

configureCertsForPlugins - configure the NetBackup VMware plug-in or Microsoft add-in for an external certificate.

SYNOPSIS

configureCertsForPlugins -registerExternalCert -certPath "path_to_external_certificate_file" -privateKeyPath "path_to_certificate_key_file" -trustStorePath "path_to_ca_certificate_file"

configureCertsForPlugins -registerNBCAcert

On UNIX systems, the directory path to this command is
/usr/openv/wmc/bin/install/

On Windows systems, the directory path to this command is
install_path\NetBackup\wmc\bin\install\n
DESCRIPTION

The configureCertsForPlugins command configures the plug-in or add-in to communicate with a NetBackup master server that uses an external certificate. This command can also configure the plug-in to communicate with a NetBackup master server that was reconfigured to use a NetBackup CA-signed certificate.

This command can be used for the following NetBackup plug-ins:

- NetBackup plug-in for vSphere Web Client
- NetBackup plug-in for vSphere Client (HTML5)
- NetBackup add-in for Microsoft SCVMM Console

Note: Additional steps are needed to complete the certificate configuration for the plug-in or add-in. See the procedure on configuring an external certificate in the appropriate NetBackup 8.1.3 plug-in or add-in guide.
OPTIONS

-certificatePath "path_to_external_certificate_file"
    Specifies the path to the certificate for the web server. This file should have a
    single certificate in PEM format.

-privateKeyPath "path_to_certificate_key_file"
    Specifies the path to the private key for the web server certificate.

-registerExternalCert
    Configures the plug-in or add-in to use an external certificate.

-registerNBCAcert
    Configures the plug-in or add-in to use a NetBackup CA-signed certificate.

-trustStorePath "path_to_ca_certificate_file"
    Specifies the path to the certificate of the intermediate or root certification
    authority that has issued the web server certificate. This file should have a
    single certificate in PEM format. The subject of this certificate should match
    the issuer of the web server certificate.

EXAMPLES

Example 1: Configure the plug-in to communicate with a NetBackup master server
that uses an external certificate.

    # configureCertsForPlugins -registerExternalCert -certificatePath "c:\server.
    pem" -privateKeyPath "c:\key.pem" -trustStorePath "c:\
    intermediateOrRootCA.pem"

Example 2: Reconfigure the plug-in to communicate with a NetBackup master server
that uses a self-signed certificate.

    configureCertsForPlugins -registerNBCAcert
configureMQ

configureMQ – configures the NetBackup Messaging Broker service.

SYNOPSIS

configureMQ [-defaultPorts] | [-externalPort port1 -internalPorts port2 port3 port4]

configureMQ -enableCluster

configureMQ -disableCluster

On UNIX systems, the directory path to this command is
/usr/openv/mqbroker/bin/install/

On Windows systems, the directory path to this command is
install_path\NetBackup\mqbroker\bin\install

DESCRIPTION

Use this command to configure NetBackup Messaging Broker or nbmqbroker service. The service is required to initiate the connection between NAT clients and the NetBackup master server or the media server.

In a cluster configuration, you can run the configureMQ command only on the active node.

OPTIONS

-defaultPorts
  Specifies the default internal and external communication ports for the NetBackup Messaging Broker service.
  The default external port is 13781. The default internal ports are 13780, 13779, and 13778. Ensure that the default port numbers are available for use.

-disableCluster
  Disables monitoring of the NetBackup Messaging Broker service in the cluster.

-enableCluster
  Enables the cluster to monitor the NetBackup Messaging Broker service.
Specify external and internal communication ports for the NetBackup Messaging Broker service. Use these options if you want to specify the ports other than the default ports. Ensure that the port numbers that you specify are unique and available for use.

The external port must be accessible to other NetBackup hosts.

**EXAMPLES**

Example: Configure the NetBackup Messaging Broker service with the non-default ports.

```
configureMQ -externalPort 13832 -internalPorts 13833 13834 13835
```
configurePorts

configurePorts – configure the web ports for the Web Services Layer (WSL) application on the master server

SYNOPSIS

configurePorts -httpPort http_port | -httpsPort https_port | -shutdownPort shutdown_port
configurePorts -autofindports value
configurePorts -overrideCluster value
configurePorts -status
configurePorts -addLegacyCloudService
configurePorts -removeLegacyCloudService

On UNIX systems, the directory path to this command is /usr/openv/netbackup/wmc/bin/install/configurePorts/

On Windows systems, the directory path to this command is install_path\NetBackup\wmc\bin\install\configurePorts\n
DESCRIPTION

The NetBackup plug-in for VMware vCenter includes a NetBackup Recovery Wizard for restoring virtual machines. The NetBackup Recovery Wizard requires the proper configuration of web ports for the Web Services Layer (WSL) application on the master server. Without the correct port configuration, you cannot authorize the plug-in to restore virtual machines that were backed up by that master server.

If the web ports (http, https, and shutdown) are not correctly configured on the master server, use the configurePorts command to manually configure the ports.

You must have administrator privileges to run this command.

OPTIONS

-addLegacyCloudService

   Enables the communication between the master server and the media server on port 5637. The NetBackup Web Management Console (nbwmc) service running on the master server uses this port to communicate with media servers
configured for cloud storage. You must restart the NetBackup Web Management Console (nbwmc) service for the changes to take effect.

This option is applicable for media server versions 7.7.x to 8.1.2 only.

- `autofindports`
  Valid values are true and false.

- `httpPort http_port_number`
  Specifies the http port number.

- `httpsPort https_port_number`
  Specifies the https port number.

- `overrideCluster value`
  Overrides the ports that are used on all nodes of the cluster for a master server that is clustered. Valid values are true and false.

  This option updates the following file on shared disk:

  Windows:

  `install_path\NetBackup\var\global\wsl\portfile`

  UNIX or Linux:

  `/usr/openv/netbackup/var/global/wsl/portfile`

  The NetBackup installer for WSL uses this file during installation in a clustered mode.

- `removeLegacyCloudService`
  Disables communication between the master server and the cloud storage media server on port 5637. You must restart the NetBackup Web Management Console (nbwmc) service for the changes to take effect.

  Port 5637 is no longer used after the legacy media servers are upgraded to version 8.2 or later. This option disables the NetBackup Web Management Console (nbwmc) service usage on the port.

- `shutdownPort shutdown_port`
  Specifies the shutdown port number.

- `status`
  Displays the current port numbers.

**EXAMPLE**

Configure the http port on the master server to 8443.

```bash
# configurePorts -httpPort 8443
```
configureWebServerCerts

configureWebServerCerts – provides a way to enable the NetBackup domain to support NetBackup or external certificate authorities. Lets the user configure certificates for the NetBackup web server.

SYNOPSIS

configureWebServerCerts -addNBCert
configureWebServerCerts -removeNBCert [-force]
configureWebServerCerts -addExternalCert [-nbHost | -webUI | -all] 
{[-certPath path_to_certificate_file] [-privateKeyPath path_to_certificate_key_file] [-trustStorePath path_to_CA_certificate_file] [-passphrasePath path_to_passphrase_file]} [-crlCheckLevel DISABLE | LEAF | CHAIN] [-crlPath directory_path_to_CRLs]
configureWebServerCerts -addExternalCert [-nbHost | -webUI] [-copyNbHost | -copyWebUI ]
configureWebServerCerts -removeExternalCert [-nbHost | -webUI | -all] [-force]
configureWebServerCerts -validateExternalCert 
{[-certPath path_to_certificate_file] [-privateKeyPath path_to_certificate_key_file] 
[-trustStorePath path_to_CA_certificate_file] 
[-passphrasePath path_to_passphrase_file] [-crlCheckLevel DISABLE | LEAF | CHAIN] [-crlPath directory_path_to_CRLs] [-fmt DETAILS | FAILURES_ONLY]}

On UNIX systems, the directory path to this command is /usr/openv/wmc/bin/install/

On Windows systems, the directory path to this command is install_path\NetBackup\wmc\bin\install\
DESCRIPTION

The configureWebServerCerts command provides a way to configure external or NetBackup certificates for the NetBackup web server. A NetBackup web server instance uses the Java Keystore as the repository for security certificates.

You must have root or administrator rights on the master server to run this command.

If you are running this command for the first time, you need to restart the NetBackup Web Management Console service (nbwmc) after you run the command.

If the NetBackup Messaging Broker (nbmqbroker) service is enabled, then you must restart the service after you successfully run the configureWebServerCerts command.

NetBackup does not support Windows certificate store as a source for the NetBackup web server certificates.

This command does not apply to the NetBackup appliance.

OPTIONS

- `--addExternalCert`
  Configures an external certificate for the web server.

- `--addNBCert`
  Configures the NetBackup certificate authority signed certificate for the web server.

- `--all`
  Configures an external certificate for communication between NetBackup hosts as well as with the NetBackup web user interface.

- `--certPath`
  Specifies the path to the certificate file. This command does not support the use of Windows certificate store paths.

A certificate file must have a certificate chain with certificates in the correct order. The chain starts with the server certificate, also known as the leaf certificate, followed by zero or more intermediate certificates. The chain must contain all intermediate certificates up to the Root CA certificate but should not contain the Root CA certificate itself. The chain is created such that each certificate in the chain signs the previous certificate in the chain.

The certificate file should be in one of the following formats:

- PKCS #7 or P7B file that is either DER or PEM encoded that has certificates in the specified order.
-copyNbHost
   Specifies that web UI communication uses the same certificate that is used for host communication.

-copyWebUI
   Specifies that host communication uses the same certificate that is used for web UI communication.

-crlCheckLevel
   Specifies the revocation check level for external certificates of the host. You can specify the following values:
   ■ DISABLE: Revocation check is disabled. Revocation status of the certificate is not validated against the CRL during host communication.
   ■ LEAF: The revocation status of the leaf certificate is validated against the certificate revocation list (CRL). LEAF is the default value for this option.
   ■ CHAIN: The revocation status of all certificates in the certificate chain are validated against the CRL.

-crlPath
   Specifies the path to the directory where the certificate revocation lists (CRL) of the external CA are located.

-fmt DETAILS | FAILURES_ONLY
   Provides details of the validation checks that are run for the external certificate-specific configuration options. The DETAILS option provides a report of all successful and all failed validation checks. The FAILURES_ONLY option provides a report of only the failed checks.

-force
   Use the -force option to forcefully remove certificate. After the removal, if there is no certificate configured for the web server, the NetBackup Web Management Console service cannot start.

-nbHost
   Configures an external certificate for communication between NetBackup hosts.

-passphrasePath
   Specifies the path to the passphrase file that stores the passphrase, which is used to encrypt the private key.

-privateKeyPath
   Specifies the path to the private key file of the certificate.
NetBackup supports PKCS #1 and PKCS #8 formatted private keys that are either plain text or encrypted. These may either be PEM or DER encoded. If, however, the key is PKCS #1 encrypted, it must be PEM encoded. For encrypted private keys, NetBackup supports the following encryption algorithms:

- DES, 3DES, and AES if the private key is in the PKCS #1 format.
- DES, 3DES, AES, RC2, and RC4 if the private key is in the PKCS #8 format.

**-removeExternalCert**

Removes the external certificate that you have configured for the web server for communication between NetBackup hosts, the NetBackup web user interface, or both, based on the option you have configured. Use this command with the `-nbHost`, `-webUI`, or `-all` options.

**-removeNBCert**

Removes the NetBackup certificate that you have configured for the web server for communication between NetBackup hosts as well as with the NetBackup web user interface.

**-trustStorePath**

Specifies the path to the certificate authority bundle file. The certificate authority bundle file should be in one of the following formats:

- PKCS #7 or P7B file having certificates of the trusted root certificate authorities that are bundled together. This file may either be PEM or DER encoded.
- A file containing the PEM encoded certificates of the trusted root certificate authorities that are concatenated together.

**-validateExternalCert**

Verifies whether the external certificate-specific configurations that are provided are valid or not. It provides a report of successful and failed validation checks.

**-webUI**

Configures an external certificate for communication with the NetBackup web user interface.

**EXAMPLES**

Example 1: Configure an external certificate for the web server for NetBackup host communication.

```bash
configureWebServerCerts -addExternalCert -nbHost -certPath /root/example_certs/device.crt -privateKeyPath /root/example_certs/device.key -trustStorePath /root/example_certs/rootCA.pem -passphrasePath root/example_certs/PassPhrase.txt
```
Example 2: Configure an external certificate for the web server for host communication using the certificate that you have configured for communication with web UI.

```bash
configureWebServerCerts -addExternalCert -webUI -copyNbHost
```

Example 3: Remove the external certificates that you have configured for all kinds of communication - web UI and NetBackup host.

```bash
configureWebServerCerts -removeExternalCert -all
```
create_nbdb

create_nbdb – create NBDB database manually

SYNOPSIS


create_nbdb -upgrade [-scripts db_scripts_directory] [-out db_scripts_output_directory] [-db_server |-server db_server_name] [-db_home pathname]

create_nbdb -drop_only [current_data_directory] [-db_server |-server db_server_name] [-db_home install_path] [-force]

create_nbdb -config_only [-dba password] [-force]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\

DESCRIPTION

This command is used to create the NetBackup database (NBDB) manually. This command can be used to drop the existing NBDB database, and to re-create it by using the non-default parameters that were used during installation. A user can perform the following actions:

- Change the default location of the data, index, and transaction log files.
- Change the size of the pre-allocated database files.
- Add an additional mirrored transaction log for increased database protection.
- Create the catalog configuration file (vxdbms.conf) from the information in the bp.conf file.
- Upgrade the NBDB.
OPTIONS

Without any options, the create_nbdb command verifies the version of an existing database and is used during upgrades. If a database does not exist, it creates it by using default parameters.

- **-config_only**
  Creates the vxdbms.conf file from the information available in the bp.conf file.

- **-data data_directory**
  Used to identify the directory of the main database files. If the pathname data_directory includes an embedded space, put the entire pathname in quotes. For example:

  ```
  create_nbdb -data "Program Files\NetBackup\bin\data"
  ```

- **-db_home install_path**
  Specifies the location of the database directory. The default directory is /usr/openv/db ..\Veritas\NetBackupDB.

- **-dba new_password**
  A new, randomly generated password is set during NetBackup installation. Use this option to set the password for the NBDB and the BMRDB databases for all DBA and application accounts. To change only the password for an existing database, use nbdb_admin -dba new_password. The password needs to be an ASCII string. Non-ASCII characters are not allowed in the password string.

- **-drop**
  Drops the existing NBDB database and creates a fresh empty database.

- **-drop_only**
  Drops the existing NBDB database.

- **-force**
  Performs the operation without user interaction.

- **-index index_directory**
  Used to identify the directory of the index database files.

- **-mlog log_mirror_directory**
  Used to create a mirrored log for increased database protection.

- **-noemm**
  Indicates that this server is not the EMM server (used to upgrade the BMR server).
-out db_scripts_output_directory
    Specifies the destination directory where `create_nbdb` sends the output results of running the upgrade scripts.

-scripts db_scripts_directory
    Specifies the location of the database upgrade scripts.

-server db_server_name
    Specifies the name of the database server.

-staging staging_directory
    Specifies the location of the staging directory that is used during catalog backup and recovery.

-sz small | medium | large
    Changes the size of the pre-allocated database files. During installation, the default size that is used is `small`.

-tlog log_directory
    Identifies the location of the transaction log.

-upgrade
    Upgrades the NetBackup database (NBDB).

SEE ALSO

See `nbdb_backup` on page 616.
See `nbdb_move` on page 618.
See `nbdb_ping` on page 620.
See `nbdb_restore` on page 621.
See `nbdb_unload` on page 623.
csconfig cldinstance

The cldinstance option for the csconfig command sets and fetches the cloud instance configuration settings.

SYNOPSIS

Synopsis information for Amazon S3

csconfig cldinstance

[-a -in instance_name -pt provider_type -sh service_host_name [-se service_endpoint_path] [-access_style access_style_type] [-http_port port_no] [-https_port port_no]]

[-ar -in instance_name -lc location_constraint [,location_constraint,location_constraint] -rn region_name [,region_name,region_name] -sh service_host [,service_host,service_host]]

[-as -in instance_name -sts storage_server_name [-storage_class storage_class] [-obj_size object_size] [-ssl 0|1|2] [-crl 0|1] [-pxtype proxy_type -pxhost proxy_host -pxport proxy_port [-pxtunnel proxytunnel_usage] [-pxauth_type proxy_auth_type [-pxuser_name proxy_user_name ]]] [-lc location_constraint,location_constraint] [-creds_broker creds_broker -url service_url -mission mission -agency agency -role role -cert_file cert_file_name -key_file private_key_file_name [-key_pass private_key_passphrase]]]

[-at api_type]

[-i [-pt provider_type | -at api_type | -in instance_name]]

[-l [-pt provider_type | -at api_type] [-at]

[-r -in instance_name]

[-rr -lc location_constraint [,location_constraint,location_constraint] -in instance_name]

[-rs -in instance_name -sts storage_server_name]

[-u -in instance_name [-sh service_host_name] [-se service_endpoint_path] [-http_port port_no] [-https_port port_no] [-access_style access_style_type]]
[-ur -in instance_name -lc location_constraint] -rn region_name -sh service_host_name
[-us -in instance_name -sts storage_server_name [-ssl ssl_usage]
[-crl crl_usage] [-lc location_constraint,location_constraint
[-auth_lc authentication_location_constraint] [-del_lc
color_constraint [,location_constraint,location_constraint]]
[-pxtype proxy_type -pxhost proxy_host -pxport proxy_port [-pxtunnel
proxytunnel_usage] [-pxauth_type proxy_auth_type [-pxuser_name
proxy_user_name]]] [-url service_url -mission mission1 -agency agency1
-role role1 -cert_file cert_file_name1 -key_file
private_key_file_name1 [-key_pass private_key_passphrase]]

Synopsis information for Microsoft Azure

[-as -in instance_name -sts storage_server_name [-storage_tier
storage_tier] [-ssl 0|1|2] [-crl 0|1] [-pxtype proxy_type -pxhost
proxy_host -pxport proxy_port [-pxtunnel
proxytunnel_usage]
[-pxauth_type proxy_auth_type [-pxuser_name proxy_user_name ]]]
[-at api_type]
[-i [-pt provider_type | -at api_type | -in instance_name]]
[-l [-pt provider_type | -at api_type]
[-rs -in instance_name -sts storage_server_name]
[-us -in instance_name -sts storage_server_name [-ssl ssl_usage]
[-crl crl_usage] [-pxtype proxy_type -pxhost proxy_host -pxport
proxy_port [-pxtunnel proxytunnel_usage] [-pxauth_type proxy_auth_type
-pxuser_name proxy_user_name ]]]

Synopsis information for Openstack Swift

[-a -in instance_name -pt provider_type [-auth_id
authentication_identifier | [-auth_ver authentication_version
-auth_url authentication_url]]
[-as -in instance_name -sts storage_server_name [-pxtype proxy_type
-pxhost proxy_host -pxport proxy_port [-pxtunnel proxytunnel_usage]
[-pxauth_type proxy_auth_type [-pxuser_name proxy_user_name]]]
[-tenant_type id | name -tenant_value tenant_value -sr
storage_region_name ] [-user_type id | name -user_value user_value
[,user_value,user_value] [-user_domain_type id | name
-user_domain_value user_domain_value] -project_type id | name
-project_value project_value [-project_domain_type id | name]
DESCRIPTION

The `csconfig` command manages the Cloud Connect configuration settings from a remote or a local computer. The `cldinstance` option sets and fetches the cloud instance configuration settings.

Using this option, you can add, update, or delete only customized cloud instances and storage servers.

OPTIONS

Parameters for option `-a`

Use this option to add a new cloud instance.
-access_style access_style_type

Use this option to provide the endpoint access style for the cloud service provider.

Only Amazon S3 supports this option.

Valid values for -access_style_type are as follows:

- 1 - Virtual Hosted Style
- 2 - Path Style

The default value for access_style_type is 2.

-auth_id authentication_identifier

Use this option to provide the identifier for the authentication URL.

Only OpenStack Swift supports this option.

-auth_url authentication_url

Use this option to provide the authentication URL provided by your cloud vendor.

The authentication URL is composed of either HTTP or HTTPS and a port number.

Only OpenStack Swift supports this option.

-auth_ver authentication_version

Use this option to provide the authentication version that you want to use.

Only OpenStack Swift supports this option.

-http_port port_no

Use this option to provide the HTTP port with which you can access the cloud provider service in a non-secure mode.

Only Amazon S3 supports this option.

-https_port port_no

Use this option to provide the HTTPS port with which you can access the cloud provider service in a secure mode.

Only Amazon S3 supports this option.

-in instance_name

Use this option to provide the cloud instance name.

-pt provider_type

Use this option to provide the cloud provider type.

When you use this option to add an OpenStack Swift cloud instance, you must first determine if the Authentication Identifier, the Authentication Version, and the Authentication URL are available within NetBackup. You can list this information with the command shown:
csconfig cldprovider -i -pt provider_type

Add the cloud instance with one of the commands shown:

- If your Provider Type lists an Authentication Version and an Authentication URL under Location Name, you can use the Authentication Identifier in this command:
  
  csconfig cldinstance -a -in instance_name -pt provider_type
  -auth_id authentication_identifier

- If there is no Location Name section under your Provider Type, you must use the cloud vendor provided information. Use the cloud vendor provided Authentication Version value and find the corresponding value under the Credentials Broker Supported section. Use this value and the Authentication URL provided by your cloud vendor in the command shown:
  
  csconfig cldinstance -a -in instance_name -pt provider_type
  -auth_ver authentication_version -auth_url authentication_url

-se service_endpoint_path

Use this option to provide the cloud service provider endpoint.

For example, in case your cloud provider service can be accessed using the https://service.my-cloud.com/services/objectstore URL, the cloud service endpoint value is /services/objectstorage.

You can leave the value blank, if the cloud provider service can be accessed directly from the https://service.my-cloud.com URL.

Only Amazon S3 supports this option.

-sh service_host_name

Use this option to provide the cloud service provider host name.

If you want to add a public cloud instance, you need to get the service host details from the cloud storage provider.

If you want to add a cloud storage instance for a private cloud deployment, use the host name that is specified in the URL using which you can access your cloud provider. For example, if the URL is https://service.my-cloud.com/services/objectstore, the host name is service.my-cloud.com.

Do not prefix the service host name with HTTP or HTTPS.

Only Amazon S3 supports this option.

Parameters for option -ar

Only Amazon S3 supports this option.
Use this option to add a region for a specific cloud instance. When you add a region, access is restricted to the specified region.

-in instance_name
   Use this option to provide the cloud instance name.

-lc location_constraint
   Use this option to provide the location identifier that the cloud provider service uses to access the buckets of the associated region. For a public cloud storage, you need to get the location constraint details from the cloud provider.

-rn region_name
   Use this option to provide a logical name to identify a specific region where the cloud storage is deployed.

-sh service_host
   Use this option to provide the service host name for the region.

Parameters for option -as

Use this option to add a cloud storage server for the cloud instance.

-agency agency
   Use this option to specify the agency name the cloud provider supplied.
   Only Amazon S3 supports this option with AmazonGov Cloud.

-cert_file cert_file_name
   Use this option to provide the certificate file name.
   The files that are mentioned in the parameters should exist on the master server at the following location:
   - On Windows: install_path\netbackup\db\cloud
   - On UNIX: install_path/netbackup/db/cloud
   Only Amazon S3 supports this option with AmazonGov Cloud.

-creds_broker creds_broker
   Use this option to provide the credential broker details. The creds_broker parameter is optional.
   When you do not specify the creds_broker parameter, CREDS_PROMPT is used by default and you do not need to specify the parameters following creds_broker in the given syntax.
   If you want to use access key credentials, use CREDS_PROMPT. The Amazon S3 connector directly communicates with the S3 service host using the access keys.
If you want to use the CAP service as your credentials broker, use `CREDS_CAP`.

Only the AmazonGov Cloud supports the `CREDS_CAP` option.

If you want to use AWS IAM Role use `CREDS_ROLE`. Only Amazon S3 and AmazonGov Cloud support the `CREDS_ROLE` option.

The valid values for `creds_broker` are:

- `CREDS_PROMPT` (default value).
- `CREDS_CAP`
- `CREDS_ROLE`

 `-crl`

Use this option to verify if the SSL certificate must be checked for revocation before communication is established between NetBackup and cloud storage provider. This option can be enabled only if the SSL option is enabled. All cloud providers that use CA signed SSL certificates support this option. Valid values are:

- 0 - Disables certificate revocation check
- 1 - Enable certificate revocation check

 `-in instance_name`

Use this option to provide the cloud instance name.

 `-key_file private_key_file_name`

Use this option to specify the private key file name the cloud provider supplied. The files that are mentioned in the parameters should exist on the master server at the following location:

- On Windows: `install_path\netbackup\var\global\wmc\cloud`
- On UNIX: `install_path/var/global/wmc/cloud`

Only Amazon S3 supports this option with AmazonGov Cloud.

 `-key_pass private_key_passphrase`

Use this option to specify the private key pass phrase the cloud provider supplied. It must be 100 or fewer characters.

Only Amazon S3 supports this option with AmazonGov Cloud.

 `-lc location_constraint`

Use the `-lc location_constraint` parameter for adding a region to a storage server. You can configure multiple regions with one storage server.

Only Amazon S3 supports this option.
Considerations for the `-lc location_constraint` parameter

- NetBackup uses with the first region (authentication location) you have specified as location constraint to:
  - Verify the credentials.
  - Get the information of all the buckets.
  - Ensure that the associated cloud instance supports the region.
  - Use an empty set of double quotation marks (""") to provide a blank value.

-`-mission mission`
  Use this option to specify the mission name the cloud provider supplied.
  Only Amazon S3 supports this option with AmazonGov Cloud.

-`-obj_size object_size`
  During the creation of a cloud storage server, you can specify a custom value for the `object_size`. Considerations for this value include the cloud storage provider, hardware, infrastructure, expected performance, and other factors.
  Once you set the `object_size` for a cloud storage server, you cannot change the value. If you want to set a different `object_size`, you must recreate the cloud storage server.

-`-project_domain_type id | name`
  Use this option to specify if you want to use either the project's domain ID or domain name that is associated with your cloud storage credentials.
  Only OpenStack Swift supports this option.

-`-project_domain_value -project_domain_type_value`
  Use this option to provide either the project's domain ID or domain name value that is associated with your cloud storage credentials.
  Only OpenStack Swift supports this option.

-`-project_type id | name`
  Use this option to specify if you want to use the project ID or project name that is associated with your cloud storage credentials. When you provide the project ID, project name and domain information is not required.
  Only OpenStack Swift supports this option.

-`-project_value project_value`
  Use this option to provide the project ID or project name value that is associated with your cloud storage credentials.
  Only OpenStack Swift supports this option.
-pxauth_type proxy_auth_type
   Use this option to provide the authentication type that must be used for proxy
type HTTP.
   Valid values are as follows:
   ■ NONE (Disables authentication)
   ■ BASIC
   ■ NTLM

-pxhost proxy_host
   Use this option to provide the host name and IP address of the proxy server.

-pxport proxy_port
   Use this option to provide the port number of the proxy server.

-pxtunnel proxy_tunnel_usage
   Use this option to specify if you want to use proxy tunneling.
   Valid values are as follows:
   ■ 0: Disable
   ■ 1: Enable (Default)
   Proxy tunneling is supported only for proxy type HTTP.

-pxtype proxy_type
   Use this option to provide the proxy type of the proxy server.
   Valid values are as follows:
   ■ HTTP
   ■ SOCKS
   ■ SOCKS4
   ■ SOCKS4A
   ■ SOCKS5
   ■ NONE (Disables the proxy type)

-pxuser_name proxy_user_name
   Use this option to provide the user name of the proxy server.

-role role
   Use this option to provide the role.
   Only Amazon S3 supports this option.
-sr  storage_region_name
    Use this option to provide the cloud storage region. You may use the cloud
    storage region that is geographically closest to the NetBackup media server
    that sends the backups to the cloud. You must use the value which was derived
    using -lr option.

    Only OpenStack Swift supports this option.

-ssl  -ssl 0, -ssl 1, -ssl 2
    Use this option to specify the SSL (Secure Sockets Layer) protocol for user
    authentication or data transfer between NetBackup and cloud storage provider.

    Only Amazon S3 supports this option.

    Valid values are as follows:
    ■  0 - Disable SSL
    ■  1 - SSL for Authentication Only
    ■  2 - SSL for data transfer and authentication (Default)

-storage_tier  storage_tier
    Use this option to provide the storage tier for Microsoft Azure. Valid values are:
    ■  ACCOUNT_ACCESS_TIER (Default)
    ■  ARCHIVE

-sts  storage_server_name
    Use this option to provide the storage server name.

-tenant_type  id | name
    Use this option to specify if you want to use either the tenant ID or tenant name
    that is associated with your cloud storage credentials.

    Only OpenStack Swift supports this option.

-tenant_value  tenant_value
    Use this option to provide the tenant ID or tenant name value that is associated
    with your cloud storage credentials.

    Only OpenStack Swift supports this option.

-url  service_url
    Use this option to provide the service URL.

    The format of the service URL is https://hostname[:port]/[path].

    Only Amazon S3 supports this option.
-user_domain_type id | name
    Use this option to specify if you want to use either the user's domain ID or domain name that is associated with your cloud storage credentials.
    Only OpenStack Swift supports this option.

-user_domain_value user_domain_value
    Use this option to provide either the user's domain ID or domain name value that is associated with your cloud storage credentials.
    Only OpenStack Swift supports this option.

-user_type id | name
    Use this option to specify if you want to use either the user ID or the user name that is associated with your cloud storage credentials. When you provide user ID, user name and domain information is not required.
    Only OpenStack Swift supports this option.

-user_type_value user_type_value
    Use this option to provide either the user ID or the user name value that is associated with your cloud storage credentials.
    Only OpenStack Swift supports this option.

Parameters for option -i

Use this option to fetch the details of all cloud instances.

-at api_type
    Use this option to fetch the details of cloud instances for the specified cloud storage API type.
    Valid values are:
    ■ s3
    ■ azure
    ■ swift

-in instance_name
    Use this option to provide the cloud instance name.

-pt provider_type
    Use this option to fetch the details of cloud instances for the specified cloud provider.

Parameters for option -l

Use this option to fetch the list of all cloud storage (or cloud instances) that are configured in NetBackup.
Use this option to fetch the details of cloud instances for the specified cloud storage API type.

Valid values are:

- s3
- azure
- swift

Use this option to fetch the list of the cloud instances specific to a cloud provider.

**Parameters for option -lr**

Use this option to fetch a list of available storage regions.

This option is supported only for OpenStack Swift using authentication version Identity V2 and V3.

Use this option to provide the cloud instance name.

Use this option to specify if you want to use either the project's domain ID or domain name that is associated with your cloud storage credentials.

Use this option to provide either the project's domain ID or domain name value that is associated with your cloud storage credentials.

Use this option to specify if you want to use either the project ID or project name that is associated with your cloud storage credentials.

When you provide project ID, project name and domain information is not required.

Use this option to provide the project ID or project name value that is associated with your cloud storage credentials.

Use this option to provide the authentication type that must be used for proxy type HTTP.

Valid values are as follows:

- NONE (Disables authentication)
- `BASIC`
- `NTLM`

-`pxhost proxy_host`
   Use this option to provide the host name or IP address of the proxy server.

-`pxport proxy_port`
   Use this option to provide port number of the proxy server.

-`pxtunnel proxy_tunnel_usage`
   Use this option to specify if you want to use proxy tunneling.
   Valid values are as follows:
   - 0: Disable
   - 1: Enable (Default)
   Proxy tunneling is supported only for proxy type HTTP.

-`pxtype proxy_type`
   Use this option to provide the proxy type of the proxy server.
   Valid values are as follows:
   - HTTP
   - SOCKS
   - SOCKS4
   - SOCKS4A
   - SOCKS5
   - NONE (Disables the proxy type)

-`pxuser_name proxy_user_name`
   Use this option to provide user name of the proxy server.

-`tenant_type id | name`
   Use this option to provide the tenant ID or tenant name that is associated with your cloud storage credentials.

-`tenant_value tenant_value`
   Use this option to provide the tenant ID or tenant name value that is associated with your cloud storage credentials.

-`user_domain_type id | name`
   Use this option to specify if you want to use either the user's domain ID or domain name that is associated with your cloud storage credentials.
-user_domain_value  user_domain_value
    Use this option to provide either the user's domain ID or domain name value that is associated with your cloud storage credentials.

-user_name  user_name
    Use this option to provide the cloud storage user name.

-user_type  id | name
    Use this option to specify if you want to use either the user ID or the user name that is associated with your cloud storage credentials.

    When you provide user ID, user name and domain information is not required.

-user_type_value  user_type_value
    Use this option to provide either the user ID or the user name value that is associated with your cloud storage credentials.

Parameters for option -r

Use this option to remove a cloud instance.

-in  instance_name
    Use this option to provide the cloud instance name.

Parameters for option -rr

Use this option to remove a region association for a specific cloud instance.

Only Amazon S3 supports this option.

-in  instance_name
    Use this option to provide the cloud instance name.

-lc  location_constraint
    Use this option to provide the location identifier that the cloud provider service uses to access the buckets of the associated region.

    For a public cloud storage, you need to get the location constraint details from the cloud provider.

Parameters for option -rs

Use this option to remove the cloud storage server for specified cloud instance.

-in  instance_name
    Use this option to provide the cloud instance name.

-sts  storage_server_name
    Use this option to provide the storage server name.

Parameters for option -u

Use this option to update an existing cloud instance.
Only Amazon S3 supports this option.

- **access_style access_style_type**
  Use this option to provide the endpoint access style for the cloud service provider.

  Valid values for **-access_style_type** are as follows:
  - 1 - Virtual Hosted Style
  - 2 - Path Style
  The default value for **access_style_type** is 2.

- **http_port port_no**
  Use this option to provide the HTTP port with which you can access the cloud provider service in a non-secure mode.

- **https_port port_no**
  Use this option to provide the HTTPS port with which you can access the cloud provider service in a secure mode.

- **-in instance_name**
  Use this option to provide the cloud instance name.

- **-se service_endpoint_path**
  Use this option to provide the cloud service provider endpoint.

- **-sh service_host_name**
  Use this option to provide the cloud service provider host name.

**Parameters for option -ur**

Use this option to update a region for a specific cloud instance.

Only Amazon S3 supports this option.

- **-in instance_name**
  Use this option to provide the cloud instance name.

- **-lc location_constraint**
  Use this option to provide the location identifier that the cloud provider service uses for any data transfer operations in the associated region. For a public cloud storage, you need to get the location constraint details from the cloud provider.

- **-rn region_name**
  Use this option to provide the cloud storage region.

- **-sh service_host**
  Use this option to provide the cloud service provider host name.
Parameters for option -us

Use this option to update the storage server for the specified cloud instance.

-agency agency
    Use this option to specify the agency name the cloud provider supplied.
    Only Amazon S3 supports this option with AmazonGov Cloud.

-auth_lc authentication_location_constraint
    Use this option to provide the authentication location constraint to update the
    cloud storage server’s authentication location.
    Only Amazon S3 supports this option.

-cert_file cert_file_name
    Use this option to provide the certificate file name.
    The files that are mentioned in the parameters should exist on the master
    server at the following location:
    ■ On Windows: install_path\netbackup\var\global\wmc\cloud
    ■ On UNIX: install_path/var/global/wmc/cloud
    Only Amazon S3 supports this option with AmazonGov Cloud.

-del_lc location_constraint
    Use this option to provide the location constraint to delete a region from the
    storage server.
    Only Amazon S3 supports this option.

-in instance_name
    Use this option to provide the cloud instance name.

-key_file private_key_file_name
    Use this option to specify the private key file name the cloud provider supplied.
    The files that are mentioned in the parameters should exist on the master
    server at the following location:
    ■ On Windows: install_path\netbackup\var\global\wmc\cloud
    ■ On UNIX: install_path/var/global/wmc/cloud
    Only Amazon S3 supports this option with AmazonGov Cloud.

-key_pass private_key_passphrase
    Use this option to specify the private key file name the cloud provider supplied. It
    must be 100 or fewer characters.
    Only Amazon S3 supports this option with AmazonGov Cloud.
-lc location_constraint
  Use this option to provide the location constraint to update the storage server to add a new region.
  Only Amazon S3 supports this option.

-mission mission1
  Use this option to specify the mission name the cloud provider supplied.
  Only Amazon S3 supports this option with AmazonGov Cloud.

-pxauth_type proxy_auth_type
  Use this option to provide the authentication type that must be used for proxy type HTTP.
  Valid values are as follows:
  - NONE (Disables authentication)
  - BASIC
  - NTLM

-pxhost proxy_host
  Use this option to provide the host name or IP address of the proxy server.

-pxport proxy_port
  Use this option to provide the port number of the proxy server.

-pxuser_name proxy_user_name
  Use this option to provide the proxy server user name.

-pxtype proxy_type
  Use this option to provide the proxy type of the proxy server.
  Valid values are as follows:
  - HTTP
  - SOCKS
  - SOCKS4
  - SOCKS4A
  - SOCKS5
  - NONE (Disables the proxy type)

-pxtunnel proxytunnel_usage
  Use this option to specify if you want to use proxy tunneling.
  Valid values are as follows:
Proxy tunneling is supported only for proxy type HTTP.

```
-ex role
  Use this option to provide the role.
  Only Amazon S3 supports this option with AmazonGov Cloud.

-url service_url
  Use this option to provide the service url.
  The format of the service URL is https://hostname[:port][/path].
  Only Amazon S3 supports this option.
```

**EXAMPLES**

Example 1: Add cloud instance of type Hitachi with custom ports for HTTP and HTTPS.

```bash
csconfig cldinstance -a -in my-hitachi.com -pt hitachi -sh my-hitachi.com -http_port 80 -https_port 443 -access_style 2
```

Example 2: Update cloud instance my-hitachi.com of type Hitachi with new Service Host (s3.finance-hitachi.com).

```bash
csconfig cldinstance -u -in my-hitachi.com -sh s3.finance-hitachi.com -se s3.hitachi.com -http_port 80 -https_port 443 -access_style 2
```

Example 3: Add storage server for Amazon S3 with proxy type HTTP and authentication type as basic and proxy tunneling disabled.

```bash
```

**Note:** This command prompts for the password.

Example 4: Add storage server for an existing AmazonGov Cloud instance with Credentials Broker supported.

```bash
```

- **0**: Disable
- **1**: Enable (Default)
Example 5: Update storage servers for existing AmazonGov Commercial Cloud Services instance with Credentials Broker supported.

csconfig cldinstance -us -in my-amzgov.com -sts abc-amzgov.com
-url https://my.host.com:8080/service-path -mission dummy_mission
-agency dummy_agency -role dummy_role -cert_file dummy_file
-key_file dummy_key_file key_pass dummy_passphrase

Note: You can update one or many parameters of a storage server at the same time.

Example 6: Add OpenStack Swift cloud instance for authentication version Identity V2.

csconfig cldinstance -a -in my-swiftstack.com -pt swstksw
-auth_ver IDENTITY_V2 -auth_url https://lon.identity.api.swiftstack.com/v2.0/tokens

Example 7: List the storage regions for an OpenStack Swift-compliant cloud provider. This command is applicable only for authentication version Identity V2.

csconfig cldinstance -lr -in my-swiftstack.com -user_name John
-tenant_type id -tenant_value 1234

Example 8: Add storage server for an existing OpenStack Swift instance.

csconfig cldinstance -as -in my-swiftstack.com -sts abc-swiftstack.com
-tenant_type id -tenant_value 1234 -sr RegionUS

Example 9: Add storage server for an existing cloud instance for a OpenStack Swift-compliant cloud using the user ID and project name. When you provide the User ID, Domain Type and Value parameters are not required. This command is applicable only for authentication version Identity V3.

csconfig cldinstance -as -in swiftstack_v3 -sts swiftstack
-user_type id -user_value user_id123 -project_type name
-project_value project_name123 -project_domain_type id
-project_domain_value domain_id123 -sr region_name

Example 10: Add storage server for an existing cloud instance for a OpenStack Swift-compliant cloud using the user name and project ID. When you provide Project
ID, Domain Type and Value parameters are not required. This command is applicable only for authentication version Identity V3.

```bash
csconfig cldinstance -as -in swiftstack_v3 -sts swiftstack -user_type name -user_value user_name123 -user_domain_type name -user_domain_value domain_name123 -project_type id -project_value project_id123 -sr region_name
```

**Example 11:** List the storage regions of an existing cloud instance (Identity V3) for a OpenStack Swift-compliant cloud using the user ID and project name.

```bash
csconfig cldinstance -lr -in swiftstack_v3 -user_type id -user_value user_id123 -project_type name -project_value project_name123 -project_domain_type id -project_domain_value domain_id123
```

**Example 12:** List the storage regions of an existing cloud instance (Identity V3) for a OpenStack Swift-compliant cloud using the user name and project ID.

```bash
csconfig cldinstance -lr -in swiftstack_v3 -user_type name -user_value user_name123 -user_domain_type name -user_domain_value domain_name123 -project_type id -project_value project_id123
```

**Example 13:** Add storage server for existing cloud instance with location constraint.

```bash
csconfig cldinstance -as -in amazon.com -sts myamz-us.com -lc us-east-1,us-west-2
```

**Example 14:** Add region for a cloud instance.

```bash
csconfig cldinstance -ar -in myamazon.com -lc us-west-1 -rn "US West (N. California)" -sh s3-us-west-1.amazonaws.com
```

**SEE ALSO**

See `csconfig cldprovider` on page 528.
See `csconfig meter` on page 530.
See `csconfig throttle` on page 532.
See `csconfig reinitialize` on page 536.
csconfig cldprovider

csconfig cldprovider – the cldprovider option for the csconfig command fetches the cloud provider configuration settings.

SYNOPSIS

```
csconfig cldprovider [-i [-pt [provider_type] | -at api_type]] [-l
[-at api_type]]
```

On UNIX systems, the directory path to this command is
```
/usr/openv/netbackup/bin/admincmd/
```

On Windows systems, the directory path to this command is
```
install_path\NetBackup\bin\admincmd\n```

DESCRIPTION

The csconfig command manages the Cloud Connect configuration settings from a remote or a local computer. The cldprovider option fetches the cloud provider configuration settings.

---

**Note:** You cannot provide multi-byte or localized format values for any of the csconfig command cldprovider options.

OPTIONS

- `at api_type`
  
  This option fetches the list of cloud providers of the specified API type.
  
  Accepted values are s3, azure, and swift
  
  For a complete list of supported cloud providers, refer to the Cloud – Supported Technology Methods section of the hardware compatibility list for your version of NetBackup. [http://www.netbackup.com/compatibility](http://www.netbackup.com/compatibility)

- `-i`
  
  Use this option to get the details of all the cloud providers that NetBackup supports.

- `-l`
  
  This option gets the list of the cloud providers that NetBackup supports.

- `pt provider_type`
  
  Use this option to fetch the details of the specified cloud provider.
Accepted values are amazon, azure, and swstksw.

EXAMPLES

Example 1: Get the list of all cloud providers.

csconfig cldprovider -l

Example 2: Get the list of all cloud providers of a specific storage API type.

csconfig cldprovider -l -at s3

Example 3: Get the details of all cloud providers.

csconfig cldprovider -i

Example 4: Get the details of a specific cloud provider.

csconfig cldprovider -i -pt amazon

SEE ALSO

See csconfig cldinstance on page 508.
See csconfig meter on page 530.
See csconfig reinitialize on page 536.
See csconfig throttle on page 532.
csconfig meter

**csconfig meter** – the meter option for the csconfig command sets and fetches the metering configuration details from the storage server.

### SYNOPSIS

```
csconfig meter [-cshost server_name][-directory location][-force][-interval time][-setdefaults]
```

On UNIX systems, the directory path to this command is `/usr/openv/netbackup/bin/admincmd/`

On Windows systems, the directory path to this command is `install_path\NetBackup\bin\admincmd`

### DESCRIPTION

The csconfig command manages the Cloud Connect configuration settings from a remote or a local computer. The meter option fetches and sets the metering configuration details from the storage server.

---

**Note:** You cannot provide multi-byte or localized format values for any of the `csconfig` command *meter* options.

### OPTIONS

- `-cshost server_name -n`
  
  This option connects a remote computer to a Cloud Connect service.

- `-directory location`
  
  The directory location for storing the metering data.

- `-force | -f`
  
  This option forces the default values for the meter parameters. Used with `-def`.

- `-interval | -i time`
  
  The metering time interval in seconds. Valid value range is 0 to 86400.

- `-setdefaults | -def`
  
  Use this option to reset all metering parameters to the default value.
EXAMPLES

Example 1: Get the metering configuration details.

csconfig meter
Metering Configuration Details:
  Metering Interval = 300 Sec
  Data Directory = /usr/openv/var/global/wmc/cloud

Example 2: Set the metering parameters, time interval = 500 sec and metering data storage location = /tmp/metered_data (UNIX path).

csconfig meter -interval 500 -directory /tmp/metered_data

SEE ALSO

See csconfig cldinstance on page 508.
See csconfig cldprovider on page 528.
See csconfig reinitialize on page 536.
See csconfig throttle on page 532.
csconfig throttle

cconfig throttle – the throttle option for the csconfig command sets and fetches the throttling configuration details from the Cloud Connect server.

SYNOPSIS


On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The csconfig command manages the Cloud Connect configuration settings from a remote or a local computer. The throttle option sets and fetches the throttling configuration details from the Cloud Connect server.

Note: You cannot provide multi-byte or localized format values for any of the csconfig command’s throttle options.

OPTIONS

-availablebw available_bandwidth | -abw

Use this option to specify the amount of bandwidth NetBackup can use for cloud-related activities.

Valid values are positive integers followed by KB or MB (e.g., 200MB). If no units are specified, the value is in bytes.
-cshost server_name | -n
  Use this option to connect a remote machine to a Cloud Connect service.

-force | -f
  Use this option to force the default values for the throttle parameters.

-interval time | -i
  Use this option to specify the sampling throttle time interval in seconds. The
  valid value range is 0-86400.

-maxconn max_connections | -mxc
  This option is the default maximum number of connections for each cloud
  provider.

-offtime start_time, end_time, bandwidth_percentage | -oft
  Use this option to specify the time interval that is considered off time for the
  cloud connection.

  Specify a start time and end time in 24-hour format. For example, 2:00 P.M.
  is 14:00.

  You can indicate how much bandwidth the cloud connection can use in
  percentage.

  The bandwidth percentage value range is 0-100. You can only specify whole
  numbers for the bandwidth percentage.

-providermaxconn max_connections | -pmc
  Use this option to specify the maximum number of connections for a specific
  provider.

-readbw read_bandwidth_percentage | -rbw
  Use this option to specify the percentage of total bandwidth that read operations
  can use. If there is insufficient bandwidth to transmit the specified amount of
  data within a few minutes, restore or replication failures may occur due to
  timeouts. Consider the total load of simultaneous jobs on multiple media servers
  when you calculate the required bandwidth.

  The bandwidth percentage value range is 0-100. You can only specify whole
  numbers for the bandwidth percentage.

-setdefaults | -def
  Use this option to reset all throttling parameters to the default value.

-sserver storage_server_name | -r
  Use this option to specify the name of the storage server.

-stype storage_server_type | -t
  Use this option to specify the type of storage server.
-weekend start_day,end_day,bandwidth_percentage | -wkd
Use this option to specify the start and stop time for the weekend.
The start day and end day range of values is Monday-Sunday or 1-7.

Note: You can configure weekdays only in English and in the US calendar format (mmddyy).

You can indicate how much bandwidth the cloud connection can use in percentage.
The bandwidth percentage value range is 0-100. You can only specify whole numbers for the bandwidth percentage.

-worktime start_time,end_time,bandwidth_percentage | -wkt
Use this option to specify the time interval that is considered work time for the cloud connection. Specify a start time and end time in 24-hour format.
The start time and end time range of values is 0-23.
You can indicate how much bandwidth the cloud connection can use in percentage or kilobytes per second. This value determines how much of the available bandwidth is used for cloud operations in this time window.
The bandwidth percentage value range is 0-100. You can only specify whole numbers for the bandwidth percentage.

-writebw write bandwidth_percentage | -wbw
Use this option to specify the percentage of total bandwidth that write operations can use.
If there is insufficient bandwidth to transmit the specified amount of data within a few minutes, backup failures may occur due to timeouts.
Consider the total load of simultaneous jobs on multiple media servers when you calculate the required bandwidth.
The bandwidth percentage value range is 0-100. You can only specify whole numbers for the bandwidth percentage.

EXAMPLES

Example 1: Get the throttling configuration details.

csconfig throttle

Throttling Configuration Details:
Read Bandwidth Percent = 100 %
Write Bandwidth Percent = 100 %
Total Available Bandwidth = 102400 KB/s
Default Maximum Connections = 10

Work Time:
  Start Time = 8 Hrs
  End Time = 18 Hrs
  Allocation Bandwidth = 100 %

Off Time:
  Start Time = 18 Hrs
  End Time = 8 Hrs
  Allocation Bandwidth = 100 %

Weekend:
  Start Day = 6 (Saturday)
  End Day = 7 (Sunday)
  Allocation Bandwidth = 100 %

Sampling Interval = 0 Sec

Example 2: Set the read bandwidth to 30% and available bandwidth to 2147483648 Bytes = 2GB.

csconfig throttle -readbw 30 -availablebw 2147483648 -f

SEE ALSO

See csconfig cldinstance on page 508.
See csconfig cldprovider on page 528.
See csconfig meter on page 530.
See csconfig reinitialize on page 536.
csconfig reinitialize

csconfig reinitialize – reinitializes the CloudStore service container components in the NetBackup Web Management Console (nbwmc) web service.

SYNOPSIS

csconfig reinitialize

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The csconfig reinitialize command lets you reinitialize the CloudStore Service container components in the nbwmc web service. When you use this option, the nbwmc service reloads the configuration settings from the Cloudstore.conf, CloudProvider.xml, and CloudInstance.xml files. You can run this command locally on the NetBackup master or media server or remotely by connecting to the server using SSH.

For changes to the cloud configuration settings to take effect, you must restart either the NetBackup CloudStore Service Container (nbcssc) or the NetBackup Web Management Console (nbwmc) service. This requirement depends on the version of NetBackup. A service restart might fail if there are any configuration errors. One example of a configuration error is the CloudProvider.xml file is invalid. Failure to restart a service can lead to a stoppage in the NetBackup operations.

This command option is provided to avoid a service restart. When you make updates to the cloud configuration settings, run this command for the nbwmc service to load the updated configuration. A restart of the nbwmc service is unnecessary.

SEE ALSO

See csconfig cldinstance on page 508.
See csconfig cldprovider on page 528.
See csconfig meter on page 530.
See csconfig throttle on page 532.
**duplicatetrace**

**duplicatetrace** – trace debug logs for duplicate job(s)

**SYNOPSIS**

```
duplicatetrace [-master_server name] -job_id number [-start_time hh:mm:ss] [-end_time hh:mm:ss] mmddyy [mmddyy ...]
duplicatetrace [-master_server name] -backup_id id [-start_time hh:mm:ss] [-end_time hh:mm:ss] mmddyy [mmddyy ...]
duplicatetrace [-master_server name] [-policy_name name] [-client_name name] [-start_time hh:mm:ss] [-end_time hh:mm:ss] mmddyy [mmddyy ...]
```

On UNIX systems, the directory path to this command is `/usr/openv/netbackup/bin/admincmd/`

On Windows systems, the directory path to this command is `install_path\NetBackup\bin\admincmd`

**DESCRIPTION**

**duplicatetrace** consolidates the debug logs for duplicate jobs and writes them to standard output. The messages sort by time. It tries to compensate for time zone changes and clock drift between remote servers and clients.

At a minimum, you must enable debug logging for `bptm` and `bpdm` on the media server and for the following directory on the master server:

**UNIX systems:**

```
/usr/openv/netbackup/bin/admincmd
```

**Windows systems:**

```
install_path\NetBackup\bin\admincmd
```

For best results, set the verbose logging level to 5. Enable debug logging for `bpdbm` on the master server and `bpcd` on all servers, clients, and the processes that are already identified.

**duplicatetrace** uses the `-job_id` or `-backup_id` option as the sole criteria for selecting the duplicate jobs it traces. The `-policy_name` option or the `-client_name` option cannot be used with `-job_id` or `-backup_id`. If neither option is specified,
then all duplicate jobs that match the selection criteria are selected. If none of the following options are specified, all the duplicate jobs that are activated on the days that day stamps (mmddyy) specify are traced: -job_id, -backup_id, -policy_name, or -client_name. If -start_time and -end_time options are used, then the debug logs that reside in the specified time interval are examined.

If duplicatetrace starts with -backup_id bid, it looks for the duplicate jobs that bpduplicate started with -backup_id bid where the backup IDs (bid) match.

duplicatetrace -policy_name policy looks for the duplicate jobs that it started with the -policy policy option, where the policy names match.

duplicatetrace -client_name client looks for the duplicate jobs that it started with the -client option where the client names (client) match.

duplicatetrace writes error messages to standard error.

You must have administrator privileges to run this command.

OPTIONS

-master_server
   Name of the master server. Default is the local host name.

-job_id
   Job ID number of the duplicate job to analyze. Default is any job ID.

-backup_id
   Backup ID number of the backup image that the duplicate job uses to analyze duplicates. Default is any backup ID.

-policy_name
   Policy name of the duplicate jobs to analyze. Default is any policy.

-client_name
   Client name of the duplicate jobs to analyze. Default is any client.

-start_time
   Specifies the earliest timestamp to start analyzing the logs. Default is 00:00:00.

-end_time
   Specifies the latest timestamp to finish analyzing the logs. Default is 23:59:59.

mmddyy
   One or more "day stamps". This option identifies the log file names (log.mmddyy for UNIX, mmddyy.log for Windows) that is analyzed.
OUTPUT FORMAT

The format of an output line is: `daystamp.millisecs.program.sequence machine log_line`  

`daystamp`
The day of the log that is displayed in yyyyymmdd format.

`millisecs`
The number of milliseconds since midnight on the local computer.

`program`
The name of program (ADMIN, BPTM, BPCD, 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.

EXAMPLES

Example 1 - Analyze the log of duplicate job with job ID 3 activated on May 1, 2010.

```
# duplicatetrace -job_id 3 050110
```

Example 2 - Analyze the log of duplicate jobs that duplicate backup image with backup ID `pride_1028666945` executed on May 20, 2010. It analyzes only those jobs that were activated with option `-backup_id pride_1028666945`.

```
# duplicatetrace -backup_id pride_1028666945 052010
```

Example 3 - Analyze the log of duplicate jobs that are activated on policy Pride-Standard and client pride on May 1, 2010 and May 3, 2010. It analyzes only the duplicate jobs that were activated with options `-policy Pride-Standard` and `-client pride`.

```
# duplicatetrace -policy_name Pride-Standard -client_name pride 050110 050310
```

Example 4 - Analyze the log of all duplicate jobs that are activated on August 5, 2010 and August 23, 2010.

```
duplicatetrace 080510 082310
```
SEE ALSO

See backupdbtrace on page 26.
See backuptrace on page 28.
See importtrace on page 541.
importtrace

importtrace – trace debug logs for import jobs

SYNOPSIS

importtrace [-master_server name] -job_id number [-start_time hh:mm:ss] [-end_time hh:mm:ss] mmddyy [mmddyy]

importtrace [-master_server name] -backup_id id [-start_time hh:mm:ss] [-end_time hh:mm:ss] mmddyy [mmddyy]

importtrace [-master_server name] [-policy_name name] [-client_name name] [-start_time hh:mm:ss] [-end_time hh:mm:ss] mmddyy [mmddyy]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\

DESCRIPTION

importtrace consolidates the debug log messages for the specified import job[s] and writes them to standard output. The messages sort by time. importtrace tries to compensate for time zone changes and clock drift between remote servers and clients.

At a minimum, enable debug logging for bpbrm, bptm, and nbtar on the media server and for the following directory on the master server:

UNIX systems:

/usr/openv/netbackup/bin/admincmd

Windows systems:

install_path\NetBackup\bin\admincmd

For best results, set the verbose logging level to 5. Enable debug logging for bpdbm on the master server and bpcd on all servers and clients in addition to the processes already identified.

duplicatetrace uses the -job_id or -backup_id option as the sole criteria for selecting the duplicate jobs it traces. The -policy_name option or the -client_name
option cannot be used with -job_id or -backup_id. If neither option is specified, then all duplicate jobs that match the selection criteria are selected. If none of the following options are specified, all the duplicate jobs that are activated on the days that day stamps (mmddyy) specify are traced: -job_id, -backup_id, -policy_name, or -client_name. If -start_time and -end_time options are used, then importtrace examines the debug logs that are generated in the specified time interval.

If importtrace starts with -backup_id id, it looks for the import jobs that bpimport started with -backup_id id where the backup IDs (id) match.

If importtrace starts with -policy_name policy, importtrace looks for the import jobs that started with bpimport with -policy policy where the policy names (policy) match.

If importtrace starts with -client_name client, importtrace looks for the import jobs that started with bpimport with -client client where the client names (client) match.

importtrace writes error messages to standard error.

You must have administrator privileges to run this command.

OPTIONS

-master_server
  Name of the master server. Default is the local host name.

-job_id
  Job ID number of the import job to analyze. Default is any job ID.

-backup_id
  Backup ID number of the backup image that the import job imports to analyze. Default is any backup ID.

-policy_name
  Policy name of the import jobs to analyze. Default is any policy.

-client_name
  Client name of the import jobs to analyze. Default is any client.

-start_time
  Earliest timestamp to start analyzing the logs. Default is 00:00:00.

-end_time
  Latest timestamp to finish analyzing the logs. Default is 23:59:59.
One or more day stamps. This option identifies the log file names (log.mmddyy for UNIX, mmddyy.log for Windows) to be analyzed.

OUTPUT FORMAT

The format of an output line is:

daystamp.millisecs.program.sequence machinelog_line

daystamp

   The day of the log displayed in yyyymmd format.

millisecs

   The number of milliseconds since midnight on the local computer.

program

   The name of program (ADMIN, BPBRM, BPCD, 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.

EXAMPLES

Example 1 - Analyze the log of import job with job ID 4 activated on August 6, 2009.

# importtrace -job_id 4 080609

Example 2 - Analyze the log of import jobs that import backup image with backup ID pride_1028666945 executed on August 20, 2009. This command would analyze only those import jobs, which were activated with option -backupid pride_1028666945.

# importtrace -backup_id pride_1028666945 082009

Example 3 - Analyze the log of import jobs that are activated on policy Pride-Standard and client pride on August 16, 2009 and August 23, 2009. This command would analyze only those import jobs, which were activated with options -policy Pride-Standard and -client pride.

# importtrace -policy_name Pride-Standard -client_name pride 081609 082309
Example 4 - Analyze the log of all import jobs that are activated on August 5, 2015 and August 17, 2015.

# importtrace 080515 081715

SEE ALSO

See backupdbtrace on page 26.
See backuptrace on page 28.
See duplicatetrace on page 537.
jbpSA

jbpSA – start BAR client interface on Java-capable UNIX machines

SYNOPSIS


The directory path to this command is /usr/openv/netbackup/bin/

DESCRIPTION

This command operates only on UNIX systems.

The jbpSA command starts the Backup, Archive, and Restore client interface on Java-capable UNIX machines.

OPTIONS

-d | -display
Displays the environment variable. For example:
-d eagle:0.0

-D prop_filename
Indicates the debug properties file name. The default name for this file is Debug.properties.

-h | -Help
Displays the possible options for the jbpSA command.

-l debug_filename
Indicates the debug log file name. The default name is unique to this startup of jbpSA and is written in /usr/openv/netbackup/logs/user_ops/nbjlogs.

-lc
Prints the command lines that the application uses to access its log file.

Note: The application does not always use the command lines to get or update data. It has some protocols that instruct its application server to perform tasks using NetBackup and Media Manager APIs. As the application evolves, fewer command lines are used.
-ms nnn

Allows the memory usage configuration for the Java Virtual Machine (JVM) where nnn is the megabytes of memory available to the application. Default: 36 MB (megabytes)

Run jnbSA on a computer with 512 megabytes of physical memory with 128 megabytes of memory available to the application.

The -ms command specifies how much memory is allocated for the heap when the JVM starts. This value may not require changes since the default is sufficient for quickest initialization of jnbSA on a computer with the recommended amount of memory.

Example:

# jbpSA -ms 36M

The memory that is allocated can be specified by using the jbpSA command or by setting the INITIAL_MEMORY option in /usr/openv/java/nbj.conf.

-mx xxx

The -mx option allows memory usage configuration for the Java Virtual Machine (JVM). The xxx value specifies the maximum heap size (in megabytes) that the JVM uses for dynamically-allocated objects and arrays. Default: 512 MB.

This option is useful if the amount of data is large (for example, a large number of jobs in the Activity Monitor).

Example:

# jbpSA -mx 512M

The maximum heap size can be specified by using the jbpSA command or by setting the MAX_MEMORY option in /usr/openv/java/nbj.conf.

-r version

Specifies which version of the Backup, Archive, and Restore client to run. NetBackup includes an administration console for all the supported versions of NetBackup. If the -r option is not specified, the default is the latest version of NetBackup.
jnbSA

jnbSA – start NetBackup Administration Console on Java-capable UNIX machines

SYNOPSIS


The directory path to this command is /usr/openv/netbackup/bin/

DESCRIPTION

This command operates only on UNIX systems.

jnbSA starts the NetBackup Administration Console on Java-capable UNIX machines.

OPTIONS

-d | -display
Display the environment variable. For example:

-d eagle:0.0

-D prop_filename
Indicate the debug properties file name. The default name for this file is Debug.properties.

-h | -help
Displays the possible options for the jnbSA command.

-l debug_filename
Indicates the debug log file name. The default name is unique to this startup of jnbSA and written in /usr/openv/netbackup/logs/user_ops/nbjlogs.

-lc
Prints the command lines that the application uses to its log file.

Note: The application does not always use the command lines to get or update data. It has some protocols that instruct its application server to perform tasks using NetBackup and Media Manager APIs. The application evolves and fewer command lines are used.
-ms nnn
Allows memory usage configuration for the Java Virtual Machine (JVM) where
nnn is the megabytes of memory available to the application. Default: 256 MB

Run jnbSA on a machine with 1 GB of physical memory with 256 MB of memory
available to the application.

The -ms command specifies how much memory is allocated for the heap when
the JVM starts. This value may not require changes since the default is sufficient
for quickest initialization of jnbSA on a machine with the recommended amount
of memory.

Example:

jnbSA -ms 256M

The memory that is allocated can be specified by using the jnbSA command
or by setting the INITIAL_MEMORY option in /usr/openv/java/nbj.conf.

-mx xxx
Allows memory usage configuration for the Java Virtual Machine (JVM). The
xxx value is the maximum heap size (in megabytes) that the JVM uses for
dynamically-allocated objects and arrays. Default: 512 MB.

This option is useful if the amount of data is large (for example, a large number
of jobs in the Activity Monitor).

Example:

jnbSA -mx 512M

The maximum heap size can be specified by using the jnbSA command or by
setting the MAX_MEMORY option in /usr/openv/java/nbj.conf.

-r version
Specifies which version of the NetBackup Administration Console to run.
NetBackup includes an administration console for all the supported versions
of NetBackup. If the -r option is not specified, the default is the latest version
of NetBackup.
ltid

ltid – start or stop the Media Manager device daemon

SYNOPSIS

/usr/openv/volmgr/bin/ltid [-v] [-logmounts [minutes]] [-noverify]

DESCRIPTION

This command operates only on UNIX systems.

The ltid command starts the Media Manager device daemon (ltid) and Automatic Volume Recognition daemon (avrd). These daemons manage Media Manager devices. With both daemons started, an operator can initiate the operator display, observe the drive status, and control the assignment of requests to standalone drives. ltid can be placed in a system initialization script.

The Media Manager volume daemon, vmd, also starts with the ltid command. ltid also starts the appropriate robotic daemons, if robotic devices were defined in Media Manager.

The stopltid command stops ltid, avrd, and the robotic daemons.

You must have administrator privileges to run this command.

OPTIONS

-v

Logs debug information using syslogd. This option is most informative when robotic devices are in use. This option starts robotic daemons and vmd in verbose mode.

-logmounts minutes

If this option is specified, ltid logs mount requests using syslogd. The mount requests are still posted to Media Manager displays. The mount requests are only logged after a delay of the specified number of minutes.

If -logmounts is specified, the default number of minutes is 3. If -logmounts 0 is specified, ltid logs the mount request through syslogd immediately. If minutes is not zero and the mount request is satisfied before the number of minutes are up, the request is not logged through syslogd.
-noverify

If this option is specified, \texttt{ltid} does not verify drive names. Normally, \texttt{ltid} verifies that the no rewind on close drive name has the correct minor number bits that relate to the following: no rewind, variable, berkeley-style, and so on. This option is normally not required, but may be helpful if you use non-standard platform device files. If this option is specified, make sure that the device files are correct.

\section*{ERRORS}

Error messages are logged by using \texttt{syslogd}.

\section*{SEE ALSO}

rc(8)
See \texttt{stopltid} on page 877.
syslogd
See \texttt{tpconfig} on page 892.
See \texttt{tpunmount} on page 917.
**manageClientCerts**

**SYNOPSIS**

`manageClientCerts` - use this command to manage the client certificates for the VMware and the SCVMM plug-ins.

`manageClientCerts -create|-delete|-renew clientName`

`manageClientCerts -list`

`manageClientCerts -addAlias|-deleteAlias clientName -IP address|-HOST alias|-ANY`

`manageClientCerts -listAliases clientName`

On UNIX and Linux systems, the directory path to this command is `/usr/openv/wmc/bin/install/`

On Windows systems, the directory path to this command is `install_path\NetBackup\wmc\bin\install`

**DESCRIPTION**

Use the `manageClientCerts` command to create, delete, and list the client tokens for the VMware and the SCVMM plug-ins, as well as add, remove, and list aliases.

**OPTIONS**

- `-addAlias`
  
  Use this option to add an alternate host name or IP address for the `clientName` that was used when generating a token. Use the `-ANY` parameter with `addAlias` to allow any host or any TCP/IP address to communicate using the specified certificate. While this command works, it is not a secure method.

- `-create`
  
  Use this option to create a certificate for the client specified.

- `-delete`
  
  Use this option to delete a certificate for the client specified.

- `-deleteAlias`
  
  Use this option to delete an alternate host name or IP address that is associated with a token.
-list
  Use this option to list all the certificates.

-listAliases
  Use this option to list all aliases for client.

-renew
  Use this option to delete a token and to create a new one. Any aliases that
  existed for the token are retained. If a token expires, you can use this option
  to renew the token. Be aware that tokens expire after one year.

EXAMPLES

Example 1 - Create a token for client vCenter1

manageClientCerts -create vCenter1
Successfully created client certificate for 'vCenter1'
to secure access to the NetBackup Web Services on Master Server
'master.example.com', port '8443'.
Please find the zip at /usr/openv/var/global/wsl/credentials/clients
/vCenter1.example.com.zip.

Example 2 - Add the alias vCenter1.example.com to the client vCenter1

manageClientCerts.sh -addAlias vCenter1 -HOST vCenter1.example.com
Successful -addAlias, for client: vCenter1, type: HOST,
alias: vCenter1.example.com

manageClientCerts -addAlias vCenter1.example.com -HOST vCenter1

Example 3 - List all the aliases for vCenter1

manageClientCerts -listAliases vCenter1
Aliases for vCenter1:
HOST = vCenter1.example.com

Example 4 – Renew a token for vCenter1

manageClientCerts -renew vCenter1
Renewing client certificate: vCenter1
Successfully deleted the entries for the client vCenter1.
Successfully created client certificate for 'vCenter1' to secure access
to the NetBackup Web Services on Master Server 'mserver1.example.com',
port '8443'.
Please find the zip at
mklogdir

mklogdir – creates log directories with the recommended permissions.

SYNOPSIS

mklogdir [-create] [-fixFolderPerm] [-dryrun] [-list] [logdirname(s)]

log directory name

[-user username]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/logs

On Windows systems, the directory path to this command is install_path\NetBackup\logs

DESCRIPTION

mklogdir creates all the NetBackup log directories for a user, with the recommended permissions.

OPTIONS

-create

Creates all NetBackup log directories with the recommended permissions as identified by Veritas. Create is the default option in case no other option is specified.

-list

Displays a list of all the NetBackup log directories along with the details about the permissions set.

-fixFolderPerm

Sets the recommended permissions for the already existing NetBackup log directories, if the permissions are not already set. This scenario refers to the use cases in case of NetBackup version upgrade.

-dryrun

Allows the user to review the changes before they are made. If you specify this option, no changes are made to the system.

-help

Displays the possible options for the mklogdir command.
logdirname

Specifies a list of one or more space-separated log directories on which an action needs to be performed. If no log directories are specified, then the action is performed on all the log directories.

-user username

Creates the user folders for the required process log directory. Use this option only for non-root users or users who are not part of administrator groups.

If the user is local user or system user, only `username` should be used. If the user is part of any domain, specify the user name in this format: "domain_short_name\username". Be aware you must enclose the user name in double quotes (").

EXAMPLES

Example 1 - Create all the NetBackup log directories for a user, with the recommended permissions.

# mklogdir -create

Example 2 - Create the `admin` and the `bpdbm` log directories with the recommended permissions.

# mklogdir admin bpdbm

Example 3 - Examine all the existing log directories and set the permissions to those directories which do not have the recommended permissions. This command needs to be used after NetBackup version upgrade to set the recommended permissions for all the existing log files.

# mklogdir -fixFolderPerm

Example 4 - Examine all the existing log directories and display the changes that need to be made to get the recommended permissions.

# mklogdir -fixFolderPerm -dryrun

SEE ALSO

See `bpgetdebuglog` on page 164.
nbauditreport

nbauditreport – Generate and view an audit report

SYNOPSIS

```
```

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\

DESCRIPTION

The nbauditreport command lets you create and view a NetBackup audit report. When auditing is configured in a NetBackup environment, the following user-initiated actions in NetBackup are recorded and available to view in an audit report:

- Actions that change the NetBackup configuration. Examples are policy creation, deletion, and modification, and changing the audit settings.

- Actions that change NetBackup run-time objects. These actions include initiating a restore job and starting or stopping the audit service.

This command only creates and displays the audit report. You must use the nbemcmd -changesetting -AUDIT ENABLED and nbemcmd -changesetting -AUDIT DISABLED commands to enable and disable auditing itself.

For more about auditing and audit reports, see the NetBackup Administrator’s Guide, Volume I and NetBackup Security and Encryption Guide.
OPTIONS

-ctgy [ALERT | ASSET | ASSETGROUP | AUDITCFG | AUDITSVC | AZFAILURE | BPCONF | CATALOG | CERT | CONFIG | CONNECTION | DATAACCESS | HOLD | HOST | JOB | LICENSING | LOGIN | POLICY | POOL | PROTECTION_PLAN_SVC | RETENTION_LEVEL | SEC_CONFIG | SLP | STORAGESRV | STU | TOKEN | USER]

Specifies the type of information to be displayed in the audit report. The audit function records and displays information on the use-initiated actions for the pertinent area (job, pool, etc.). The following are the possible values for this option and the items that are audited for each value:

- ALERT - failure in alert generation or failure in sending email notifications.
- ASSET - deleting an asset, such as a vCenter server or a virtual machine, as part of the POST /asset-cleanup process in the Asset Database API.
- ASSETGROUP - creating, modifying, or deleting an asset group as well any action on an asset group for which a user is not authorized.
- AUDITCFG - auditing configuration changes
- AUDITSVC - starting and stopping the NetBackup Audit service (nbaudit)
- AZFAILURE - authorization failures
- BPCONF - changes to the bp.conf file (UNIX only).
- CATALOG - verifying and expiring images; and reading front-end usage data
- CERT - certificate deployment
- CONFIG - changes made to the configuration settings (for example SMTP server configuration) or to the excluded status codes list for alerts
- CONNECTION - dropped host connections
- DATAACCESS - the audit messages that are related to success and failure of access to different NetBackup operations. For NetBackup 8.3, audit messages are displayed for restore and browse images operations only.
- HOLD - create, modify, and delete hold operations.
- HOST - NetBackup host database-related operations
- JOB - job changes
- LICENSING - track any access to information that is related to licensing
- LOGIN - logon attempts
- POLICY - Adding, deleting, or updating policy attributes, clients, schedules, and backup selections lists.
- POOL - disk storage pool changes
- PROTECTION_PLAN_SVC - modifications to the protection plan
- RETENTION_LEVEL - changes to the retention level
- SEC_CONFIG - changes made to the security configuration settings
- SLP - Creating, modifying, or deleting a storage lifecycle policy (SLP) when initiated through a NetBackup graphical user interface, API, or the nbstl command. Successful attempts to activate or suspend an SLP from a NetBackup graphical user interface or API are also audited and logged. Activating and suspending an SLP using the nbstlutil command are not audited.
- STORAGESRV - storage server information
- STU - storage unit changes
- TOKEN - authorization tokens
- USER - adding or deleting users

The default condition, when none of the options are specified, is to display the audit report of all categories.

-fmt [SUMMARY | DETAIL | PARSABLE]

Specifies the output format of the audit report.

- SUMMARY is the default condition (no option used). The audit report is a summary only. It displays the audit report in columnar format using the description, user, and timestamp headings.
- DETAIL displays a comprehensive list of auditing information. For example, when a policy is changed, this view lists the name of the attribute, the old value, and the new value.
- PARSABLE displays the same set of information as the DETAIL report but in a parsable format. The report uses the pipe character (|) as a separator of the audit data. Use keywords available with the report (DESCRIPTION, ACTION, OLDV, NEWV, etc.) to parse the audit record.

The parsable report contains the following fields:

- DESCRIPTION. The details of the action that was performed. The details include the new values that are given to a modified object and the new values of all attributes for a newly created object. The details also show any deleted objects.
- **TIMESTAMP.** The time that the action occurred. The time is displayed in Coordinated Universal Time (UTC) and is indicated in seconds.

- **CATEGORY.** The category of user action that was performed. Categories such as POLICY may contain several sub-categories such as schedules or backup selections. Any modifications to a sub-category are listed as a modification to the primary category. The categories are as follows:
  - ALERT - failure in alert generation or failure in sending email notifications.
  - AUDITCFG - Auditing configuration changes
  - AUDITSVC - Starting and stopping the NetBackup Audit service (nbaudit)
  - AZFAILURE - Requests that fail authorization checks
  - BPCONF - Changes to the `bp.conf` file (UNIX only)
  - CATALOG - Verifying and expiring images; and reading front-end usage data
  - CERT - Creating, revoking, renewing, and deploying of certificates and specific certificate failures
  - CONFIG - changes made to the configuration settings (for example SMTP server configuration) or to the excluded status codes list for alerts
  - DATAACCESS - The audit messages that are related to success and failure of access to different NetBackup operations. For NetBackup 8.3, audit messages are displayed for restore and browse images operations only.
  - HOLD - Create, modify, and delete hold operations.
  - HOST - Information that is related to NetBackup host database operations.
  - JOB - Job changes such as cancelations or deletions
  - LICENSING - track any access to information that is related to licensing
  - LOGIN - The success and failure that is related to NetBackup Administration Console and NetBackup API logon attempts.
  - POLICY - Modification to policy attributes, clients, schedules, or backup selections
  - POOL - Disk storage pool changes
  - PROTECTION_PLAN_SVC - modifications to the protection plan
  - RETENTION_LEVEL - changes to the retention level
  - SEC_CONFIG - Information that is related to changes that are made to the security configuration settings
  - SLP - Creation, modification, or deletion SLP attributes or windows when they are initiated through a NetBackup graphical user interface, API, or the `nbsl` command.
  - STORAGESRV - Storage server creation, modification, or deletion
STU - Storage unit creation, modification, or deletion
TOKEN - Creating, deleting, and cleanup of tokens and specific token issuing failures
USER - Adding or deleting users

■ CONNECTION - Information about the dropped host connections.

■ ACTION. The activity that was performed. The following actions are possible for all categories: Detailed descriptions of the specific activities that are performed for each action are found in the DESCRIPTIONS and the DETAILS fields of the command output.

■ REASON. Reason that is given for the performed action if any. If the audit reason for host and host ID-to-host name mapping operations contains more than 512 characters, the reason text is truncated to 512 characters.

■ DETAILS. Detailed information on the activity that is separated into attributes (ATTR_num), each with a descriptive name followed by OLDV/NEWV (old value/new value) pair.

Example for a policy deletion: ATTR_1: Policy Type OLDV: Standard NEWV:

-notruncate
Displays the old and new values of a changed attribute on separate lines in the details section of the report. This option is used with the -fmt DETAIL option.

-order [DTU | DUT | TDU | TUD | UDT | UTD]
Specifies the order in which the information is displayed in the parsable format of the audit report. This option can be used only with the -fmt PARSABLE option. The D, T, and U designators represent the following:

■ D - description
■ T - timestamp
■ U - user

-pagewidth NNN
Specifies the page width for the details section of the audit report. This option is used with the -fmt DETAIL option.

-sdate mm/dd/yyyy-hh:mm:ss | mm/dd-hh:mm -edate mm/dd/yyyy-hh:mm:ss | mm/dd-hh:mm
Sets the start date-time (-sdate) or the end date-time (-edate) of the audit report data that you want to view. No time indication is necessary.
If the start date is specified and the end date is not, the displayed audit data is from the specified start time to the present. If the end date is specified and the start date is not, the displayed audit data is up to the end date.

```
-user username[:domainname]
```

Indicates the name of the user for whom you want to display audit information.

**EXAMPLES**

**Example 1** - Display all audit events that are reported from April 1, 2013 to the present.

```
# nbauditreport -sdate 04/01/13
```

<table>
<thead>
<tr>
<th>USER</th>
<th>DESCRIPTION</th>
<th>TIMESTAMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin@entry</td>
<td>Schedule 'test1' was added to Policy 'test1'</td>
<td>04/06/13</td>
</tr>
<tr>
<td>Admin@entry</td>
<td>Audit setting(s) of master server 'server1' were modified</td>
<td>04/06/13</td>
</tr>
<tr>
<td>Admin@entry</td>
<td>Audit setting(s) of master server 'server1' were modified</td>
<td>04/06/13</td>
</tr>
<tr>
<td>sys@server1</td>
<td>The nbaudit service on master server 'server1' was started</td>
<td>04/06/13</td>
</tr>
<tr>
<td>sys@server1</td>
<td>The nbaudit service on master server 'server1' was stopped</td>
<td>04/06/13</td>
</tr>
<tr>
<td>sys@server1</td>
<td>The nbaudit service on master server 'server1' was started</td>
<td>04/06/13</td>
</tr>
</tbody>
</table>

Audit records fetched: 7

**Example 2** - Display a detailed audit report for when Joe modified a set of policy attributes. Because the policy was changed only one time since 6/8/13, one audit record is retrieved.

```
# nbauditreport -fmt DETAIL -ctgy POLICY -sdate 6/8/13
```

DESCRIPTION: Attributes of Policy 'pol_stugrp' were modified

USER: joe
TIMESTAMP: 06/08/2013 19:14:25
CATEGORY: POLICY
ACTION: MODIFY
DETAILS:

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>OLD VALUE</th>
<th>NEW VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Proxy Client</td>
<td></td>
<td>stu_grp</td>
</tr>
<tr>
<td>2 Residence</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3 Collect TIR info</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>5 Collect BMR Info</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
Audit records fetched: 1

The DETAILS entry shows the old value and new value of all the attributes that Joe changed.

Example 3 - Display an audit report for all hold operations that were performed since August 30, 2013.

```bash
# nbauditreport -ctgy HOLD -sdate "08/30/13 22:46:50" -fmt DETAIL
```

DESCRIPTION: Hold with hold name test hold for report1 is created
USER: root@aellora.mydomain.com
TIMESTAMP: 08/30/13 22:47:56
CATEGORY: HOLD
ACTION: CREATE
REASON:
DETAILS:

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>OLD VALUE</th>
<th>NEW VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 On-hold image list</td>
<td>nakul2.mydomain.co</td>
<td></td>
</tr>
</tbody>
</table>

DESCRIPTION: Hold with hold name test hold for report1 is created
USER: root@aellora.mydomain.com
TIMESTAMP: 08/30/13 22:47:54
CATEGORY: HOLD
ACTION: CREATE
REASON:

Audit records fetched: 2

Example 4 - Display a detailed audit report for all security operations.

```bash
# nbauditreport -ctgy SEC_CONFIG -fmt DETAIL
```

DESCRIPTION: Added 'AccessRule' with ID 'jsmith:Backup administrator: All objects'.
USER: secadmin@domain
TIMESTAMP: 05/02/2018 10:38:24
CATEGORY: SEC_CONFIG
ACTION: CREATE
REASON:
DETAILS:

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>OLD VALUE</th>
<th>NEW VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Object Group ID</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>2 Object Group Name</td>
<td></td>
<td>All objects</td>
</tr>
<tr>
<td>3 Object Group Description</td>
<td></td>
<td>Represents all objects</td>
</tr>
<tr>
<td>4 Role ID</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>5 Role Name</td>
<td>Backup administrator</td>
<td></td>
</tr>
<tr>
<td>6 Role Description</td>
<td>Manage protection plans</td>
<td></td>
</tr>
<tr>
<td>7 Rule ID</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>8 Rule Description</td>
<td>Protect and manage all assets</td>
<td></td>
</tr>
<tr>
<td>9 Principal Type</td>
<td>User</td>
<td></td>
</tr>
<tr>
<td>10 Principal Subject ID</td>
<td>domain:user:vx</td>
<td></td>
</tr>
</tbody>
</table>

Audit records fetched: 1
**nbcatsync**

`nbcatsync` – run a utility that resyncs the disk media IDs in the image catalog after catalog recovery operations complete

**SYNOPSIS**

```
nbcatsync -backupid catalog_backup_id [-prune_catalog] [-no_sync_slp] [-dryrun] [-keepgoing]
```

```
nbcatsync -sync_dr_file dr_file_path [-copy number] [-dryrun]
```

On UNIX systems, the directory path to this command is `/usr/openv/netbackup/bin/admincmd`

On Windows systems, the directory path to this command is `install_path\NetBackup\bin\admincmd`

**DESCRIPTION**

`nbcatsync` is a post-processing utility that is used in the catalog restore process. After `bprecover` restores the actual catalog files, the `nbcatsync` utility can do the following:

- Fix the disk media IDs in the fragment records.
- Mark all recovered images as SS_COMPLETED.
- Restore disabled functionality.
- Prune images from the catalog which were not found on any currently configured disk volumes. The `-prune_catalog` option deletes catalog entries for the images that do not exist locally.
- Constrain the operation to a set of images based on the catalog restore that was performed.

You can easily create a list of affected backup images for any given catalog restore option. The catalog backup image `.f` file lists the images that the catalog restore recovers. This file lists the images to which you can constrain the operations of the `nbcatsync` utility.

The utility uses the current device configuration in EMM to obtain a list of disk volumes to scan for the image fragments that are found in the image list. After the EMM database, the images on currently configured storage, and the image catalog have all been reconciled, `nbcatsync` tries to turn on normal NetBackup processing.
Note: Use the `nbcatsync -dryrun` option to validate the `nbcatsync` utility operation before the utility actually does it. Because `nbcatsync` actions are irreversible, you would have to perform `bprecover -wizard` again to get the previous contents of the image catalog.

OPTIONS

- **-backupid catalog_backup_id**
  Specifies the catalog backup ID that contains a set of backup images. This option enables `nbcatsync` to fix disk media ID references in the image headers that are restored from this catalog backup image ID.

- **-copy number**
  Specifies the copy of the catalog to be restored. This option allows catalog recovery from a non-primary copy.

- **-dryrun**
  Gives the user a chance to validate actions `nbcatsync` normally perform. It lists all the modifications that can occur if the `nbcatsync` command does run.

- **-keepgoing**
  Ignores bad disk volumes. Otherwise, `nbcatsync` aborts when it encounters an unexpected error while it searches for images on a disk volume.

- **-no_sync_slp**
  Prevents the scrubbing of the storage lifecycle policy which removes the EMM image records and sets the SS_COMPLETED state in the image catalog to zero. Normally, `nbcatsync` disassociates images from any storage lifecycle policy processing that is performed at the primary site. Then `nbcatsync` can apply appropriate storage lifecycle policy settings for the DR site on the fixed images. However, when `-no_sync_slp` is specified, `nbcatsync` does not change these settings of fixed images, so use this option with care.

- **-prune_catalog**
  Prunes all non-existent images. `-prune_catalog` removes copies of images on the disk volumes that are not found on any of the disk volumes at the DR site. If none of the copies of an image are located, the image itself is deleted.

- **-sync_dr_file dr_file_path**
  Specifies the DR file at the DR site that corresponds to the catalog backup image to restore from.
EXAMPLES

Example 1 - Fix the disk media ID references in DR file test.txt, so that bprecover can find the catalog backup image. At the DR site, run the following command:

```
# nbcatsync -sync_dr_file test.txt
```

Example 2 - Perform a dry run of fixing the disk media ID references in the image headers of image ID rg9pctrain05_1254127131 that is restored from the catalog backup. When you are satisfied with the results, you can repeat the command without the -dryrun option.

```
# nbcatsync -backupid rg9pctrain05_1254127131 -dryrun
```

SEE ALSO

See bprecover on page 379.

See cat_export on page 487.

See cat_import on page 490.
**NBCC**

NBCC – run the NetBackup consistency check (NBCC) utility.

**SYNOPSIS**

```
```

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/support/

On Windows systems, the directory path to this command is `install_path\NetBackup\bin\support\`

**DESCRIPTION**

The **NBCC** command executes the NBCC utility that is used to confirm the integrity of portions of the NetBackup catalog and databases, including the following elements:

- Tape media and associated images
- The NBDB image, ImageCopy table records, ImageFragment table records, and the image catalog
- Enterprise Media Manager (EMM) server entries and configured storage unit entries

If **NBCC** detects catalog inconsistencies, it generates a set of output files. It can create a support package bundle of these files by using available system utilities.

These inconsistencies include the images whose associated media servers are not known to the EMM database. In these cases, you can use the `-unknown_image_servers_option` feature to select one of the following options: comment out, expire, or let a known media server inherit the images associated with these unknown media servers.

For more about the NBCC utility, see the *NetBackup Troubleshooting Guide*.

**OPTIONS**

- `--batch`
  Runs NBCC in a non-interactive mode. In this mode, the following occurs:
- If the output report already exists, NBCC automatically overwrites it.
- After the processing of `bpimagelist` information, any media servers that EMM does not know about are flagged. The full analysis then generates all repairs to be commented out for later review.
- If NBCC detects no NetBackup catalog inconsistencies, it does not create a support package.

`-debug`  
Adds additional program debug information to the `nbcc-info.txt` file, which greatly increases the size of this file.

`-gather`  
Gathers NetBackup configuration and catalog information only. This option does not check NetBackup catalog consistency.

`-help`  
Outputs a more expanded version of help information about the NBCC utility.

`-idar`  
Includes the identification of the abandoned tape media resources in the consistency check.

`-kbfree freespace`  
Specifies the amount of free file system space that is required to run NBCC. Only whole numbers are allowed. The default value is located in the help output.

The NBCC default is: Free file system space (Kilobytes)= 2048000.

To skip all free file system space checking, set this value to zero (0) to run in a non-English locale environment.

`-locale locale_name`  
Designates the NetBackup common_local_name. NBCC searches for this name in the following file:

On UNIX: `/usr/openv/msg/.conf`

On Windows: `\VERITAS\msg\LC_CONF`

This name determines the associated date format to use with the `bpimagelist` `-d` command line option.

`-nocleanup`  
If NBCC runs the consistency checks with no inconsistencies detected, it does not clean up the resultant support package or files.
**Note:** Do not use the `-nocleanup` option and the `-gather` option together. They are mutually exclusive because of the consistency check state.

- **-nozip**
  
  Skips the creation of a support package bundle. The generated NBCC files remain in the output directory.

- **-terse**
  
  Extracts only the fields that are associated with the consistency checks from each catalog record into the individual catalog content files.

- **-unknown_image_servers_option**
  
  Designates the action that the consistency analysis takes for any media server that is detected in the image database that is unknown to the EMM. `option` is one of the following values:

  - **comment_all** - Comments out all Suggested Repair Actions (SRAs) that the analysis program generates that are related to the images associated with an unknown media server. Thus, NBCCR does not try to process these commented-out repairs.
  
  - **expire_all** - The SRAs that the analysis program generates for NBCCR to process expire all images that are associated with any unknown media servers.
  
  - **inherit_all hostname** - Designates a known media server (`hostname`) to replace the unknown server. This new server inherits all the images that are associated with any unknown media server. The analysis program generates these SRA items for NBCCR to process. For example, the following command lets media server MS1 inherit all the images that are associated with any unknown media servers.

    ```
    # NBCC -unknown_image_servers_inherit_all MS1
    ```

- **-upgrade**
  
  Includes only the consistency checks that relate to the ability to upgrade the NetBackup catalog.

- **-use_reg_cmd [32 | 64]**
  
  Enables the use of the `Reg.exe` utility to query the Windows registry. The version of `Reg.exe` that supports the `/reg:32` or the `/reg:64` command line parameters must be installed so that this option works correctly.

  This option operates only on Windows systems.
PREREQUISITES

The following items are needed before you can use the NBCC utility:

- For NBCC to create a support package (if required), the path to the following programs must be included in the $PATH environment variable: `tar` and `gzip`. If `tar` is not available, use the `makecab` program (if available) to bundle and compress the output files.
  - If these programs are unavailable and you need a single support package file, manually bundle the files in the output directory into a support package.
- If you do not use the command line option `-kbfree 0`, NBCC inspects file system usage characteristics. Then it unloads the configuration information and catalog information and creates a support package. This information includes available free file system space (in Kilobytes). (Refer to the `-kbfree` option description.)
  - The EMM server must be operational.
  - The `vmd` process must run on the master server and on all other servers that act as the EMM server in the NetBackup configuration.
  - The `bpdbm` process must run on the master server.
  - On the installed NetBackup, all media servers and the `ltid` process must be running, and the network services must be configured.
  - The UTC time on all servers in the NetBackup configuration and the server where the NBCC utility is run, must be synchronized within a few minutes of each other.

Note: Failure to ensure that the clocks are synchronized may cause NBCC to report inaccurate results.

PROGRAM USAGE

The following are program usage considerations:

- NBCC runs from the support directory (see synopsis). If you want to run from a different directory, NBCC uses the following default directory location:
  - On UNIX: `/usr/openv/netbackup/bin/support/config`
  - On Windows: `install_path\NetBackup\bin\support`
To ensure that catalog consistency problems are identified and fixed correctly, verify the following: No NetBackup jobs are running or started from the time when the data is collected until the time when the repair work is completed. Because this condition is not possible in most configurations, NBCC tries to identify the tape media that are associated with active NetBackup jobs. Due to the propagation delay that may occur during normal processing, not all active tape media may be identified. Hence, you should carefully review the consistency analysis results.

NBCC detects EMM master servers. If more than one master server is detected, NBCC identifies the one that is associated with the system on which NBCC runs. NBCC uses the identified EMM master server to determine which EMM media servers are associated with that master server.

RETURN VALUES

The following exit values are returned:

0 = Consistency checks skipped (-gather)
    No inconsistency detected

1 = Inconsistency detected

2 = Program error condition detected:

    Invalid command line option
    .nbcc.lock file exists
    File permission problem
    File open/read/write problem
    Insufficient free disk space
    Unable to obtain the version of NetBackup
    Issue with NetBackup configuration information/detection
    Issue with NetBackup catalog information/detection

3 = -help information displayed
    -version information displayed

SEE ALSO

See NBCCR on page 571.
See nbcplogs on page 606.
See nbsu on page 867.
NBCCR

NBCCR – run the NetBackup consistency check repair (NBCCR) utility that repairs NetBackup database inconsistencies.

SYNOPSIS


On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/support/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\support\n
DESCRIPTION

The NBCCR command executes the NBCCR utility that is used to apply the repair actions that are related to tape. The repair actions are contained in a Suggested Repair Actions (SRA) file. This utility executes NetBackup commands to perform these repairs. Veritas Technical Support generates the SRA file based on an analysis of data that the NBCC command collects. The NBCCR command should be run only at the direction of Veritas Technical Support. It should be used only to apply repairs in an SRA file that Veritas Technical Support generates. The NBCCR command creates a history file containing the results of each repair action attempted.

The following items can cause inconsistencies: the improper use of command-line commands, attempts to restore corrupted data, or the improper decommission of a media server. A full file system can also cause inconsistencies.

For more about the NBCCR utility, see the NetBackup Troubleshooting Guide.

OPTIONS

-emmpwd EMMpassword

Specifies the name of the EMM password if different than the default password.
Note: Veritas recommends that you use the -emmpwd option to supply the password for the EMM database. NetBackup no longer uses a default password at NetBackup versions 7.7 and later. Failure to supply the proper password can result in failed repairs, which can make the inconsistencies harder to repair.

-help
Outputs the extended help information and exits.

-kbfree freespace
Specifies the amount of free file system space that is required to run NBCCR. Only whole numbers are allowed. The default value is located in the help output.

This value overrides the default free space value of 1024000 (1024*1024).

To skip all free file system space checking, set this value to zero (0) if you run in a non-English locale environment.

-sra SRAfile
Specifies the suggested repair action (SRA) file name. The default name is the following: master_name.NBCCA.SRA_timestamp.txt. The timestamp format is yyyymmdd_hhmmss.

-safe_pool_name safefilename
Overides the default safe pool name. The default is NBCC_SafePool.

-version
Prints the version of the NBCCR utility and exits.

-volumedatabasehost volDB_host
Only needed if the volume database host (or EMM host) is not the master server. If the volume database host is not the master, the volume database host needs to be specified here. If multiple masters use the same volume database host, it must be specified here. If there are multiple volume database hosts on one master, do the following: Ensure that all tapes that the SRA file references are for the same volume database host, which must be specified on the command line.

-use_reg_cmd [32 | 64]
Enables the use of the Reg.exe utility to query the Windows registry. The version of Reg.exe that supports the /reg:32 or the /reg:64 command line parameters must be installed so that this option works correctly.

This option operates only on Windows systems.

SEE ALSO

See NBCC on page 566.
See nbcplogs on page 606.
See nb su on page 867.
nbcertcmd — request and manage the host ID-based security certificates and tokens that are used to authorize certificate requests. Enroll an external certificate with a NetBackup host.

SYNOPSIS

nbcertcmd -checkClockSkew [-server master_server_name]
nbcertcmd -cleanupCRLCache -expired | -issuerHash SHA-1_hash_of_CRL_issuer_name
nbcertcmd -cleanupToken [-server master_server_name]
nbcertcmd -createCertRequest -requestFile request_file_name [-server master_server_name]
nbcertcmd -createECACertEntry -host host_name | -hostId host_ID -subject subject_name_of_the_certificate [-server master_server_name]
nbcertcmd -createToken -name token_name [-reissue -host host_name | -hostId host_id] [-maxUses number] [-validFor numDnumHnumM] [-reason description_for_auditing] [-server master_server_name]
nbcertcmd -deleteAllCertificates
nbcertcmd -deleteCertificate -hostId host_id [-cluster]
nbcertcmd -deleteECACertEntry -subject subject_name [-server master_server_name]
nbcertcmd -deleteToken -name token_name [-reason description_for_auditing] [-server master_server_name]
nbcertcmd -deployCertificate -certificateFile certificate_file_name
nbcertcmd -displayCACertDetail [-server master_server_name] [-json | -json_compact]
nbcertcmd -displayToken -name token_name [-json | -json_compact] [-server master_server_name]
nbcertcmd -ecaHealthCheck [-trustStorePath path_to_CA_certificate_file] [-certPath path_to_certificate_file] [-privateKeyPath path_to_certificate_key_file] [-passphraseFile path_to_passphrase_file] [-crlCheckLevel LEAF | CHAIN | DISABLE]
nbcertcmd -enrollCertificate [-force] [-preCheck] [-cluster] [-server master_server_name] [-remoteHost remote_host_name]


nbcertcmd -getCRL [-server master_server_name] [-cluster]

nbcertcmd -getExternalCertDetails -certPath path_to_certificate_file [-json | -json_compact]

nbcertcmd -getNBKeysize [-server master_server_name] [-json]

nbcertcmd -getSecConfig [-certDeployLevel] [-caUsage] [-server master_server_name]

nbcertcmd -hostSelfCheck [-cluster] [-server master_server_name]

nbcertcmd -listAllCertificates [-jks]

nbcertcmd -listAllDomainCertificates [-json | -json_compact] [-server master_server_name]

nbcertcmd -listCACertDetails [-json | -json_compact] [-cluster]

nbcertcmd -listCertDetails [-ECA | -NBCA] [-json | -json_compact] [-cluster]

nbcertcmd -listEnrollmentStatus [-remoteHost remote_client_name] [-cluster] [-json | -json_compact]

nbcertcmd -listToken [-all] [-json | -json_compact] [-server master_server_name]

nbcertcmd -reissueCertificates [-cluster] [-server master_server_name]

nbcertcmd -removeCACertificate -fingerPrint certificate_fingerprint [-cluster]

nbcertcmd -removeEnrollment [-cluster] [-server master_server_name] [-remoteHost remote_client_name]

nbcertcmd -renewCertificate [-hostnameCerts] [-host host_name] [-cluster] [-server master_server_name]
nbcertcmd -revokeCertificate -host host_name | -hostId host_id [-reasonCode value] [-server master_server_name]
nbcertcmd -setSecConfig -certDeployLevel level [-server master_server_name]
nbcertcmd -signCertificate -token | -file authorization_token_file-requestFile request_file_name -certificateFile certificate_file_name
nbcertcmd -updateConf
nbcertcmd -updateCRLCache

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\

DESCRIPTION

The nbcertcmd command is used to request and manage host ID-based security certificates on each NetBackup host. A NetBackup host can be a master server, media server, or client. Use the command to enroll an external CA signed certificate with a NetBackup host.

This command is also used to create and manage the authorization tokens that may be required to request certificates for NetBackup hosts.

Additionally the command is used to set and retrieve the security configuration attributes.

The Privilege details table lists the operations that require administrator privileges and also the operations that do not require special privileges.
<table>
<thead>
<tr>
<th>Table A-1</th>
<th>Privilege details</th>
</tr>
</thead>
<tbody>
<tr>
<td>** Commands that require NetBackup administrator privileges **</td>
<td></td>
</tr>
<tr>
<td>-cleanupToken, -createECACertEntry, -createToken, -deleteToken, -deleteECACertEntry, -displayToken, -listAllDomainCertificates, -listToken, -reissueCertificates, -revokeCertificate, and -setSecConfig</td>
<td></td>
</tr>
<tr>
<td>** Note:** These operations require a bpnbat web log-on (bpnbat -login -logintype WEB) using an account that has NetBackup administrator privileges.</td>
<td></td>
</tr>
<tr>
<td>** Commands that require host administrator privileges **</td>
<td></td>
</tr>
<tr>
<td>-cleanupCRLCache, -createCertRequest, -deleteAllCertificates, -deleteCertificate, -deployCertificate, -displayCACertDetail, -ecaHealthCheck, -enrollCertificate, -getCACertificate, -getCertificate, -getCRL, -hostSelfCheck, -listAllCertificates, -listCertDetails, -listEnrollmentStatus, -removeCACertificate, -removeEnrollment, -updateCRLCache, -renewCertificate, and -updateConf</td>
<td></td>
</tr>
<tr>
<td>** Commands that do not require special privileges **</td>
<td></td>
</tr>
<tr>
<td>-checkClockSkew, -getExternalCertDetails, -getNBKeysize, -getSecConfig, -listCACertDetails, and -signCertificate.</td>
<td></td>
</tr>
</tbody>
</table>

For more information about host ID-based security certificates and authorization tokens, see the NetBackup Security and Encryption Guide.

The `nbcertcmd` supports the following operations:

- `cleanupCRLCache`  
  Cleans up the NetBackup Certificate Revocation List (CRL) cache.  
  This command option is only applicable for external CA-signed certificates.

- `cleanupToken`  
  Deletes the tokens that have reached their maximum usage count or have expired.  
  This command option is only applicable for NetBackup CA-signed certificates.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-createCertRequest</td>
<td>Generates a NetBackup security certificate signing request on the NetBackup host and saves it into the specified file. The command should be used on the NetBackup host when there is no connectivity with the master server. The command must be executed on the NetBackup host for which you want to request the certificate. Use the <code>-server</code> option to specify the master server name in the certificate signing request. This name is the master server from which the NetBackup host expects the certificate.</td>
</tr>
<tr>
<td>-createECACertEntry</td>
<td>Adds an entry for the host and the associated subject name of the certificate in the NetBackup database for secure communication with the master server. If you want to provide the subject name using the OpenSSL API, ensure that it is in the RFC 2253 format. This command option is only applicable for external CA-signed certificates.</td>
</tr>
<tr>
<td>-createToken</td>
<td>Creates a token for authorizing certificate requests. This command option is only applicable for NetBackup CA-signed certificates.</td>
</tr>
<tr>
<td>-checkClockSkew</td>
<td>Displays the time difference (in seconds) between the current host and the master server.</td>
</tr>
<tr>
<td>-deleteAllCertificates</td>
<td>Deletes all NetBackup certificates and keys that are available on the NetBackup host. This option is only applicable on media servers and clients. This command option is only applicable for NetBackup CA-signed certificates.</td>
</tr>
<tr>
<td>-deleteCertificate</td>
<td>Deletes the NetBackup certificate of the NetBackup host that is associated with the specified host ID and removes the specified host ID entries from the <code>CertMapInfo.json</code> file. This option is available on all NetBackup hosts. This command option is only applicable for NetBackup CA-signed certificates.</td>
</tr>
<tr>
<td>-deleteECACertEntry</td>
<td>Removes the association of the external certificate with the host. The certificate entry is deleted from the database. This command option is only applicable for external CA-signed certificates.</td>
</tr>
<tr>
<td>-deleteToken</td>
<td>Deletes the specified token. This command option is only applicable for NetBackup CA-signed certificates.</td>
</tr>
</tbody>
</table>
-deployCertificate  Reads the host security certificate from the specified certificate file and deploys it on the NetBackup host. The command must be executed on the NetBackup host on which the certificate signing request was generated.

This command option is only applicable for NetBackup CA-signed certificates.

-displayCACertDetail  Displays the NetBackup CA certificate details from the specified master server.

This command option is only applicable for NetBackup CA-signed certificates.

-displayToken  Displays the attributes and the value of a specified token.

This command option is only applicable for NetBackup CA-signed certificates.

-ecaHealthCheck  Checks whether the details that you have provided for the external CA-signed certificate are valid.

This command option is applicable only for external CA-signed certificates.

-enrollCertificate  Enrolls an external CA signed certificate with the NetBackup domain. This certificate is used during host communication.

This command option is only applicable for external CA-signed certificates.

-getCACertificate  Connects to the master server and gets the certificate of the NetBackup Certificate Authority (CA). It then displays the fingerprint of the certificate and adds it to the NetBackup trust store after confirmation from the user.

This command option is only applicable for NetBackup CA-signed certificates.

-getCertificate  This option performs the following actions:

- Requests a NetBackup certificate for the NetBackup host from the master server.
- Adds the certificate to the NetBackup trust store.
- Fetches the latest NetBackup certificate revocation list (CRL) and security level from the master server.

This command option is only applicable for NetBackup CA-signed certificates.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-getCRL</code></td>
<td>Fetches the latest certificate revocation list from the NetBackup CA on the master server. You can use the <code>-server</code> option to specify an alternate master server. Use the <code>-cluster</code> option to fetch the latest CRL from the global certificate store. This command option is only applicable for NetBackup CA-signed certificates.</td>
</tr>
<tr>
<td><code>-getExternalCertDetails</code></td>
<td>Lists the details of the specified external CA-signed certificate. This command option is only applicable for external CA-signed certificates.</td>
</tr>
<tr>
<td><code>-getNBKeysize</code></td>
<td>Displays the key size for the new certificate key pair that NetBackup generates.</td>
</tr>
<tr>
<td><code>-getSecConfig</code></td>
<td>Retrieves the specified security configuration attribute.</td>
</tr>
<tr>
<td><code>-hostSelfCheck</code></td>
<td>Indicates if the host's certificate is revoked or not revoked. In case of NetBackup CA-signed certificates, to ensure that you have the latest CRL information, first run <code>nbcertcmd -getCRL</code>. In case of external CA-signed certificates, to ensure that you have the latest CRL information, first run <code>nbcertcmd -updateCRLCache</code>. Before running the <code>nbcertcmd -updateCRLCache</code>, ensure that the latest CRLs are available at the location that is defined in the <code>ECA_CRL_PATH</code> configuration option.</td>
</tr>
<tr>
<td><code>-listAllCertificates</code></td>
<td>Lists the details of all security certificates that are available on the NetBackup host.</td>
</tr>
<tr>
<td><code>-listAllDomainCertificates</code></td>
<td>Requests all of the NetBackup certificates for the domain from a NetBackup master server. By default, this operation uses the first server entry in the NetBackup configuration (<code>bp.conf</code>). You can use the <code>-server</code> option to specify an alternate master server. This command option is only applicable for NetBackup CA-signed certificates.</td>
</tr>
<tr>
<td><code>-listCACertDetails</code></td>
<td>Lists the details of trusted CA certificates that are stored in the NetBackup trust store of the NetBackup host.</td>
</tr>
<tr>
<td><code>-listCertDetails</code></td>
<td>Lists the certificate details for each security certificate that is deployed on the NetBackup host.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-listEnrollmentStatus</td>
<td>Retrieves the enrollment status for the associated master servers from the local certificate store. The enrollment status can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- Enrolled</td>
</tr>
<tr>
<td></td>
<td>- Not enrolled</td>
</tr>
<tr>
<td></td>
<td>- To be updated</td>
</tr>
<tr>
<td>-listToken</td>
<td>Lists the tokens. The option does not display the token value. This command option is only applicable for NetBackup CA-signed certificates.</td>
</tr>
<tr>
<td>-reissueCertificates</td>
<td>Generates a new key pair and reissues the host ID-based and host name-based certificates to the host. In a cluster, do the following to reissue certificates:</td>
</tr>
<tr>
<td></td>
<td>- Run the <code>nbcertcmd -reissueCertificates -cluster</code> command on the active node to update CA certificate in the global trust store and reissue the virtual identity certificate.</td>
</tr>
<tr>
<td></td>
<td>- Run the <code>nbcertcmd -reissueCertificates</code> command on each cluster node to reissue host ID-based and host name-based certificates.</td>
</tr>
<tr>
<td>-removeCACertificate</td>
<td>Removes the NetBackup CA certificate from the NetBackup trust store that is used for secure communications, whose fingerprint matches with the input fingerprint. Use the <code>-listCACertDetails</code> option to view fingerprint of existing CA certificates. This command option is only applicable for NetBackup CA-signed certificates.</td>
</tr>
<tr>
<td>-removeEnrollment</td>
<td>Removes the external certificate details with respect to the specified master server from the local certificate store. The certificate is neither deleted from the system nor from the NetBackup database.</td>
</tr>
<tr>
<td>-renewCertificate</td>
<td>Renews an existing host ID-based certificate. Use the <code>-hostnameCerts</code> option to renew host name-based certificates. Use the <code>-host</code> option to change the primary name of the host. This command option is only applicable for NetBackup CA-signed certificates.</td>
</tr>
<tr>
<td>-revokeCertificate</td>
<td>Revokes a NetBackup certificate. The NetBackup host can no longer use the certificate to communicate with the master server. This command option is only applicable for NetBackup CA-signed certificates.</td>
</tr>
<tr>
<td>-setSecConfig</td>
<td>Sets the specified security configuration attribute.</td>
</tr>
</tbody>
</table>
-signCertificate  Reads the certificate signing request from the specified request file and sends it to the NetBackupCA on the master server that is listed in the signing request. The signed certificate is stored in the specified certificate file. The command must be executed on the NetBackup host which has connectivity with the master server. This command option is only applicable for NetBackup CA-signed certificates.

-updateConf  Updates the external certificate-specific configuration options once the ecaHealthCheck command is successfully run.

-updateCRLCache  Updates the NetBackup CRL cache with the CRL files that are present at ECA_CRL_PATH. The ECA_CRL_PATH setting is specified in the NetBackup configuration file. The CRL file present at ECA_CRL_PATH is used if it is valid and more current than the cached CRL copy. This command option is only applicable for external CA-signed certificates.

**Note:** Clustered NetBackup hosts have two certificate stores, a local certificate store and a global certificate store. The command operates on the local certificate store by default, unless the -cluster option is specified.

**Note:** Please be aware the nbcertcmd command does not support non-US ASCII (non-7 bit ASCII) characters for user-defined strings.

**OPTIONS**

-all  Displays all tokens, including the tokens that have reached their maximum usage count or have expired.

-caUsage  Specifies the certificate authorities (CA) - NetBackup CA, external CA, or both - that the NetBackup domain supports. The output of the command can be one of the following:

- **NBCA:ON ECA:OFF** - Indicates that the web server uses only the NetBackup certificate authority signed certificates.

- **NBCA:OFF ECA:ON** - Indicates that the web server uses only the external certificate authority signed certificates.
- **NB:ON ECA:ON** - Indicates that the web server uses both the NetBackup certificate authority-signed certificates as well as the external certificate authority signed certificates.

---

### -certDeployLevel level

Specifies the NetBackup certificate's deployment level. The option is applicable for both the `-getSecConfig` and `-setSecConfig` commands. The `-setSecConfig` command requires that you specify a level. Certificate deployment levels for the `-setSecConfig` parameter are:

- **0** - Very High: Automatic certificate deployment is disabled.
- **1** - High: Certificates are automatically deployed to known hosts.
- **2** - Medium: Certificates are automatically deployed to all requesting hosts.

---

### -certPath

Specifies the path to the certificate file.

---

### -crlCheck

Specifies the revocation check level for external certificates of the host. You can specify the following values:

- **DISABLE** or **0**: Revocation check is disabled. Revocation status of the certificate is not validated against the CRL during host communication.
- **LEAF** or **1**: The revocation status of the leaf certificate is validated against the CRL. **LEAF** is the default value for this option.
- **CHAIN** or **2**: The revocation status of all certificates in the certificate chain are validated against the CRL.

---

### -crlPath

Specifies the path to the directory where the certificate revocation lists (CRL) of the external CA are located.

---

### -ECA

Lists the certificate details for each external certificate authority signed certificate that is deployed on the NetBackup host. If this option is not specified, the NetBackup certificate details are retrieved.

---

### -envtoken environment_variable

Indicates the name of an environment variable that contains the authorization token to be used for the request.

---

### -file file_name

Specifies the path of the file containing either the authorization token (on the first line) or the CA certificate hash.
-fingerprint certificate_fingerprint
    Specify the CA certificate fingerprint.

-fmt details | failures_only
    Provides details of the validation checks that are run for the external
certificate-specific configuration options. The details option provides a report
of all successful and all failed validation checks. The failures_only option
provides a report of only the failed checks.

-force
    If the option is used with the -getCertificate option, the certificate is
overwritten, if it exists. If the option is used with the -enrollCertificate
option, the given certificate is enrolled irrespective of the existing enrollment
status.

-host host_name
    Specifies the host name.

-hostId host_id
    Specifies the NetBackup host ID.

-hostnameCerts
    Specifies that you want to renew host name-based certificates.

-jks
    Displays the web server certificate information from Java keystore. This option
is available only on the NetBackup master server.

-json
    Generates output data in json format that spans multiple lines.

-json_compact
    Generates output data in json format on a single line.

-maxUses number
    Specifies the maximum usage count of the token. If this option is not specified,
the default value is 1. The maximum value for maxUses is 99999.

-name token_name
    Specifies the token name.

-NBCA
    Lists the certificate details for each NetBackup certificate that is deployed on
the NetBackup host.

-passphrasePath
    Specifies the path to the passphrase file that stores the passphrase, which is
used to decrypt the private key.
-privateKeyPath
    Specifies the path to the private key file of the certificate.

-preCheck
    Examines the external certificate and determines if it can be enrolled.

-reason description_for_auditing
    Specifies the reason that is stored in the audit record for this operation.

-reasonCode value
    Specifies a reason code for revocation of a certificate. The values that are shown are the only valid numbers for the -reasonCode value:
    0 - Unspecified, 1 - Key Compromise, 2 - CA Compromise, 3 - Affiliation Changed, 4 - Superseded, 5 - Cessation of Operation

-reissue
    Creates a token that can be used to reissue a certificate. Use this option with either the -host option or the -hostID option.

-remoteHost
    When you use -remoteHost with the -removeEnrollment option, an external certificate is enrolled for the specified remote host with the master server that you provide with the -server option.

    When you use -remoteHost with the -listEnrollmentStatus option, the -remoteHost option lists the enrollment status for the master servers that are associated with the specified remote host.

    When you use -remoteHost with the -removeEnrollment option, the -remoteHost option removes the enrollment of the specified remote host that exists with the specified master server.

    Ensure that the name of the server from where you run the -remoteHost option is listed in the SERVER configuration option of the remote host.

    For example: If you want to enroll a certificate for remoteHost1 from Server1, ensure the following in the configuration file on the remoteHost1: SERVER = Server1

-requestFile file_name
    Specifies the path of the certificate request file.

-server master_server_name
    Specifies an alternate master server. By default, this command uses the first server entry in the NetBackup configuration.
-subject
   Specifies the subject name of the external certificate. If you want to provide
   the subject name using the OpenSSL API, ensure that it is in the RFC 2253
   format.

-token
   Indicates that an authorization token is used for the request. Prompts the user
   to securely specify a token.

-trustStorePath
   Specifies the path to the certificate authority bundle file.

-updateTrustVersion
   Updates the NetBackup database with the host’s trust version. For successful
   activation of the NetBackup CA migration, the host’s trust version should match
   the master server’s trust version. A trust version of a host is an
   automatically-generated alphanumeric value and it defines the host’s CA setup.
   Each time the CA setup is changed, for example a CA is removed from the
   host’s trust store, the trust version is updated.

   A host’s trust version can be different than the master server’s trust version in
   the following scenarios:
   ■ One or more CA certificates from the master server’s trust store are not
     present in the host’s trust store
   ■ The host’s trust version is not updated in the NetBackup database

-validFor numDnumHnumM
   Specifies the validity of the token. Input format for this value should be for
   number of days, hours, and minutes. For example, 12D6H30M, would have a
   validity of 12 days, 6 hours, and 30 minutes. You can choose to specify one
   or more values. If this option is not specified, the default value is 24 hours.
   Please note that if you want to set the validity of the token to 12 hours, you
   don’t need to specify values for days or minutes. You can specify 12H. The
   maximum validity period that you can specify is 999 days.

-web
   Configures an external certificate for communication with the NetBackup web
   user interface.

EXAMPLES

Example 1: Create a token to request a certificate re-issue.
# nbcertcmd -createToken -name acme01_HR05 -reissue -validFor 10D -host HRfileservlet.acme.com -reason "issued token on request of Alice through email dated 12/08/2016"

Token XXXXXXXXXXXXXXX created successfully.

Example 2: Obtain a certificate from a specified master using a token

# nbcertcmd -getCertificate -token -server nbmaster01.acme.com

Authorization Token:
Host certificate received successfully from server nbmaster01.acme.com.

Example 3: Request and deploy a certificate on a NetBackup host that has no connectivity with the master server.

- Run the command that is shown on the NetBackup host that has no connectivity with the master server:
  
  # nbcertcmd -createCertRequest -requestFile /tmp/request_file_name -server master.servername
  
  Host certificate request generated successfully.

- Copy the /tmp/request_file_name to a NetBackup host that has connectivity with the master server and run the command that is shown on that NetBackup host:
  
  # nbcertcmd -signCertificate -file authorization_token_file -requestFile /tmp/request_file_name -certificateFile /tmp/signed_certificate
  
  Sending certificate request to server: master.servername

  Host certificate request signed successfully.

- Copy the /tmp/signed_certificate to the original NetBackup host where the request file (/tmp/request_file_name) was generated and run the command shown:
  
  # nbcertcmd -deployCertificate -certificateFile /tmp/signed_certificate
  
  Deploying certificate from master server: master.servername

  Host certificate deployed successfully

SEE ALSO

See bpnbat on page 242.
nbcertupdater

nbcertupdater – run the certificate update utility

SYNOPSIS

nbcertupdater -host host_name [-broker broker_name] [-port broker_port] [-v] [-d] [-nolog]
nbcertupdater -listonly -ofile output_file [-v] [-d] [-nolog]
nbcertupdater -help

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/
On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The certificate update utility (nbcertupdater) provides an automated mechanism to contact a set of NetBackup hosts that can run a setuptrust operation with a specified authentication broker. The utility can also query the NBU_Machines private domain of the local authentication broker to generate the following: the set of NetBackup hosts that you can contact for the setuptrust operation.

The utility can only be run as a local administrator on the master server. It runs in three modes:

- Process a single host. You specify a single host name on the command line. The utility contacts the host and runs setuptrust with the specified authentication broker.
- Process multiple hosts. You specify the host names in an input file. If an input file is unspecified, nbcertupdater automatically generates the list of hosts to contact from the NBU_Machines private domain of the local authentication broker. It spawns a child to process each host. The -numparallel option controls the number of hosts that are processed in parallel.
Create the host list from the authentication broker. The utility creates the list from the NBU_Machines private domain of the local authentication broker and writes it to the output file. The hosts are not processed.

OPTIONS

-b | -broker broker_name
The broker with which trust should be set up. If a broker is not specified, trust is set up with the NetBackup master server.

-d
Enables debug mode. The utility prints debug messages on the console.

-h | -host host_name
Specifies the NetBackup host where the setuptrust operation is performed.

-help
Prints command usage information.

-i | -ifile input_file
Specifies the name of the input file that contains the names of NetBackup hosts to be processed. Each line in the input file maps to a host name (except for comment lines).

-l | -listonly
Generates the list of NetBackup hosts from the local authentication broker, but does not process them.

-na | -numattempts attempts_per_host
Specifies the number of attempts to process the host before the utility declares failure. The default is 1.

-nolog
Shuts off all logging for the utility operation.

-np | -numparallel num_parallel_hosts
Specifies the number of hosts to be processed in parallel. The default is 3.

-o | -ofile output_file
Specifies the name of the output file.

-p | -port broker_port
Specifies the port number of the selected broker. If this option is not specified, the default broker port is used to contact the broker.

-v
Enables verbose mode. The utility prints extra informational messages on the console.
OUTPUT MESSAGES

HOST_NOT_FOUND

The host name cannot be found.

BPCD_CONN_FAIL

Failed to connect to bpcd on host. The host may not have NetBackup client software installed on it.

# bpnbat -ShowBrokerCerts

USER_INTERRUPT

User requested termination of operation. This error is returned if the user presses Ctrl-C to terminate the program.

SUCCESS

The host processed successfully.

EXAMPLES

Example 1 - Update a NetBackup host where the authentication client libraries are installed on it.

# nbcertupdater -h huffman.abc.com
Logging to directory /openv/netbackup/logs/certupdater>
Processing host huffman.abc.com
Host processed successfully

Example 2 - Generate a list of computer names from the NBU_Machines private domain of the local authentication broker. This list is the same as the list that is displayed when you run the bpnbat -ShowMachines command.

# nbcertupdater -listonly -o outfile.txt
Logging to directory </usr/openv/netbackup/logs/certupdater>
Generating host list from the local AB
Writing result to file <outfile.txt>

Example 3 - Use an input file to specify the hosts to be updated. The first host is updated successfully. bpcd is not running on the second host.

# cat infile.txt
huffman.vxindia.com
atom.vxindia.com
# nbcertupdater -i infile.txt -o outfile.txt
Logging to directory </usr/openv/netbackup/logs/certupdater>
Reading host names from file infile.txt
Attempt 1: Processing 2 hosts
Processing host huffman.abc.com (1/2)
Processing host atom.abc.com (2/2)
Completed host huffman.abc.com (SUCCESS)
Completed host atom.abc.com (BPCD_CONN_FAIL)
Total hosts attempted: 2 (1 succeeded)
Writing result to file <outfile.txt>

# cat outfile.txt
#huffman.abc.com #SUCCESS@(02/17/10 16:58:19)
atom.abc.com #BPCD_CONN_FAIL@(02/17/10 16:58:19)
nbclutil

nbclutil – the cloud storage utility for performing various operations specific to cloud deployment.

SYNOPSIS

nbclutil -appendcert -sourcecert source_certificate_path_and_name

nbclutil -copycert -sourcecert source_certificate_path_and_name [-destcert destination_certificate_path]


nbclutil -get_supported_api_list

nbclutil -validatecreds [-storage_server servername] [-username username] [-j]

nbclutil -help

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin

DESCRIPTION

Use the nbclutil command to validate user credentials and create buckets for Amazon S3 compatible cloud storage providers and Microsoft Azure.

Note: This utility only supports Red Hat Linux.

OPTIONS

-appendcert

This option appends certificate data in a .pem format to NetBackup cloud store CA certificate bundle. Use this option if your cloud vendor’s CA certificate isn’t present in the NetBackup cloud store CA bundle (cacert.pem) at the db/cloud location, or if it’s expired. The data is appended to the certificate in the install_path/var/global/wmc/cloud directory on UNIX and the install_path\netbackup\var\global\wmc\cloud directory on Windows.
-copycert
   This option copies the certificate to a specified destination.

-createbucket
   Creates a bucket in the cloud storage provider. The createbucket option requires the storage server, user name, and region name options for Amazon S3 compatible cloud storage providers. For Microsoft Azure, the region name option is not supported.

-destcert destination_certificate_path
   Use this option to copy the certificate to a specific path destination. By default, the certificate is copied to the install_path/var/global/wmc/cloud directory on UNIX and the install_path/netbackup/var/global/wmc/cloud directory on Windows. This parameter is optional. If the source file extension is not .pem but it is a valid .pem format, the command copies the file to the destination with the .pem extension.

   Be aware that you cannot use the -destcert option with the -appendcert option.

-get_supported_api_list
   Displays a list of nbcluthil supported APIs.

-help
   Displays help information for the command or option.

-j
   Generates output data in the json format that spans multiple lines.

-region
   For Amazon S3 compatible cloud storage region support, specifies the region in which to create the bucket. Use the Amazon suggested region values. If you do not add the region value, the default region is used.

-sourcecert source_certificate_path_and_name
   The file name and path of the source certificate.

-storage_server
   Specifies the cloud storage server for bucket creation or validation.

-username
   Specifies the user name of a user that has administrator privileges.

-validatecreds
   Validates the user credentials for the cloud storage provider. The validatecreds option requires the storage server and user name options.
When you run the `nbclutil` command with this option, a password prompt is displayed.

**EXAMPLES**

Example 1: Copy the certificate to a non-default location.

```
nbclutil -copycert -sourcecert /root/cert/file.pem
         -destcert /root/destpath/
```

Example 2: Append a certificate.

```
nbclutil -appendcert -sourceCert /root/certpath/file.pem
```

Example 3: Create Bucket in Amazon S3

```
nbclutil -createbucket -storage_server mystorage_server
         -username myusername -bucket_name bucketname -region us-west-1
```
nbcloudrestore

nbcloudrestore – restores an in-cloud asset using a Perl script.

SYNOPSIS


On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/goodies/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\goodies

DESCRIPTION

Use the nbcloudrestore command to restore in-cloud assets. The command supports Windows, RedHat Linux, and SUSE Linux master server platforms.

You must use Perl version 5.10 or later. You must also install the Perl modules that are listed on the NetBackup master server before you run the nbcloudrestore command. The modules must also appear in the list of search paths in the include paths (@INC).

- Getopt::Long
- Term::ReadKey
- HTTP::Response
- HTTP::Request
- JSON
- URI
- Data::Dumper
- LWP::UserAgent
- LWP::Protocol::http
- Pod::Usage
OPTIONS

-backupid backup_id
Use this option to provide the backup image identifier to use for this recovery. You can obtain the backup ID from the NetBackup Administration console > NetBackup Management > Catalog or with the bpimagelist command.

-copy_number copy_number
Specify the backup copy you want to restore. Valid values are 1 to 10. If not specified, primary copy is used.

-domainname domain_name
Use this option to provide the domain name for the user that is used to connect to the NetBackup master server.

-domaintype domain_type
Use this option to provide the domain type for the user that is used to connect to the NetBackup master server. Supported values are:

- NIS
- NIS+
- NT
- Vx
- Unixpwd
- Ldap

-destination_assetid destination_asset_id
Use this option to provide the NetBackup asset identifier for the recovery destination. If not specified, the asset is restored to its original location. This option is currently supported only with the recovery API.

-filter [filter]
Use this option to select the backup images for recovery based on the specified filter. This option must be used with the source_assetid option. The date range is specified in the format shown: YYYY-MM-DDTHH:MM:SSZ. You can also use ge to specify greater than or equal to, and le for less than or equal to when you specify the filter. The date range must contain a recovery point. Refer to the Recovery Points tab for the asset in the NetBackup web user interface. If more than one backup image matches the filter, NetBackup selects the most recent one.
-master_server master_server
  Use this option to specify the NetBackup master server that is used for running restore jobs.

-overwrite_existing overwrite_existing
  Use this option to overwrite an existing cloud asset. Accepted values for this option are true, which overwrites the original database, and false, which retains the original database. This parameter is optional.

-password password
  Use this option to provide the password for the user that is used to connect to the NetBackup master server. When you provide an empty value for password parameter, you are prompted for the password. For security reasons, the password is not displayed when you enter it at the prompt.

-port [port_number]
  Use this option to provide the port number to connect to the NetBackup master server.

-recovery_type recovery_type
  Specify the recovery type. Valid values are ORIGINAL, ALTERNATE, and ROLLBACK.

-recovered_state recovered_state
  Use this option with the ALTERNATE recovery type to select the recovered state of a database. Valid values are RECOVERED or NOT RECOVERED. This parameter is optional.

-source_assetid nb_source_asset
  Use this option to provide the NetBackup source asset identifier that was used at the time of backup. Recovery is performed using the most recent backup image, unless a filter is specified. You can obtain the source_assetid from the NetBackup web user interface by referring to the list of discovered cloud assets.

-username username
  Use this option to provide the user name to connect to the NetBackup master server.

-verbose verbose
  Use this option to set verbose levels for diagnostics purpose. Supported values are:
  ■ 1 for minimal
  ■ 2 for normal (the default value)
  ■ 3 for detailed
-wait_time  wait_time

Use this option to specify wait time in minutes. NetBackup waits for a completion status for the given duration from the master server before it returns you to the system prompt. If the wait time expires before the operation is complete, the command exits with a time-out status. The operation, however, still completes on the server. If you specify 0 or empty value, the default time-out value of 180 seconds is used.

EXAMPLES

Example 1: Restore an asset using a source asset ID with a date range.

./nbcloudrestore.pl -master_server example.server.com -username root
     -password - source_assetid 18e0a55a-6732-40d9-9c98-323fc2975bdc
     -filter "backupTime ge "2018-05-01T01:01:01Z" and backupTime le
     "2018-05-31T23:20:50Z""

Example 2 - Restore an asset using the backup ID.

./nbcloudrestore.pl -master_server example.server.com -username root
     -password - backupid aws-ec2-ap-south-1-i-02df039d2b68671b_1525946138

SEE ALSO

See bpiimagelist on page 171.
nbcomponentupdate

nbcomponentupdate – update the JRE version

SYNOPSIS


On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/goodies/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\goodies\n
DESCRIPTION

This utility lets you upgrade the installed version of the JRE in Veritas NetBackup and OpsCenter products. This utility does not support JRE update for NetBackup Plug-in for VMware vCenter.

The NetBackup installed version of the JRE is the supported major version for that NetBackup release. Use this utility to update to a minor version of the supported major JRE version. Veritas recommends that you update to another major JRE version only if the JRE vendor declares an end-of-life for the installed JRE version.

Close the product, such as NetBackup, before you attempt to update the JRE. If the product is active when you attempt the update, the utility exits with an error message that requests you to close the product.

Caution: Do not stop the utility while the JRE update is in progress. This action can cause the product that uses the JRE, such as NetBackup, to become unstable.

If there are additional versions of the JRE installed on your system for different applications, the NetBackup JRE does not interfere with them. The NetBackup JRE does not provide integration with web browsers and does not allow Java Applets or Web Start to run. For that reason, the NetBackup JRE cannot be used in a browser-based attack that uses Java Applet or Web Start vulnerabilities.

More information about the nbcomponentupdate command is available.
If you use OpsCenter or the NetBackup Remote Administration Console, the location of the command is as follows:

- **OpsCenter Server**
  - UNIX/Linux: SYMCOpsCenterServer/bin/
  - Windows: install_path\server\bin\n
- **OpsCenter Agent**
  - Windows: install_path\agent\bin\n
- **OpsCenter View Builder**
  - Windows: install_path\viewbuilder\bin

- **NetBackup Remote Administration Console**
  - Windows: install_path\java

---

### OPTIONS

- **-component value**
  Updates the specified component. The only valid value for this option is JRE.

- **-dryrun**
  Runs a test to verify if the operation is allowed.

- **-force**
  Skips the interactive mode. If you use -force and the -product is RemoteJavaConsole, you must use the -version option.

- **-help | -?**
  Prints the help.

- **-logpath path**
  Specifies the location of the log files. By default, the logs are generated in the system temp folder. On a Windows computer, you can specify the path %temp%nbcomponentupdate_date_time.log. Please note that the behavior of the option depends on what is specified.

  - If the path you specify is a folder or a drive, the log file is generated in the specified location. If you specify -logpath as C:\logs, the log file is C:\logs\nbcomponentupdate_date_time.log.

  - If you have specified a file name for -logpath and the file does not exist in that location, a new file is created with the specified name. If you specify C:\samplelogfile.log, the logs are generated in the C:\samplelogfile.log file.
If you have specified a file name in the log path and the file exists in that location, the logs are appended to that file. If you specify -logpath as C:\samplelogfile.log, the logs are appended to the samplelogfile.log file.

**Note:** Do not specify a network path such as an NFS or a CIFS share for the log path.

- **-path component_path**
  Specifies the path where the new version of JRE for the upgrade is located. The component_path is either the installed JRE location or the extracted JRE folder.

- **-product [NetBackup | OpsCenterServer | OpsCenterAgent | OpsCenterViewBuilder | RemoteJavaConsole]**
  Updates the JRE version of the specified product. This option is not case-sensitive. If the selected product is the NetBackup Remote Administration Console, the command lists all installed Remote Administration Console versions. You are then prompted to select a supported version of Remote Administration Console you want to update.

- **-revert**
  Reverts the currently installed update of the JRE to the previously installed JRE version.

- **-skipmajorversioncheck**
  Allows the utility to perform a JRE update to any higher major or higher minor version.

- **-version value**
  The version of the Remote Java Console that you want to upgrade or revert. This option is only available if you specify RemoteJavaConsole for the -product option. This limitation is because only the Remote Java Console maintains multiple versions that you can upgrade or revert.

  If you do not specify this option, the utility lists all the installed Remote Java Console version. The utility then prompts you to select a supported version of the console to upgrade or revert. If you use the -force option, you must specify the -version option.

**EXAMPLES**

Example 1: A dry run for an OpsCenter upgrade
Example 2: An interactive update for NetBackup

$ /usr/openv/netbackup/bin/goodies/nbcomponentupdate -product NetBackup -component jre -path /downloadedJre/jre1.8.0_91/

Command line: /usr/openv/netbackup/bin/goodies/nbcomponentupdate -product NetBackup -component jre -path /downloadedJre/jre1.8.0_91/

Java Runtime Environment(JRE) version installed with product 'Veritas NetBackup': 1.8.0_31 (64bit)
Java Runtime Environment(JRE) version found at path '/downloadedJre/jre1.8.0_91': 1.8.0_91 (64bit)

This utility will update the Java Runtime Environment(JRE) binaries present at '/usr/openv/java/jre' path

This utility may start and stop all (or some) services depending upon the present state of services.

Do you want to continue (Y[es]/N[o]): Yes

Performing upgrade steps ...
After upgrading, Java Runtime Environment (JRE) version installed with product 'Veritas NetBackup': 1.8.0_91 (64bit)

Successfully upgraded Java Runtime Environment (JRE) for Veritas NetBackup. The log file generated for this operation is /tmp/logs/nbcomponentupdate/nbcomponentupdate_12-08-2016_16.15.13.log

Example 3: Non-interactive revert for NetBackup

```
# ./nbcomponentupdate -product NetBackup -component jre -revert -force
Command line: /usr/openv/netbackup/bin/goodies/nbcomponentupdate -product NetBackup -component jre -revert -force

Java Runtime Environment (JRE) version installed with product 'Veritas NetBackup': 1.8.0_91 (64bit)
After revert, Java Runtime Environment (JRE) version with product 'Veritas NetBackup': 1.8.0_31 (64bit)

This utility will update the Java Runtime Environment (JRE) binaries present at '/usr/openv/java/jre' path

This utility may start and stop all (or some) services depending upon the present state of services.

Performing revert steps ...
```

[1/4] Pre-installation step is in progress
[1/4] Pre-installation step is completed successfully

[2/4] Installation step is in progress
[2/4] Installation step is completed successfully

[3/4] Post-installation step is in progress
[3/4] Post-installation step is completed successfully

[4/4] Commit and Cleanup step is in progress
[4/4] Commit and Cleanup step is completed successfully
Installation step is completed successfully

Post-installation step is in progress

Post-installation step is completed successfully

Commit and Cleanup step is in progress

Commit and Cleanup step is completed successfully

After reverting, Java Runtime Environment(JRE) version installed with product 'Veritas NetBackup': 1.8.0_31 (64bit)

Successfully reverted Java Runtime Environment(JRE) for Veritas NetBackup.
The log file generated for this operation is /tmp/logs/nbcomponentupdate/nbcomponentupdate_22-08-2016_13.07.42.log

Example 4: An interactive revert for Remote Java Console

D:\sandbox>nbcomponentupdate.exe -product remotejavaconsole -component jre -revert -logpath D:\LogFolder
Command line: D:\sandbox\nbcomponentupdate.exe -product remotejavaconsole -component jre -revert -logpath D:\LogFolder

Following NetBackup Remote Java Console instances found on the host are supported by the utility:

1> NetBackup - Java (NB-Java) 7.7 JRE : 1.8.0_31 (64bit)

2> NetBackup - Java (NB-Java) 7.7.1 JRE : 1.8.0_31 (64bit)

3> NetBackup - Java (NB-Java) 7.7.2 JRE : 1.8.0_77 (64bit)

** NOTE **
Unsupported versions of Veritas NetBackup Remote Java Console found on the host:
NetBackup - Java (NB-Java) 7.6, NetBackup - Java (NB-Java) 7.5

Please enter choice [(1 - 3) or Q(uit) to exit]: 3

After revert, Java Runtime Environment(JRE) version with product 'Veritas NetBackup Remote Java Console': 1.8.0_31 (64bit)

This utility will update the Java Runtime Environment(JRE) binaries present at 'D:\RJC772\Java\jre' path
Do you want to continue (Y[es]/N[o]): y

Performing revert steps ...

[1/4] Pre-installation step is in progress
[1/4] Pre-installation step is completed successfully

[2/4] Installation step is in progress
[2/4] Installation step is completed successfully

[3/4] Post-installation step is in progress
[3/4] Post-installation step is completed successfully

[4/4] Commit and Cleanup step is in progress
[4/4] Commit and Cleanup step is completed successfully

After reverting, Java Runtime Environment (JRE) version installed with product 'Veritas NetBackup Remote Java Console' : 1.8.0_31 (64bit)

Successfully reverted Java Runtime Environment (JRE) for Veritas NetBackup Remote Java Console.
The log file generated for this operation is D:\LogFolder\nbcomponentupdate_22-08-2016_16.22.13.log
nbcplogs

nbcplogs – copy all NetBackup logs to a designated destination

SYNOPSIS


On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/support/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\support\n
DESCRIPTION

The nbcplogs command copies logs from various locations in the NetBackup system to a common area where you can more easily troubleshoot a problem. This utility lets you determine what logs are copied. To reduce the size of the copied logs, you can use the time frame option to specify a start time and an end time.

If you have a case ID provided by Technical Support in the form ######, rename the log files with the case ID number. Then manually upload the files to the Veritas Evidence server. More information is available:

http://www.veritas.com/docs/000097935

For more about nbcplogs, see the NetBackup Troubleshooting Guide.

OPTIONS

--compress-before-bundle
Compresses the log files, then bundles them and adds them to the tarball. Compressing the files first instead of after the files are copied reduces peak disk usage.

destination
Specifies the destination of the logs to be collected.
-d | --duration valued | valueh | valuem
Sets the duration of the log data to be collected. The time units of the duration can be in d[ays], h[ours], or m[in]. For example:

--duration 5h /tmp/logs

--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 when you copy large log files such as bpdbm. This option is rarely needed and should be used with caution.

--filecopy
File copy is the default condition. It copies the entire log file.

--help-long
Displays a complete set of options available for the nbcplogs command.

-l | --logs log_type[.sub] [...] [,...]
Limits the log types that are collected to only those specified on the command line. The sub option lets you specify a sub-category of a log type. If no log types are specified, all log types are copied.

--list-products
Lists all the possible logs that can be reported on.

--list-subproducts log_product
Lists all the log subproducts for the specified log product.

--nbsu | --no-nbsu
Enables (--nbsu) or disables (--no-nbsu) running the nbsu utility as part of the nbcplogs command operation. The nbsu command utility gathers a wide range of diagnostic information that is helpful when it is used with the log data that is gathered.

The default condition is that nbsu runs and creates a support package to send to Technical Support.

-s | --start mm/dd/yyyy-hh:mm:ss | mm/dd-hh:mm -e | --end
mm/dd/yyyy-hh:mm:ss | mm/dd-hh:mm
Sets the start time (-s) or the end time (-e) for the collection of logs.

The -s option specifies a start date and time for the logs. If no corresponding -e option is used, the utility collects all log data from the start time to the present.
The -e option specifies an end date and time for the logs. If no corresponding 
-s option is used, the utility collects all log data present in the log files up to 
the end date.

If no start time or end time is specified, the default time period is the last 24 
hours.

--tmpdir=pathname

Specifies the staging directory the command uses when it bundles the logs 
into a tarball.

If --tmpdir is not specified, the default staging directory is used. That directory 
is:

Windows: C:\temp

UNIX or Linux: /tmp

--use-reg-cmd [32|64]

This option is required when you run the nbcplogs command on a non-English 
Windows server.

--write-config

Lets you to view or modify nbcplogs configuration values. This option creates 
a nbcplogs configuration file (nbcplogs.conf), which you can then edit.

EXAMPLES

Example 1 - Copy all volmgr logs between 1:00 and 2:00.

# nbcplogs --start 01:00 --end 02:00 --logs volmgr /tmp/logs

Example 2 - Copy the last 24 hours of nbpem logs and bpdbm logs, and run the nbsu 
utility:

# nbcplogs -l nbpem,bpdbm

Example 3 - Display the complete set of options available to use with the nbcplogs 
command:

# nbcplogs --help-long

Example 4 - List all the log directories available on your system:

# nbcplogs --list-products

* products:
*   db : /usr/openv/db/log
*   dberror : /usr/openv/netbackup/db/error
Example 5 - Display the complete set of log subproducts available for the `nbcplogs` command:

```bash
# nbcplogs --list-subproducts vxul
* vxul.111 = /usr/openv/logs/nbemm aliases: 111, nbemm, vxul.nbemm
* vxul.116 = /usr/openv/logs/nbpm aliases: 116, nbpm, vxul.nbpm
* vxul.117 = /usr/openv/logs/nbjm aliases: 117, nbjm, vxul.nbjm
* vxul.118 = /usr/openv/logs/nbrb aliases: 118, nbrb, vxul.nbrb
* vxul.119 = /usr/openv/logs/bmrd aliases: 119, bmrd, vxul.bmrd...
```
nbcredkeyutil

nbcredkeyutil – refreshes the encryption key that NetBackup's credential management system uses.

SYNOPSIS

nbcredkeyutil -add | -list
nbcredkeyutil -help

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd

DESCRIPTION

The nbcredkeyutil command is used to add new encryption keys and list the existing keys that NetBackup's credential management system uses.

OPTIONS

-add

Adds a new encryption key to NetBackup's credential management system, the new key will be used for future encryption work. The existing keys are maintained for decryption.

-help

Displays the nbcredkeyutil command syntax.

-list

Lists the encryption keys' tags that are found in NetBackup's credential management keystore.
**nbdb_admin**

nbdb_admin – start or stop individual databases and change default password

**SYNOPSIS**

```
nbdb_admin -dba new_password [-dbn NBDB | NBAZDB] [-backup directory]
nbdb_admin -start | stop [database_name]
nbdb_admin [-vxdbms_nb_data directory] [-vxdbms_nb_staging directory] [-vxdbms_nbdb_backup_owner y|n] [-vxdbms_nb_server servername | EMMSERVER] [-auto_start NONE | NBDB | BMRDB | NBAZDB]
nbdb_admin -adjust_server_settings [database_name]
nbdb_admin -enable_request_logging [-persistent] [-duration minutes] [-logfile filename]
nbdb_admin -disable_request_logging
nbdb_admin -analyze_request_log -logfile filename
nbdb_admin -list
nbdb_admin -reorganize [database_name]
nbdb_admin -validate [database_name] [-full]
```

On UNIX systems, the directory path to this command is /usr/openv/db/bin/

On Windows systems, the directory path to this command is \install_path\NetBackup\bin\n
**DESCRIPTION**

The nbdb_admin command can be used to start or stop the NetBackup database (NBDB), the NetBackup Authorization database (NBAZDB), or the Bare Metal Restore database (BMRDB).

The nbdb_admin command line utility can also be used to enable the customer to change the DBA and application passwords. The DBA and application passwords are encrypted and stored in the *vxdbms.conf* file. The permissions on the file enable the root user on UNIX or a Windows administrator to read or write it.
During installation, a randomly generated password is created for the NBDB, NBAZDB, and BMRDB databases for all DBA and application accounts. The same password is used for the NBDB and the BMRDB DBA and application accounts such as EMM_MAIN. A different randomly generated password is created for the NBAZDB database.

This command can enable and disable a request logging tool that is used to troubleshoot NetBackup database performance issues at the highest SyBase database logging level. Use request logging for a problem that has an active support case. An `analyze_request_log` option reads the request log that the NBDB generates and performs some basic log analysis. Because of the excessive resource usage and general overhead, we do not recommend that you use this tool in a production environment.

**OPTIONS**

- `--adjust_server_settings directory`
  Adjusts the settings of the given database `directory` through the Sybase utility. If no database is specified, the default is to adjust all databases.

- `--analyze_request_log`
  Reads the request log generated by the NetBackup database and does some basic analysis. This procedure can cause excessive resource utilization and is not recommended for use on a production environment. Request logging for NBDB may be useful only if the customer is experiencing NBDB performance issues and has an active support case.

- `--auto_start NONE | NBDB | BMRDB | NBAZDB`
  Sets which databases are automatically started when the database server is started. You can specify the NetBackup database (NBDB), the BMR database (BMRDB), or the NetBackup Authorization database (NBAZDB). The database daemon must be stopped and restarted to take effect. Or you can choose not to start any of the databases by using NONE.

- `--dba new_password [-dbn NBDB | NBAZDB] [-backup directory]`
  Changes the existing password for the NBDB and the BMRDB databases for all DBA and application accounts if `-dbn` is not specified or if `-dbn NBDB` is specified. It changes the existing password for the NBAZDB database if the `-dbn NBAZDB` option is specified. The NBAZDB database password is different than the password for the NBDB and the BMRDB databases and application accounts. The password must be an ASCII string. Non-ASCII characters are not allowed in the password string.
If the -backup option is used, the new password is saved in the specified directory with the file name nbdbinfo.dat. Otherwise, it is saved under the default location with the same file name.

**Note:** If the password is set to the old default password (nbusql), it is reset to a randomly generated password at the next NetBackup upgrade.

This action is also true for the NBAZDB password which is reset to a different randomly generated password. If the NBAZDB password is the same as the NBDB password, the NBAZDB password is reset to a randomly generated password at the next NetBackup upgrade.

This action will require a restart of the NetBackup Web Management Console service.

- **disable_request_logging**
  Deactivates request logging and removes any request log settings from the server.conf file. Any change in server.conf requires that you restart the NetBackup relational database service.

- **duration minutes**
  Disable request logging after the specified time in minutes. Specify 0 to manually disable later.

- **enable_request_logging**
  Activates request level logging for NBDB at the maximum level for troubleshooting. The overhead of request logging may affect performance and is not recommended for regular use. Request logging for NBDB may be useful only if the customer is experiencing NBDB performance issues and has an active support case.

- **list**
  Lists all database files.

- **logfile filename**
  Specifies the absolute path to the log file for NBDB to use. If this option is not present, the absolute path is generated at the default location.

- **persistent**
  Saves the request logging settings to the server.conf file so that request logging continues after the NetBackup relational database service (NBDB) is restarted.

- **reorganize database_name**
  Reorganizes the given database through the Sybase utility. If no database is specified, the default is to reorganize all databases.
-start | -stop database_name

Starts or stops the database that is identified in the database_name field. You can specify the NBDB database or the BMRDB database. The database_name field is optional. The NBDB database is the default for this command.

Note: Before you take the database offline with the -stop option, stop all services that are running except SQL Anywhere.

-validate database_name [-full]

Validates the indexes and keys on all of the tables in the specified database. If no database name is specified, the option validates all the databases. It scans each table and checks that each row exists in the appropriate indexes. The number of rows in the table must match the number of entries in the index.

The -full option performs a full validation of the database or databases. It ensures that every row that is referenced in each index exists in the corresponding table. For foreign key indexes, it also ensures that the corresponding row exists in the primary table.

The validation checks do not require that all NetBackup activity be suspended. However, the checks may report any transient errors that are a result of transactions that are in progress.

-vxdbms_nb_data directory

This command updates the VXDBMS_NB_DATA parameter that is stored in the bp.conf file on UNIX systems and in the registry on Windows systems. This parameter contains the main location of the NBDB and the BMRDB databases.

-vxdbms_nbdb_backup_owner y|n

This command updates the VXDMMS_NBDB_BACKUP_OWNER parameter in the bp.conf file on UNIX systems and in the registry on Windows systems. This command specifies if the master server owns the backup of the databases that are included in the catalog backup. The default for this parameter is yes.

-vxdbms_nb_server servername | EMMSERVER

Changes the database server name to the given servername or EMMSERVER from bp.conf file.

-vxdbms_nb_staging directory

Changes the staging directory from the default to the specified directory. This option saves the information in the vxdbms.conf file.

SEE ALSO

See nbdb_backup on page 616.
See nbdb_move on page 618.
See nbdb_ping on page 620.
See nbdb_restore on page 621.
See nbdb_unload on page 623.
nbdb_backup

nbdb_backup – run the program that is used to make a backup of the databases in a directory

SYNOPSIS

```
nbdb_backup [-dbn database_name] [-offline | -online] destination_directory [-tlog_only] [-truncate_tlog]
```

On UNIX systems, the directory path to this command is /usr/openv/db/bin/
On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

The `nbdb_backup` command enables the customer to make either an online backup or offline backup of the SQL Anywhere files to a file system directory. Use this command to perform maintenance operations and make a copy of a database.

OPTIONS

- **-dbn database_name**
  Sets the database that `database_name` identifies for backup. The possible databases are NBDB and BMRDB. The default is to back up both databases if they are installed on the server.

- **-offline | -online**
  Enables either an offline or an online backup of the SQL Anywhere database files.
  - Online backup - the database is up and in operation during the backup.
  - Offline backup - shuts down the database.

- **destination_directory**
  Identifies the directory where the backup is stored.

- **-tlog_only**
  Generates only the database transaction log backup along with the configuration files for an online backup.
-truncatelog

Truncates the database transaction log after the backup completes on an online backup.

SEE ALSO

See nbdb_move on page 618.
See nbdb_ping on page 620.
See nbdb_restore on page 621.
See nbdb_unload on page 623.
nbdb_move

nbdb_move – move location of the NBDB database files after installation

SYNOPSIS

nbdb_move -data data_directory [-index index_directory] [-tlog log_directory] [-mlog log_directory] [-config_only] [-owner EMM | DBM | DARS]

On UNIX systems, the directory path to this command is /usr/openv/db/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

nbdb_move moves the NBDB and the BMRDB database files from the default directory locations to customer-specified directories. This action separates data from indexes and transaction logs to improve performance. This command also moves database data files and transaction files to the following default location:

On UNIX systems: /usr/openv/db/data.

On Windows systems: install_path\NetBackupDB\data.

Caution: Veritas supports moving the NetBackup catalog to a non-default location on a Windows cluster after installation or upgrade. Before any upgrades, however, you must move the NetBackup catalog back to the default location for the upgrade to succeed. Do not attempt a NetBackup upgrade if the catalog is not in the default location. You master server is rendered unusable if you fail to move the database back to the default location before upgrade.

Note: In a cluster environment, nbdb_move moves the database files to the desired location and changes the VXDBMS_NB_DATA entry in bp.conf on the active node. However, you must manually change the VXDBMS_NB_DATA entry in bp.conf on the inactive node.
OPTIONS

-`config_only`
  Updates the configuration files with the directory locations specified. The database files are not moved. Use this option in a recovery operation when the database files were already relocated manually and need their configuration settings to be saved.

-`data data_directory`
  Moves the main database files to the customer-specified directories that `data_directory` designates.

-`index index_directory`
  Changes the directory of the index database files.

-`mlog log_directory`
  Creates a mirrored transaction log and puts it in a designated directory location. If a mirrored log already exists, this command can be used to move it to a different location.

-`owner EMM | DBM | DARS`
  Moves the database data, index, or log files for a specified data space.

-`tlog log_directory`
  Changes the transaction log directory.

SEE ALSO

See `nbdb_backup` on page 616.
See `nbdb_ping` on page 620.
See `nbdb_restore` on page 621.
See `nbdb_unload` on page 623.
nbdb_ping

nbdb_ping – display status of NetBackup database (NBDB) or BMR database (BMRDB).

SYNOPSIS

nbdb_ping [-q] [-dbn database_name]

On UNIX systems, the directory path to this command is /usr/openv/db/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

The nbdb_ping command is used to check and display the status of the NetBackup database (NBDB) or the BMR database (BMRDB). Enter the command with no options to display the status of NBDB.

OPTIONS

-dbndatabase_name
    Displays the status of the specified BMR database.

-q
    Puts the command in Quiet Mode. It does not make any standard output.

SEE ALSO

See nbdb_backup on page 616.
See nbdb_move on page 618.
See nbdb_restore on page 621.
See nbdb_unload on page 623.
nbdb_restore

nbdb_restore - recover the database that is backed up to a directory using
nbdb_backup

SYNOPSIS

nbdb_restore -recover source_directory [-dbn database_name]
[[-ignore_tlog]

nbdb_restore -recover -staging [-dbn database_name]

On UNIX systems, the directory path to this command is
/usr/openv/db/bin/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\

DESCRIPTION

The nbdb_restore command does a restore and recovery from a backup to a
directory using nbdb_backup. The recommended method to protect the SQL
Anywhere NBDB and BMRDB databases is through the Catalog Backup interfaces.

nbdb_restore restores from the staging directory to recover only the NBDB. The
default is to apply the current online transaction log. By default, the current online
transaction log is applied to make the database as consistent as possible with the
current db/images directory.

OPTIONS

-dbnd database_name
    Specifies the database name of the NBDB to be recovered.

-ignore_tlog
    Does not apply the current online transaction log to the NBDB recovery
    operation.

-recover source_directory
    The location of the backup.

-staging
    Restores the NBDB from the staging directory.
EXAMPLES

Example 1 - Restore and recover NBDB from the copy in the default staging directory.

# nbdb_restore -dbn NBDB -ignore_tlog -recover -staging

SEE ALSO

See nbdb_backup on page 616.
See nbdb_move on page 618.
See nbdb_ping on page 620.
See nbdb_unload on page 623.
**nbdb_unload**

nbdb_unload – unload NetBackup databases (NBDB) or BMR (BMRDB)

**SYNOPSIS**

```
nbdb_unload [-dbn database_name] [-t tablelist] [-s] [-staging] destination directory
nnbdb_unload [-dbn database_name] -rebuild [-verbose]
```

On UNIX systems, the directory path to this command is
/usr/openv/db/bin/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\

**DESCRIPTION**

The `nbdb_unload` command unloads the specified database. By default the NBDB database is unloaded. The other value for `-dbn` includes BMRDB for the Bare Metal Restore database.

**Note:** The Enterprise Media Manager (EMM) database is a component of the NBDB database.

The `nbdb_unload` command creates .dat files, one for each table in the database or in the table list. Each .dat file contains comma-separated lines, one for each row in the table. It also creates a `reload.sql` file that contains the SQL statements that are required to reload the database. For example:

```sql
LOAD TABLE "BmrDba.BMR_Configuration" FROM
```

UNIX systems:

```
/temp/data/345.dat
```

Windows systems:

```
c:\temp\data\345.dat
```

Run the `reload.sql` file to transfer the destination directory contents to a support computer and use it to create a copy of the customer’s database.
OPTIONS

-\texttt{dbn} \textit{database\_name}
  Specifies the database that is to be unloaded.

-\texttt{rebuild}
  Rebuilds the default NetBackup database (NBDB).

-\texttt{s}
  Unloads the schema only - no data is unloaded.

-\texttt{staging}
  Unloads the media table and related tables to a set of flat files. You can use
  SQL tools to insert the subset of data that is needed into another copy of NBDB.

-\texttt{t} \textit{table\_list}
  Specifies a comma-separated list of tables to unload instead of all the tables
  in the database.

-\texttt{verbose}
  Generates more detailed information for the output.

\textit{destination\_directory}
  Specifies the directory where the user wants the dump of the data and schema.

EXAMPLES

Example 1 - Unload the NBDB database (including all of EMM), data and schema:

UNIX systems: \# nbdb\_unload /tmp/nbdb\_dump

Windows systems: \# nbdb\_unload C:\temp\nbdb\_dump

Example 2 - Unload only the NBDB schema:

UNIX systems: \# nbdb\_unload -s /tmp/nbdb\_dump

Windows systems: \# nbdb\_unload -s C:\temp\nbdb\_dump

Example 3 - Unload only the EMM\_STU table (by using fully qualified table names):

UNIX systems: \# nbdb\_unload -t EMM\_MAIN.EMM\_STU /tmp/stu

Windows systems: \# nbdb\_unload -t EMM\_MAIN.EMM\_STU C:\temp\stu

Example 4 - Unload the BMR database:

UNIX systems: \# nbdb\_unload -dbn BMRDB /tmp/bmr\_dump

Windows systems: \# nbdb\_unload -dbn BMRDB C:\temp\bmr\_dump
SEE ALSO

See `nbdb_backup` on page 616.
See `nbdb_move` on page 618.
See `nbdb_ping` on page 620.
See `nbdb_restore` on page 621.
nbdb2adutl

nbdb2adutl – used to query or extract DB2 archive logs from the NetBackup catalog.

SYNOPSIS

nbdb2adutl nbdb2adutl query logs db database_name [inst instance_name] [between sn1 and sn2] [chain n | all] [partition n | all] [browse_client client_name]

nbdb2adutl nbdb2adutl extract logs db database_name [inst instance_name] [between sn1 and sn2] [chain n | all] [partition n | all] [browse_client client_name]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

Use the nbdb2adutl command to interact with the DB2 archive logs found in the NetBackup catalog.

When you use the query option, the command queries the NetBackup catalog for DB2 archive log backups. The inst option is only required when the instance name (DB2INSTANCE) is not found in the environment.

When you use the extract option, the command restores DB2 archive logs from NetBackup to the user’s current working directory. Existing log files are not overwritten. For this reason, be careful when you use all with either partition or chain. The inst option is only required when the instance name (DB2INSTANCE) is not found in the environment.

By default, the original user who backed up the archive logs or any user from the same group has access to the archive log backups. Permissions are set at backup time using the BKUP_IMAGE_PERM option. See the NetBackup for DB2 Administrator’s Guide for more information.
OPTIONS

between sn1 and sn2

Identifies the range of archive log sequence numbers. The specified sequence numbers are inclusive in the range. If the option is omitted, all sequence numbers that meet the specified criteria are returned.

browse_client client_name

Identifies the name of the client where the backups were performed. Used for alternate client restores. Master server must be configured for alternate client restore, i.e altnames, etc. If not specified, the browse client is determined from the bp.conf.

chain n | all

Identifies the archive log chain number. Use all to indicate that you want all chain numbers included. The default value is 0.

db database_name

Name of the database.

extract

Identifies that a restore operation is to be performed.

inst instance_name

Name of the instance. The option is required if the name of the instance cannot be obtained from the DB2INSTANCE environment value.

logs

Identifies that the DB2 archive logs are the object.

partition n | all

Identifies the DB2 database partition. Use all to specify all partition numbers. The default is 0.

query

Used to search the NetBackup catalog for DB2 archive log backups.

EXAMPLES

Example 1: Query all the logs for a database named sample where the instance is prod, the partition is 0, and the chain is 0.

nbdb2adutl query logs db sample inst prod

Example 2: Query log sequence numbers 5 to 10 for the sample database, where the instance is prod, the partition is 0 and the chain is 0. Instance prod is found in the environment.
nbdb2adutl query logs db sample between 5 and 10

Example 3: Restore log sequence numbers 5 to 10 for the sample database, where the instance is prod, the partition is 0, and the chain is 0.

nbdb2adutl extract logs db sample inst prod between 5 and 10

Example 4: Alternate client restore log sequence number 5 to 10 for the sample database from the production server prodbox.sample.com, where instance is prod, the partition is 0, and chain is 0.

nbdb2adutl extract logs db sample inst prod between 5 and 10 browse_client prodbox.sample.com

SEE ALSO

See bplist on page 215.
nbdbms_start_server

nbdbms_start_server – start and stop database server

SYNOPSIS

nbdbms_start_server

nbdbms_start_server -stop [-f]

nbdbms_start_server -stat

The directory path to this command is /usr/openv/db/bin

DESCRIPTION

This command operates only on UNIX systems.

Sybase ASA runs as a daemon on UNIX that starts or stops by using a script. If you initiate the program without any argument, the server starts.

OPTIONS

-stop

Causes the server to shut down.

-stat

Returns a status that indicates if the server is up or down. A zero (0) indicates that the server is active (up).

-f

Causes a forced shutdown of the server irrespective of active connections. This option is only applicable when used with the -stop option.
nbdbms_start_stop

nbdbms_start_stop – start and stop NetBackup database on the server

SYNOPSIS

nbdbms_start_stop [start | stop]

The directory path to this command is /usr/openv/netbackup/bin/

DESCRIPTION

This command operates only on UNIX systems.
The nbdbms_start_stop command starts and stops the Sybase ASA daemon.

OPTIONS

stop
   Causes the server to shut down.

start
   Starts the server.
nbdc

nbdc – add, modify, or list NetBackup data classifications

SYNOPSIS

nbdc -add -n name -r rank [-v] [-M master_server] [-d description]
nbdc -L | -l [-v] [-M master_server]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

The nbdc command names data classifications and sets their rank. Data classifications are the labels that the user can attach to backup images. They allow NetBackup to treat different kinds of data differently. Only storage lifecycle policies can use data classifications.

The nbdc command can do one of the following:

- Add (-add) a new data classification. The new level requires a name and a rank, and optionally, a description and a master server name if multiple master servers are present.
- List (-L or -l) the data classifications.
- Modify (-modify) the name, rank, or description of a specified data classification.

OPTIONS

-d description
   Specifies the new description for the designated data classification. This description is commentary only.

-dc class
   Specifies the data classification ID (GUID) to be modified.
-l
List the data classifications. The output contains only information. The fields do not have names. A line appears for each level with the fields that are space delimited.

-L
List the data classifications. The field name identifies the output fields. A line is output for each level and is formatted to print within the field headings.

-M master_server
Specifies a master server. The default is the local server.

-n name
Identifies the new name for the specified data classification. Default names are Platinum, Gold, Silver, and Bronze.

-r rank
Identifies the new rank for the specified data classification ID. The rank is the method by which NetBackup determines the importance of a data classification in relation to other data classifications.

-v
Selects the verbose mode for logging.

EXAMPLES

Example 1 - List all data classifications. Only two levels (ranks) are shown.

```
# nbdc -L

Rank: 4
Name: Bronze
Description: "lowest rank"
Classification ID: B1F664D41DD111B2ACFB99708C0940D1

Rank: 1
Name: Platinum
Description: "highest rank"
Classification ID: B4C999D41DD111B2FFFB99704C6660D4
```

Example 2 - Change the description of Rank 4 to "really the lowest rank":

```
# nbdc -modify -sl B1F664D41DD111B2ACFB99708C0940D1 -d "really the lowest rank"
```
SEE ALSO

See nbstl on page 845.

See nbstlutil on page 854.
nbdecommission

nbdecommission – decommission an old media server, NDMP host, or replication host

SYNOPSIS

nbdecommission -oldserver hostname

[-list_ref | -newserver hostname [-bulk_media_move] [-file op_dump_file]]

[-machinetype [media | foreign_media | ndmp | replication_host]]

[-M master_server] [-reason "reason"] [-v]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/
On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The nbdecommission utility is an interactive tool that assists in disabling, removing, or identifying policies, storage units, backup images, storage lifecycle policies, and storage devices so that a media server, NDMP host, or a replication host can be retired or replaced. The -list_ref -oldserver hostname option displays all that is associated with the old server, which allows users to break the associations on their own. This option does not decommission the server.

The -oldserver hostname [-newserver hostname] option provides detailed guidance to decommission the old server. You can run the command on the master server or any server that is not decommissioned. The decommissioning process is clean and removes old media server or replication host entries in the EMM database which can slow down backup operations. The command does not assume that the old server is up and responsive. The optional -newserver lets you specify a replacement server for the old server. The -newserver option is not valid for the replication_host machine type.
**Note:** Replication hosts are unique in that they are not a host in the local NetBackup domain. Rather, a replication host is a storage server in the target or the source domain of a replication relationship. The `nbdecommission` utility guides the removal of the replication relationship(s) with the storage server in the local domain, not the actual storage server in the remote domain.

**Warning:** Be careful when you use the `nbdecommission` command. Because the command may expire images, data loss may occur. Therefore, you should understand completely what the command does before you use it. Veritas recommends that you first preview all of the references to a media server, NDMP host, or replication host before you decommission it.

### OPTIONS

- **-file decom_ops.txt**
  Writes the command operations to the specified file. Replace `decom_ops.txt` with a name that signifies its purpose or contents. You can use the `-file` option to maintain a record of the command operations.

- **-list_ref -oldserver hostname**
  Displays the items that are associated with the old server. Use this option to break the associations yourself or to view existing associations.

- **-machinetype**
  The type of the server that you want to decommission. List one of the following types: `media`, `foreign_media`, `ndmp`, or `replication_host`.
  
  If not provided, `nbdecommission` automatically determines the type of server.

- **-newserver hostname**
  Specifies a new server to replace the old server that is to be decommissioned. If you specify a new server, it becomes the default media server or NDMP host for the replacement operations.
  
  This option is not valid for the replication host machine type.

- **-oldserver hostname**
  Initiates detailed guidance in decommissioning the old server. The command can be run on the master server or any server that is not decommissioned.
  
  This option does not assume that the old server is up and responsive.

- **-reason "string"**
  Indicates the reason for performing this command action. The reason text string that you enter is captured and appears in the audit report. Enclose the string as a string.
with double quotes ("...") and the string cannot exceed 512 characters. It cannot begin with a dash character (-) nor contain a single quotation mark (').
nbdelete

nbdelete – remove deleted fragments from disk volumes

SYNOPSIS

nbdelete -allvolumes [-ost_worm_lock | -snapshots | tar] [-priority number]
nbdelete -list [-snapshots | tar] [[-dt disk_type -media_id name] | -backup_id bid [-copy_number number]]
nbdelete (-dt disk_type -media_id name | -backup_id bid [-copy_number number]) [-ost_worm_lock | -snapshots | -tar] [-media_server name -storage_server name -priority number -bpdm_media_server name]
nbdelete -deletion_stats [-U] [-snapshots] -stype server_type [-dp disk_pool_name [-dv disk_volume_name]]
nbdelete -deletion_stats [-U] [-tar] -media_id name
nbdelete -purge_snap_deletion_list -stype server_type -media_id name -dp disk_pool_name -dv disk_volume_name [-force]
nbdelete -purge_deletion_list (-media_id name | -backup_id bid [-copy_number number]) [-force]
nbdelete -list

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The nbdelete command removes all deleted fragments from the disk volumes that
are specified on the command line. The -allvolumes option removes the fragments
from all volumes that contain deleted fragments. The -dt, -media_id,
-media_server, and -storage_server options specify an individual volume where
deleted fragments should be removed.

The nbdelete command can also be used to refresh the write-once read-many
(WORM) properties of copies by using the -ost_worm_lock option.
The `nbdelete` command can perform three operation types. These operations can be combined in a single execution of the command. The `-tar` option removes fragments from storage. The `-snapshots` option deletes snapshots. The `-ost_worm_lock` option finds the copies that require a retry or refresh of setting storage WORM attributes.

**OPTIONS**

- **-allvolumes**
  Queries the image list in the EMM database to obtain the list of volumes with deleted fragments. It removes the fragments from those volumes and deletes eligible imported snaps, unimported snaps, and NetBackup (tar) images in that order. `-allvolumes` calls `bpdm` on master server to delete imported snaps. It also queries the storage servers with unimported snapshots but does not direct `bpdm` to delete them.

  If no operation mode parameters (`-tar`, `-snapshots`, or `-ost_worm_lock`) are specified, the default modes are `-tar` and `-snapshots`. You must explicitly specify the `-ost_worm_lock` parameter in order for WORM processing to take place.

- **-bpdm_media_server name**
  Starts up `bpdm` on the specified media server. Use if a media server has a much faster network connection to the disk volume's storage server for the delete operations.

- **-copy_number cnum**
  Limits the images to be processed to the specified copy number.

- **-deletion_stats**
  Displays information about disk fragments in the `DeletedImageFragment` table or snapshots in the `DBM_DeletedSnapReplica` table that are ready to be deleted.

  Fragment or snapshot records are placed in these tables when their corresponding copies are expired from the NetBackup image catalog. This option queries `nbemm` to retrieve the number of deletable fragments and the total number KBytes that are waiting to be deleted.

- **-dp disk_pool_name**
  Specifies the disk pool name. When `-dp` is used with `-stype` but not `-dv`, then `-bprecover` returns stats for all images for the disk pool. Only applicable to operations that are related to snapshots.
-dt disk_type
  Specifies the disk type where the deleted fragments should be removed. The
  following are the valid values for disk_type:

  0 - All
  1 - BasicDisk
  6 - DiskPool

-dv disk_volume_name
  Specifies the disk volume name. Only applicable to operations that are related
to snapshots.

-force
  Proceeds without asking for user verification.

**Note:** Before you run nbdelete with the -force option, ensure that all media
servers and valid disks can communicate with the master server. If they are
unable, the -force option removes the expired images from EMM but it orphans
the image fragments on the disk. Once an expired image is removed from
EMM, there is no further attempt to remove the image disk fragments.

-list
  Lists imported and unimported snapshots or NetBackup (tar) images eligible
for deletion. The list may be limited to the image with the specified backup ID
and the specified copy number. You can also limit the list to images on a given
media ID.

-media_server name
  Specifies the name that represents the media server for the volume whose
deleted fragments are to be removed.

-media_id
  Specifies a 6-character media ID (that is, @aaaa0).

-ost_worm_lock
  Finds copies which have a Pending WORM state. Copies in such a state
indicate that some failure may have occurred while NetBackup tried to set the
WORM attributes for that copy. If any copies that require attention are found
in the catalog, requests are made to storage attempting to set the correct
WORM attributes.

  Note that this operation does not result in deletion of any fragments.

-priority number
  Specifies a new priority for the job that overrides the default job priority.
-purge_deletion_list
   Removes all entries from deletion lists for a disk volume without trying to contact
   storage or delete anything from storage. This function is useful if a storage
   server has been decommissioned but deletable image records are still in the
   NetBackup catalog.

-purge_snap_deletion_list
   Removes all entries from snapshot deletion lists for a disk volume without trying
   to contact storage or delete anything from storage. This function is useful if a
   storage server has been decommissioned but deletable image records are still
   in the NetBackup catalog.

-snapshots
   Deletes all eligible imported and unimported image snapshots. When
   -snapshots is used with -deletion_stats on the command line, nbdelete
   displays stats for deletable unimported snapshots.

-storage_server name
   Specifies the name that represents the storage server of the volume whose
   deleted fragments are to be removed.

-stype server_type
   Specifies a disk storage server type. If you do not use the -dp option with
   -stype, the command returns stats for all images of the storage server type.
   Only applicable to operations that are related to snapshots.

-tar
   Deletes NetBackup (tar) images.

-U
   User mode query, with text header for each result. Default is comma-separated
   values.

EXAMPLES

Example 1

# nbdelete -deletion_stats -U -stype AdvancedDisk -dp ad_dp -dv /dv1
Frags : 6
KB : 2134

Example 2

# nbdelete -deletion_stats -U -media_id "aaaa0"
Frags : 2
KB : 64
Example 3: Only process WORM attributes for a specific copy.

```
#nbdelete -backup_id client_123456789 -copy_number 3 -ost_worm_lock
```

Example 4: Remove fragments from storage as needed; process WORM attributes as needed; and skips snapshots processing.

```
#nbdelete -allvolumes -tar -ost_worm_lock
```
**nbdeployutil**

nbdeployutil – deployment utility that gathers and analyzes master server information regarding clients and capacity

**SYNOPSIS**

nbdeployutil --debug-inputs dir1 [dir2 dir3]


nbdeployutil --report [--capacity ; --traditional] [--day-boundary=time] [dir1 dir2 dir# | --dirsfile=filename | --parentdir=directory] [--log=filename] [--nolog] [--overlap-details] [--runtimestats]

nbdeployutil --retry dir1 [dir2 dir#]

nbdeployutil --version

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
**DESCRIPTION**

The nbdeployutil utility gathers and analyzes deployment information from the master server. The utility performs a deployment analysis according to one of two NetBackup licensing models, either Traditional Licensing or Capacity Licensing. A Traditional Licensing deployment analysis counts the number of clients and servers then compares this information against licensed options. Capacity Licensing deployment analysis calculates how much source data is protected.

The command is run in two steps. nbdeployutil gathers the data in the first step and analyzes the data in the second step.
The `nbdeployutil` command supports incremental reporting. With this feature, `nbdeployutil` runs based on a specified frequency to incrementally gather data and generate capacity-based licensing reports. For more information on how to enable and use this feature, please see the NetBackup Administrator’s Guide Volume II.

The utility generates a log file named `nbdeployutil-gather-timestamp.log` during the gathering operation. The utility generates a log file named `nbdeployutil-report-timestamp.log` during the analysis and the report generating operation. By default the log files are created in the directory where the gathered data resides.

For more information on Traditional and Capacity based licensing, see the NetBackup Administrator’s Guide Volume II.

**OPERATIONS**

```plaintext
--client-timeout seconds
    This option enforces a time-out for `bptestbpcd` within `nbdeployutil` independent of the NetBackup configuration.

    This option is only applicable if the `--gather` option is specified. The option not applicable if `--capacity` is specified.
```

```plaintext
--debug-inputs
    Converts the files that are used to generate the report into human-readable format. These new files are easier to read than the raw output. You can only specify the directories that contain basic ASCII characters. Directories with extended ASCII characters are not permitted.
```

```plaintext
--exclude-all-clients
    This option lets you exclude all clients from `bptestbpcd` connections. The specified clients show up in the report as unconnectable.

    This option is only applicable if the `--gather` option is specified. The option not applicable if `--capacity` is specified.
```

```plaintext
--exclude-clientlist path
    Use this option to specify a file that contains a list of clients to exclude from `bptestbpcd` connections. List each client name on a separate line within the file. The specified clients show up in the report as unconnectable.

    This option is only applicable if the `--gather` option is specified. The option not applicable if `--capacity` is specified.
```
--exclude-clients client1[,client2,...]
This option lets you exclude any of the specified clients from bptestbpced connections. The specified clients show up in the report as unconnectable.

This option is only applicable if the --gather option is specified. The option not applicable if --capacity is specified.

--gather
Collects data for analysis with the report option. If the capacity or traditional parameter is used, only data for that specific license model is collected. If neither capacity nor traditional is specified, gather collects data for both license models.

On NetBackup 8.0 or later master servers, when you run the nbdeployutil --gather command in capacity licensing, you are prompted for additional information. You must enter the credential information that is shown for authentication of the NetBackup web management service:

- **Domain Type**: Enter a domain type value from NIS, NISPLUS, WINDOWS, vx, unixpwd, ldap. This value is case-sensitive.
- **Domain Name**: Name of the domain that the master server host belongs to. If the master server does not belong to any domain, enter the name of the master server.
- **User name**: Name of the user that has administrator privileges.
- **Password**: The password of the same user that has administrator privileges. When you enter the password, characters are intentionally not displayed in the command line.

In a multi-master server scenario, you must enter the credentials for all the master servers that are mentioned with the gather command.

--report

Produces a license report based on the data that is collected with the gather option. Specify the directory or list of directories for the utility to use for the report. You must use either the capacity or the traditional parameter when using the --report operation.

--retry

Reruns the gather operation and attempts to reconnect to hosts which failed during gather process as determined by the information in the gather directory. This action is helpful with the traditional licensing model when multiple hosts are reported as unreachable.
--version
Returns the version of the command. This option is used to identify the latest NetBackup product version the command is designed to run against. The version string also indicates special versions of the utility, such as engineering binaries. This option is useful if utility was manually copied to a pre-7.1 master server.

OPTIONS

--bpimagelist
Use to pass specific options to bpimagelist command during the gather part of the process.

--capacity
Specifies the license model when used with gather or report. Use capacity to report on deployment according to NetBackup’s per terabyte capacity licensing model.

--client or --clientlist
Collects the data or reports on data for a specified client or list of clients only. When using client, separate multiple clients with a comma. To use the clientlist parameter, list the clients in the filename on separate lines. When you use the --client or the --clientlist option, the report may show some media servers as not connectable even though the utility can connect to them. This problem should not affect the summary information.

--day-boundary
Moves the start of the report window for creating reports. The default report window starts at midnight and runs to 11:59:59 P.M. Specify the time value as hh:mm in 24 hour notation, where 6:00 A.M. is 06:00 and 6:00 P.M. is 18:00.

--dirsfile
A file containing a list of directories which the report parameter uses to generate a report. This parameter is an alternative to listing all the files after the report parameter. You can also use the parentdir parameter to list a parent directory for the report parameter to use.

--end
Specifies the end date for a restricted date range of the collection period. This option is used only with the start option. The format for this parameter is "MM/DD/YYYY hh:mm:ss". Specify the time value hh:mm:ss in 24 hour notation, where 6:00 A.M. is 06:00:00 and 6:00 P.M. is 18:00:00. Double quotation marks must surround the date time value.
--hoursago
Changes the default value for the image gather time interval. The value is specified in hours. The default value is 2160 hours (90 days).

--log
Forces the log output to go to a specific log file. By default, the log output is written to a log file within the directory where the gathered data and report is stored.

--master
Gathers capacity licensing data for the specified master server. This option is only used with --gather. For the local host to gather data from a remote server, the host name must appear in the server list of the remote server.

This option only supports remotely gathered capacity licensing information. Remotely gathered traditional licensing data is not supported.

--nolog
Disable the creation of the debug log file.

--output
Saves the results in the indicated output directory. You can only specify the directories that contain basic ASCII characters. Directories with extended ASCII characters are not permitted. If the operation is a gather, the output directory holds gathered data. For report operations, the report and log file are put in the output directory instead of co-located with the gathered data in the specified input directory. If the output option is not specified, the output is placed in the following directory:

- UNIX: /usr/openv/var/global/reports/YYYYMMDD_hhmmss_masterserver
- Windows: install_path\NetBackup\var\global\reports\YYYYMMDD_hhmmss_masterserver

--overlap-details
Displays the duplicate backup selections in the Duplicate Selections column of the capacity licensing report. This option can only be used for ASCII or English-only characters in the backup selection data.

--parentdir
Specifies the top level in a directory tree containing many directories with the gathered licensing data that the report parameter should use to generate a report. You can also use the dirsfile parameter to specify a file that contains a list of directories.
--runtimestats
Displays runtime statistics for the utility. The statistics include memory and CPU usage.

Example UNIX output:

stats mem 40.1 M, cpu 27.0% after splitting t/fixture/
   nbdeployutil_sidon/bpimagelist_sidon.out
stats mem 40.1 M, cpu 28.0% after parsing records from t/fixture/
   nbdeployutil_sidon/tmp/policy_db_arc_tab_2gig_nt_client_tomet7.out
stats mem 40.6 M, cpu 50.0% after calculating for UNKNOWN-1 in
   t/fixture/nbdeployutil_sidon/ stats mem 40.6 M, cpu 51.0% after
   main report loop took 1 sec

--start
Specifies the start date for a restricted date range for the collection period. The format for this parameter is "MM/DD/YYYY hh:mm:ss". Specify the time value hh:mm:ss in 24 hour notation, where 6:00 A.M. is 06:00:00 and 6:00 P.M. is 18:00:00. Be aware the double quotation marks around the date time value are required.

--traditional
Used with gather or report to specify the license model. Use --traditional to report on deployment according to NetBackup traditional per server licensing model. The default value is 2160 hours (90 days).

--verbose
Outputs detailed progress information of the utility to the screen, which has no effect on the information in the debug log file. The contents of the log file are always verbose.

PREREQUISITES

The following are the prerequisites for the nbdeployutil utility:

- The master server daemons or services must run in the environment to gather the data.
- Confirm that sufficient disk space exists on the master server that runs the gather command. Gathering capacity licensing data collects bpimagelist output for the previous 90 days. The size of the output is a function of the number of images in the catalog for that period. The default time period can be moved or shrunk. Shorter time range analysis causes less accurate or incomplete figures.
- Microsoft Excel is required to view the report. The software does not have to be installed on the master server.
EXAMPLES

Example 1 - Create a deployment analysis report for both NetBackup's capacity licensing model and traditional license model. The directory paths are for a Windows system, but this example applies to a UNIX system as well.

```
# nbdeployutil --gather
NetBackup Deployment Utility, version 7.1.0000.0000
Gathering license deployment information...
   Discovered master server marybl2g1
   Output for marybl2g1 at: D:\Program Files\VERITAS\netbackup\var\global\reports\20101029_170534_marybl2g1
Gather DONE
Execution time: 1 min
To create a report for this master server, run the following:
   nbdeployutil.exe --report "D:\Program Files\VERITAS\netbackup\var\global\reports\20101029_170534_marybl2g1"

D:\>nbdeployutil.exe --report --traditional "D:\Program Files\VERITAS\netbackup\var\global\reports\20101029_170534_marybl2g1"
NetBackup Deployment Utility, version 7.1.0000.0000
Analyzing license deployment for master marybl2g1 ...
   Report created at: D:\Program Files\VERITAS\netbackup\var\global\reports\20101029_170534_marybl2g1\report-20101029_170705.xls
Analysis DONE
Execution time: 27 secs
```

Example 2 - Targeted deployment capacity analysis. The command gathers data for a subset of clients for a timeframe different than the default. The directory paths are for a Windows system, but this example applies to a UNIX system as well.

```
# nbdeployutil.exe --gather --output pickedclient --start "11/01/10 06:00:00" --end "11/02/10 01:00:00" --clients marybl2g1,marybl7g1 / --verbose NetBackup Deployment Utility, version 7.1.0000.0000
Gathering license deployment information...
   run: bpgetconfig
   run: bpimagelist -M marybl2g1 -d "11/01/10 06:00:00" -e "11/02/10 01:00:00" -l -client marybl2g1
   run: bpimagelist -M marybl2g1 -d "11/01/10 06:00:00" -e "11/02/10 01:00:00" -l -client marybl7g1
   Output for marybl2g1 at: pickedclient\20101102_155246_marybl2g1
Gather DONE
```
To create a report for this master server, run the following:

```bash
nbdeployutil.exe --report "pickedclient\20101102_155246_marybl2g1"
```

D:\# nbdeployutil.exe --report --capacity pickedclient\20101102_154010_marybl2g1 --start "11/01/10 06:00:00" --end "11/02/10 01:00:00" --clients marybl2g1, marybl7g1 --verbose

NetBackup Deployment Utility, version 7.1.0000.0000
Analyzing license deployment ...
Master marybl2g1
Report created at: pickedclient\20101102_154010_marybl2g1\report-20101102_155414.xls
Analysis DONE
Execution time: 2 secs

SEE ALSO

See `bpimagelist` on page 171.
**nbdevconfig**

nbdevconfig – preview, import, create, or inventory disk pools

**SYNOPSIS**

```
nbdevconfig -adddv -stype server_type [-dp disk_pool_name [-dv disk_volume_name]] [-M master_server]


nbdevconfig -createdp [-noverbose] -dp disk_pool_name -stype server_type -storage_servers storage_server... [-hwm high_watermark_percent] [-lwm low_watermark_percent] [-max_io_streams n] [-comment comment] [-dvlist filename] [-M master_server] [-reason "string"]


nbdevconfig -deletedp [-noverbose] -stype service_type -dp disk_pool_name [-M master_server] [-force_targetslp_removal] [-reason "string"]

nbdevconfig -deletedv [-noverbose] -dp disk_pool_name -stype server_type -dv disk_volume_name [-M master_server] [-reason "string"]
```
nbdevconfig -deletests [-noverbose] -storage_server storage_server
-stype server_type [-reason "string"]

nbdevconfig -getconfig [-l | -U] stype service_type -storage_server
storage_server [-configlist filename]

nbdevconfig -help operation

nbdevconfig -importenclr [-noverbose] -enclosure enclosure_name
-storage_servers storage_server... [-hwm high_watermark_percent]
[-lwm low_watermark_percent] [-comment comment] [-M master_server]

nbdevconfig -inventorydp [-preview | -noverbose] -stype server_type
-dp disk_pool_name [-media_server media_server] [-M master_server]

nbdevconfig -mergedps [-noverbose] -stype service_type -primarydp
disk_pool_name_1 -secondarydp disk_pool_name_2 [-M master_server]
[-reason "string"]

nbdevconfig -previewdv -storage_server storage_server -stype
server_type [-media_server media_server] [-dv disk_volume_name] [-dp
disk_pool_name] [-dvlist file_name] [-M master_server] [-replication
source | target | both] [[-include Primary | ReplicationSource |
ReplicationTarget | Snapshot | Independent | Mirror]...] [[-exclude
Primary | ReplicationSource | ReplicationTarget | Snapshot |
Independent | Mirror]...]

nbdevconfig -previewenclr [-l|-U] -enclosure enclosure_name |
-storage_server storage_server... [-M master_server]

nbdevconfig -setconfig -stype service_type -storage_server
storage_server [-configlist filename] [-reason "string"]

nbdevconfig -updatedp [-noverbose] -stype server_type -dp
disk_pool_name [-M master_server] [-reason "string"]

nbdevconfig -updatedv [-noverbose] -stype server_type [-dp
disk_pool_name] -dv disk_volume_name [-media_server media_server]
[-M master_server]

nbdevconfig -updatests [-noverbose] -storage_server storage_server
-stype server_type -media_server media_server [-reason "string"]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/
DESCRIPTION

The nbdevconfig command performs the following operations:

- **-adddv** adds a new disk volume to an existing disk pool. The disk volume must have the same attributes and flags as the disk pool. For example, you cannot add a mirror volume to a non-mirror disk pool. You can add multiple volumes by using the nbdevquery -preview option to collect like volumes on a file (-dvlist) to be added to the disk pool.

- **-changedp** changes the indicated properties of the disk pool. Specify the disk pool name option (-dp) and the storage server type (-stype) to identify the disk pool uniquely.

- **-changestate** changes the state of the disk pool or disk volume. If -dv is specified, then -changestate changes the specified disk volume of the disk pool. Otherwise, it changes the state of the disk pool itself. The value for the state can be UP, DOWN, or RESET.

- **-changests** changes the storage server.

- **-createdp** creates a disk pool from the specified list of disk volumes. Additional properties like High Water Mark and comments can be specified. The disk pool name cannot exceed 256 characters.

- **-createdv** creates a disk volume that you can then specify (-dvlist option) when you create a disk pool. Most commonly, use this option for the following: AdvancedDisk volumes that NetBackup cannot discover (such as CIFS volumes, which are not visible to Windows services) and for buckets in Amazon cloud storage regions other than US Standard

- **-creatests** creates a storage server. The storage server name cannot exceed 128 characters and cannot contain colon (:) characters.

- **-deletedp** deletes the specified disk pool from the NetBackup device database. Expire and delete all images before you run this option.

- **-deletedv** deletes the specified disk volume from the specified disk pool. No backup image fragments can exist on the volume. No backup jobs can be active on the volume. The disk volume and disk pool must be DOWN.

- **-deletests** deletes the specified storage server.

- **-getconfig** retrieves the default configuration parameters for the disk pool attributes.
-help operation specifies an operation (-changestate, -deletedp, ...) for which you want usage information.

-importenclr creates a disk pool from the specified enclosure. You can also specify additional properties like High Water Mark and comments.

-inventorydp discovers new storage or changed storage in a disk pool and accepts these changes. Storage changes include new volumes, change of volume size, or new LUNs. Use the -preview option if you only want to view the details of the changes to the disk pool without accepting them.

-mergedps merges the specified primary and secondary disk pools. Disk_pool_name_2 merges into "disk_pool_name_1" leaving only "disk_pool_name_1." Merge the specified primary and secondary disk pools.

-previewdv previews inventory changes to be made, but does not perform the inventory update.

-previewenclr lists the details of all enclosures (disk arrays) that any disk pool uses or may use.

-setconfig sets the configuration parameters for the disk pool.

-updatedp updates the disk pool replication properties with fresh values from the storage server. If the storage administrator changes replication properties of disk volumes on the storage server, the following occurs: This command forces NetBackup to update the disk pool properties to reflect the storage configuration.

-updatedv updates properties of one or more disk volumes in a pool.

-updatests updates the properties of the specified storage server.

The vmupdate command detects whether new tapes have been added to or removed from a robotic library. In the same way, the inventory and the preview options of nbdevconfig detect if the storage administrator has changed the composition of the disk pool. An inventory detects if new volumes were added, existing volumes were resized (added more space), or volumes were removed. The inventory operation can also accept new space. (For example, it updates the NetBackup database with the existence of new disk volumes or configures new volumes from the new space.)

OPTIONS

The following is a description of each of the nbdevconfig options:
-clearattribute attribute

Removes an attribute from the specified storage server or the specified disk pool for restore or duplication operations. It is used only with the -changests and -changedp options. You can specify more than one -clearattribute attribute on the command line. Refer to the -setattribute description for a list of attributes used by -changeests and a list used by -changedp.

-comment comment

Adds a comment for the disk pool. Quotation marks (" ") are required if the comment contains any spaces.

-config region:region-url

For Amazon cloud storage region support, specifies the region in which to create the bucket. Following are few examples. For complete list refer to the Amazon documentation:

- ap-northeast-1 Asia Pacific (Tokyo)
- ap-southeast-1 Asia Pacific (Singapore)
- ap-southeast-2 Asia Pacific (Sydney)
- eu-west-1 European Union (Ireland)
- sa-east-1 South America (Sao Paulo)
- us-west-1 US West (Northern California)
- us-west-2 US West (Oregon)

If the region-url string does not exactly match the notation, the bucket is created in the US Standard region. If this option is omitted, the bucket is created in the US Standard region.

**Note:** For Amazon virtual private cloud (VPC), this option is mandatory except for US-Standard region. If this option is omitted, bucket is not created and you will encounter an error.

-configlist filename

Captures the configuration parameter information and sends it to the specified file or to the appropriate disk pool.

-del_storage_servers storage_server...

Deletes the specified storage servers.
-dp disk_pool_name
   Specifies the name of the disk pool that \texttt{nbdevconfig} previews, inventories, or creates. The disk pool name cannot exceed 256 characters.

-dv disk_volume_name
   The name of the disk volume.
   For cloud storage, the characters that each vendor allows may vary. Also, the terminology for volumes may differ (for example, Amazon uses \textit{buckets} to describe volumes). Consult your cloud vendor documentation for naming conventions.

-dvlist filename
   The file name that contains a list of the disk volumes. Specify one volume only for cloud disk pools and media server deduplication pools.

-enclosure enclosure_name
   The unique name of the enclosure. When it is used with the \texttt{previewenclr} option, it displays details about the enclosure. This option runs successfully only if the vendor CLI is installed on the master server and its name in the disk array's host map.

   When it is used with the \texttt{importenclr} option, it creates the disk pool from the specified enclosure.

-exclude [Snapshot | Primary | Independent | ReplicationSource | ReplicationTarget | Mirror]
   Limits the command output to the disk volumes that are not capable of the specified target retention type (snapshot, primary, independent, mirror, replication source, or replication target).

   To exclude more than one flag, list the \texttt{-exclude} option more than once (for example, \texttt{-exclude primary -exclude ReplicationTarget}).

-force_targetslp_removal
   Forces the deletion of a disk pool that has an associated AIR target lifecycle policy when deletion of that disk pool results in an error. This option can be used only with the \texttt{-deletedp} operation.

-hwm high_watermark_percent
   The percentage of used capacity at which the storage (disk volume) is considered full. No new jobs can be assigned to the volume, and staging expiration operations can be triggered.
-include [Snapshot | Primary | Independent | ReplicationSource | ReplicationTarget | Mirror]

Limits the command output to the disk volumes that are capable of the specified target retention type (snapshot, primary, independent, mirror, replication source, or replication target).

To include more than one flag, list the modifier more than once (for example, -include Snapshot -include ReplicationTarget).

-l

Sets the list type to the short output. It produces parsable, raw output with all fields on one line with no headers. The first field indicates the version of the output as an aid to the script operation.

-lwm low_watermark_percent

The percentage of used capacity to which staging and expiration operations drain each volume in the disk pool upon reaching the high water mark.

-M master_server

The name of the master server.

-max_io_streams n

Limits the number of jobs that are allowed for each volume in the disk pool to the specified number n. This number is the sum of the jobs that read backup images and the jobs that write backup images. When the limit is reached, NetBackup chooses another available volume for write operations. If none is available, NetBackup queues jobs until a volume becomes available. Factors that affect the optimal number of streams include disk speed, CPU speed, and the amount of memory.

This parameter is not supported for BasicDisk. NetBackup does not limit the number of streams for BasicDisk storage units.

-media_server media_server

The media server that executes the operation.

-noverbose

Suppresses all stdout messages, including successful confirmation output such as "Disk pool disk_pool_name was successfully inventoried."

-reason "string"

Indicates the reason for performing this command action. The reason text string that you enter is captured and appears in the audit report. Enclose the string with double quotes ("...") and the string cannot exceed 512 characters. It cannot begin with a dash character (-) nor contain a single quotation mark (').
**-setattribute attribute**

Applies an attribute to the storage server or data pool for the read side of restore or duplication operations. It is used only with the `-changest` and `-changedp` options. The attributes help you manage the restore traffic and duplication traffic. You can specify more than one `-setattribute attribute` on the command line.

The following attributes are used with storage servers:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenStorage</td>
<td>managed as OpenStorage storage server</td>
</tr>
<tr>
<td>DiskGroups</td>
<td>aware of disk pools / enclosures</td>
</tr>
<tr>
<td>ActiveDiskGroups</td>
<td>allow active management of disk groups</td>
</tr>
<tr>
<td>ActiveServers</td>
<td>allow active management of storage srvrs</td>
</tr>
<tr>
<td>RovingVolumes</td>
<td>active mount/unmounts for disk volumes</td>
</tr>
<tr>
<td>CopyExtents</td>
<td>allow optimized duplication</td>
</tr>
<tr>
<td>AdminUp/Down</td>
<td>administrative state is UP/DOWN</td>
</tr>
<tr>
<td>InternalUp/Down</td>
<td>internal state is UP/DOWN</td>
</tr>
<tr>
<td>SpanImages</td>
<td>allow images to span disk volumes</td>
</tr>
<tr>
<td>BasicStaging</td>
<td>allow basic image staging</td>
</tr>
<tr>
<td>LifeCycle</td>
<td>allow image life cycle management</td>
</tr>
<tr>
<td>CapacityMgmt</td>
<td>allow capacity management</td>
</tr>
<tr>
<td>FragmentImages</td>
<td>allow image fragmentation</td>
</tr>
<tr>
<td>CatalogBackup</td>
<td>allow catalog backups</td>
</tr>
<tr>
<td>Cpr</td>
<td>allow checkpoint / restart</td>
</tr>
<tr>
<td>RandomWrites</td>
<td>allow random write access</td>
</tr>
<tr>
<td>FT-Transfer</td>
<td>allow access through FT channel</td>
</tr>
<tr>
<td>PrefRestore</td>
<td>preferred use for restores</td>
</tr>
<tr>
<td>ReqRestore</td>
<td>required use for restores</td>
</tr>
<tr>
<td>ReqDuplicate</td>
<td>required use for duplications</td>
</tr>
<tr>
<td>CapacityManagedRetention</td>
<td>allow capacity managed retention</td>
</tr>
<tr>
<td>CapacityManagedJobQueuing</td>
<td>allow capacity managed job queuing</td>
</tr>
<tr>
<td>OptimizedImage</td>
<td>allow virtual image construction</td>
</tr>
<tr>
<td>MetaData</td>
<td>describe client data during backup</td>
</tr>
<tr>
<td>QueueOnDown</td>
<td>queue jobs when server status is down</td>
</tr>
</tbody>
</table>

The following attributes are used with data pools:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patchwork</td>
<td>associated with enclosure</td>
</tr>
<tr>
<td>Visible</td>
<td>visible and managed through UI</td>
</tr>
<tr>
<td>OpenStorage</td>
<td>managed as OpenStorage disk pool</td>
</tr>
<tr>
<td>RovingVolumes</td>
<td>active mount/unmounts for disk volumes</td>
</tr>
<tr>
<td>SingleStorageServer</td>
<td>limited to single storage server</td>
</tr>
<tr>
<td>CopyExtents</td>
<td>allow optimized duplication</td>
</tr>
<tr>
<td>AdminUp/Down</td>
<td>administrative state is UP/DOWN</td>
</tr>
</tbody>
</table>
InternalUp/Down: internal state is UP/DOWN
SpanImages: allow images to span disk volumes
BasicStaging: allow basic image staging
LifeCycle: allow image life cycle management
CapacityMgmt: allow capacity management
FragmentImages: allow image fragmentation
CatalogBackup: allow catalog backups
Cpr: allow checkpoint / restart
RandomWrites: allow random write access
FT-Transfer: allow access through FT channel
CapacityManagedRetention: allow capacity managed retention
CapacityManagedJobQueuing: allow capacity managed job queuing
OptimizedImage: allow virtual image construction
MetaData: describe client data during backup
Snapshot: disk pool holds Snapshots
Primary: disk pool is capable of Snapshots from sources mounted on a client
ReplicationSource: disk pool can be a source for Image or Snapshot replication
ReplicationTarget: disk pool can be a target for Image or Snapshot replication
Mirror: this replication target disk pool can use a mirrored replication method
Independent: this replication target can use a non-mirrored replication method

The following are additional descriptions of attributes related to restore and duplication operations:

- **PrefRestore.** The storage server is preferred for the read side of restore operations. More than one storage server can have the `PrefRestore` attribute.

  The storage servers and data pools that are marked as `PrefRestore` are considered for use first. If none are available, any unmarked storage server is considered for use.

  Normal NetBackup load balancing occurs among all storage servers marked `PrefRestore`.

- **ReqRestore.** The storage server is required for the read side of restore operations. More than one storage server can have the `ReqRestore` attribute.

  If a `ReqRestore` server is not available, NetBackup considers `PrefRestore` servers for use. If none are available, jobs queue until a `ReqRestore` or `PrefRestore` is available.
If you configure **ReqRestore** servers but not **PrefRestore** servers, unmarked storage servers are never considered for restore jobs. Jobs are queued until a **ReqRestore** storage server is available to execute the job. Normal NetBackup rules for job retry apply. Normal NetBackup load balancing occurs for all storage servers marked **ReqRestore**. Load balancing does not occur between the **ReqRestore** and **PrefRestore** storage servers.

- **ReqDuplicate**. The storage server is required for the read side of duplication operations. More than one storage server can have the **ReqDuplicate** attribute. If any storage server is marked as **ReqDuplicate**, only the storage servers that are marked as **ReqRestore** are considered for use. If a **ReqRestore** server is unavailable, jobs queue until a **ReqRestore** server is available to execute the job. Normal NetBackup rules for job retry apply. **ReqDuplicate** also applies to storage server allocation for synthetic backup operations.

- **-st storage_type**
  
  The type of storage being used:
  
  1 -- Formatted disk (default) OR 2 -- Raw disk
  4 -- Direct attached OR 8 -- Network attached (default)

  The two values are added together. For example a **storage_type** of 10 indicates a raw disk (2) that is network attached (8).

- **-state UP | DOWN | RESET**
  
  Selects the state of the disk pool or disk volume. Specify UP to up the disk pool or disk volume and DOWN to down the disk pool or disk volume.

  The RESET option does the following:
  
  - Sets the internal state to UP (both disk volume and disk pool)
  - Sets committed_space to ZERO (disk volume only)
  - Sets the precommitted space to ZERO (disk volume only)

- **-storage_server storage_server**
  
  A single storage server. Interpretation differs depending upon one of the following options that are used with it:

  - previewdv: -**storage_server** restricts the output to arrays that are connected to the specified servers. All of the hosts must be connected to all storage (LUNs) within the disk volume.
- creatests: -storage_server identifies the host name of the storage server. The storage server name cannot exceed 128 characters and cannot contain colon (:) characters.

- setconfig: -storage_server identifies the storage server that contains the disk pool whose configuration parameters you have set. The storage server name cannot exceed 128 characters.

-storage_servers storage_servers...
The list of storage server names for creating a disk pool. Separate the items in this list with spaces, not commas.

-stype server_type
  Specifies a string that identifies the storage server type. The server_type value can originate from one of the following sources:
  - Veritas provided storage. Possible values are AdvancedDisk and PureDisk.
  - Third-party disk appliances. The vendor supplies the server_type string.
  - Cloud storage. Use the csconfig cltprovider -l command to determine the possible stype values. The cloud stype values reflect the cloud storage provider. Cloud storage stype values can also incorporate a suffix (for example, amazon_crypt). Possible suffixes are:
    - _raw: The NetBackup backup image is sent to the cloud in raw format. Use this option if you do not want to compress or encrypt data before sending to cloud storage.
    - _rawc: Compresses the data before it is written to the cloud storage.
    - _crypt: Encrypt the data using AES-256 encryption before writing the data to cloud storage. You must have KMS configured in NetBackup to use this option.
    - _cryptc: Compress and encrypt the data before writing to cloud storage.
  - Replication Director OpenStorage partners. Possible values are Network_NTAP, Network_NTAP_CDOT, or EMC_Celerra.

The storage server type is case sensitive.

-U
Lists the configuration attributes in a user-readable, formatted listing with one attribute per line and more attributes than a listing in raw output mode (-l). See Example 1.
EXAMPLES

Example 1 - Preview all enclosures that the storage servers see and display in user readable mode.

```
# nbdevconfig -previewenclr -U -storage_servers daloa -M daloa
Preview of Enclosure imported_dp as Disk pool
  Disk Pool Name : imported_dp
  Disk Pool Id   : imported_dp
  Disk Type      : AdvancedDisk
  Availability   : Free
  Raw Size (GB)  : 1.20
  Usable Size (GB): 1.20
  Num Volumes    : 3
  Storage Server : daloa.example.com
```

Example 2 - Delete a disk pool. First expire all images on the disk group.

```
# nbdevconfig -deletedp -dp Disk-Pool-2
Disk pool Disk-Pool-2 has been deleted successfully
```

Example 3 - Mark a Media Server Deduplication Pool as DOWN.

```
# nbdevconfig -changestate -stype PureDisk -dp diskpool_alpha -state DOWN
```

Example 4 - Mark a disk volume as UP.

```
# nbdevconfig -changestate -stype AdvancedDisk -dp diskpool_alpha -dv alpha_vol1 -state UP
```

Example 5 - Inventory a disk group.

```
# nbdevconfig -inventorydp -preview -stype AdvancedDisk -dp Disk-Pool-2
Old Raw Size (GB): 97.85
New Raw Size (GB): 103.45

Old Formatted Size (GB): 97.80
New Formatted Size (GB): 103.40

Old Host List: willow,Pear,dunamo
New Host List: Dellco,carrot,Pear,dynamo

Affected Storage Units
------------------------
SSO-STU-7 - willow [...] would be removed from media server list
SSO-STU-9 - willow [...] would be removed from media server list, \ switch to "any available" media server list.

Affected Storage Units
------------------------
SSO-STU-7 - willow [...] was removed from media server list
SSO-STU-9 - willow [...] was removed from media server list, \ switch to "any available" media server list.

SEE ALSO

See nbdevquery on page 663.
See vmupdate on page 982.
nbdevquery

nbdevquery – display NetBackup disk media status

SYNOPSIS

nbdevquery -listconfig [-l | -U] -stype server_type -storage_server storage_server [-EMM emm_server]


nbdevquery -listdv [-l | -U | -D] -stype server_type [-dp disk_pool_name [-dvlist file]] [-M master_server] [-EMM emm_server]

nbdevquery -listglobals

nbdevquery -listmediaid id [id...][ [-l | -U] [-EMM emm_server]

nbdevquery -listmounts [-l | -U] [-stype server_type] [-dp disk_pool_name] [-M master_server] [-EMM emm_server]

nbdevquery -listreptargets -stunit label[-U] [[-include Primary | ReplicationSource | Mirror]...] [[-exclude Primary | ReplicationSource | Mirror]...]

nbdevquery -liststs [-l | -U] [-stype server_type] [-storage_server storage_server] [-EMM emm_server]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\

DESCRIPTION

The nbdevquery command line utility is the disk equivalent of bpmedialist for tape. The following are the operations that nbdevquery performs:

- -listdp lists all disk pools in the system.
- -liststs lists all storage servers in the system.
-listdv displays status for disk volumes of imported disk pools. It includes such things as whether the volume is online or offline and the number of current readers (or writers) to the volume.

When you use the -listdv command with the -D option, nbdevquery returns a large set of data including the following values that NetBackup uses to determine the available free space within the disk pool:

- **total_capacity**: The total size of the disk as derived from the file system.
- **free_space**: The amount of free space on the disk as derived from the file system.
- **potential_free_space**: The total size of all fragments on the disk that have been duplicated as part of a storage lifecycle policy and are eligible for expiration. The potential_free_space value is computed after duplication and expiration sessions. This information is applicable only when capacity managed retention is used for a storage destination.
- **committed_space**: The amount of data that NetBackup estimates as being written to the disk, based on all in-progress backups.
- **precommitted_space**: A helper value for committed_space. This value is decreased as a backup job proceeds and the total_capacity and free_space information is updated.

NetBackup uses free_space, potential_free_space, and committed_space to determine how much space is available on a disk. It uses the following formula:

\[
\text{available space} = \text{free space} + \text{potential free space} - \text{committed space}
\]

- **-listmediaid** lists all disk volumes that have been given a disk media ID.
- **-listmounts** lists the disk mount points for the disk pool.
- **-listconfig** lists storage server configuration details.
- **-listglobals** lists all global disk attributes.
- **-listreptargets** lists valid replication target storage units or groups for a specified source storage unit or storage unit group. You can list the set of storage units to configure as targets for storage lifecycle policy replication operations.

**OPTIONS**

- **-D**

  Sets the list type to dump debug data. This option dumps information without further processing. The output format and displayed fields are subject to change without notification.
-dp disk_pool_name
  Specifies the name of the disk pool to be queried. This pool is the data storage area for this storage unit.

-dv disk_volume
  Displays the status for only the specified disk volume. For BasicDisk, the input value is the path. In all other cases, the input value is the volume name.

-dvlist filename
  Specifies the file that contains the volume information.

-include | -exclude [ Primary | ReplicationSource | Mirror ]...
  Includes or filters out targets if multiple choices exist.

-l
  Sets the list type to short output. This option produces parsable output with all fields on one line, no headers. The first field indicates the version of the output as an aid to the script operation. Date and time values appear in UNIX long format; status values appear in integer form.

-listconfig
  Lists the storage server configuration details.

-listdp
  Lists all imported disk pools in the NetBackup database. For an OpenStorage disk, -listdp lists all the disk pools that have been configured.

  **Note:** The following properties do not apply to cloud storage disk pools: Raw Size, Usable Size, High Watermark, and Low Watermark.

  You can view the disk pool properties by using the -U option of the listdp command.

-listdv
  Lists the status for all disk volumes of imported disk pools and returns a list of all disk volumes in the NetBackup database. See Example 3.

-listglobals
  Lists all NetBackup Disk Service Manager global disk attributes. If SPR is enabled, the SCSI Persistent Reservation setting is set to one (1). If LUN masking is enabled, the output shows zero (0) rather than 1.

-listmediaid id...
  Lists all disk volumes that have been given the specified disk media IDs.

-listmounts
  Lists the disk mount points for the disk pool.
-listreptargets
Lists valid replication target storage units or groups for a source storage unit or storage unit group.

-liststs
Lists all servers that host storage. These include Veritas provided storage such as Media Server Deduplication Pool, third-party appliances, and cloud storage.

-storage_server storage_server
The host name of the storage server. The name was given to the storage server when it was created.

-stype server_type
Specifies a string that identifies the storage server type. The server_type value can originate from one of the following sources:

- Veritas provided storage. Possible values are AdvancedDisk and PureDisk.
- Third-party disk appliances. The vendor supplies the server_type string.
- Cloud storage. Use the csconfig cldprovider -1 command to determine the possible stype values. The cloud stype values reflect the cloud storage provider. Cloud storage stype values can also incorporate a suffix (for example, amazon_crypt). Possible suffixes are:
  - _raw: The NetBackup backup image is sent to the cloud in raw format. Use this option if you do not want to compress or encrypt data before sending to cloud storage.
  - _rawc: Compresses the data before it is written to the cloud storage.
  - _crypt: Encrypt the data using AES-256 encryption before writing the data to cloud storage. You must have KMS configured in NetBackup to use this option.
  - _cryptc: Compress and encrypt the data before writing to cloud storage.

The storage server type is case sensitive.

-U
Lists the configuration information about the specified disk pool, storage server, or disk storage (see Example 1). Some of the items cannot be changed.

EXAMPLES

Example 1 - List in user format the configuration information about all servers that host storage in the system.
# nbdevquery -liststs -stype Network_NTAP -U
Storage Server : plinko
Storage Server Type : Network_NTAP
Storage Type : Formatted Disk, Direct Attached
State : UP
Flag : OpenStorage
Flag : AdminUp
Flag : InternalUp
Flag : LifeCycle
Flag : CapacityMgmt
Flag : FragmentImages
Flag : Cpr
Flag : RandomWrites
Flag : FT-Transfer
Flag : PrimaryEnabled
Flag : SnapShotEnabled
Flag : MirrorEnabled
Flag : WORM

Example 2 - View all disk pool information for djs_bp in user format. Volume SnapVaultB is a valid source volume for replication because it is a replication source and it has a target parameter, ntpdfm:SnapMirrorA1.

nbdevquery -listdp -stype DjsArray -U
Disk Pool Name : djs_bp
Disk Type : DjsArray
Disk Volume Name : SnapVaultB
Disk Media ID : @aaaa
Total Capacity (GB) : 68.21
Free Space (GB) : 55.93
Use% : 88
Status : UP
Flag : ReadOnWrite
Flag : AdminUp
Flag : InternalUp
Flag : ReplicationSource
Flag : ReplicationTarget
Flag : Primary
Flag : Snapshot
Flag : WORMCapable
Num Repl Sources : 1
Num Repl Targets : 1
Replication Source : ntpdfm:@aaaa@:PrimarySnapshot
Replication Target : ntpdfm:SnapMirrorA1
Example 3 - Do a disk drive dump of the disk pool sim_dp1 that PureDisk uses.

```
# nbdevquery -listdp -dp sim_dp1 -stype PureDisk -D
Disk Drive Dump
  name : <sim_dgl>
  id : <sim_dgl>
  server_type : <PureDisk>
  master_server : <daloa.example.com>
  access_media_server : <>
  disk_storage_type : 6
  total_capacity : 1286602752
  used_space : 0
  sts_state : 0
  availability : 2
  connectivity : 0
  high_watermark : 98
  low_watermark : 80
  num_diskvolumes : 3
  num_disks : 0
  num_stservers : 2
  system_tag : <Imported from STS>
  user_tag : <>
Storage Server [0]
  name : <daloa.example.com>
  id : <>
  server_type : <PureDisk>
  storage_type : 6
  access_media_serv. : <>
Storage Server [1]
  name : <blackjack.example.com>
  id : <>
  server_type : <PureDisk>
  storage_type : 6
  access_media_serv. : <>
```

SEE ALSO

See nbemmcmd on page 678.
See nbdevconfig on page 650.
nbdiscover

nbdiscover — test query rules for automatic selection of VMware virtual machines for backup

SYNOPSIS

nbdiscover -noxmloutput path | -policy policy_name [-sched policy_schedule_type] [-includedonly | -excludedonly] [-noreason] [-escapechar x] [-quotechar x]

nbdiscover -noxmloutput query [-includedonly | -excludedonly] [-noreason] [-escapechar x] [-quotechar x]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\

DESCRIPTION

The nbdiscover command is similar to the Test Query button in the VMware policy. It returns the virtual machines that NetBackup selects based on the specified query rules. You can specify the name of a policy that contains the query, or the query itself. The -noxmloutput option is required for user-friendly output (the default XML output is not supported for general use).

The nbdiscover command must be run on either the discovery host or the backup host.

For more information on how to create and test rules from the policy's Query Builder, see the NetBackup for VMware Administrator's Guide.

OPTIONS

-escapechar x
   Specifies the ASCII decimal value of an alternate escape character to be used in the nbdiscover output when you use the -noxmloutput option. The default escape character is a backslash (\) or -escapechar 92.

-excludedonly x
   Returns only excluded virtual machines that do not match the rules in the query.
-includedonly x
    Returns only included virtual machines that match the rules in the query.

-noreason
    Omits from the results any explanation as to why a virtual machine was excluded by the query or failed the query. A virtual machine fails the query if the query cannot exclude the virtual machine and the virtual machine cannot be selected for backup.

-noxmloutput
    Displays one virtual machine per line. In the output, a plus sign (+) in the first column indicates that the virtual machine matches the rules in the query. A minus sign (-) indicates that the virtual machine does not match the rules in the query.

-policy policy_name
    Specifies a policy that contains a query. nbdiscover filters the virtual machines based on that query and on other policy attributes, such as Primary VM identifier (for example, VM host name or VM display name).

query
    Specifies a query without a policy. You must compose the query manually and enclose it in double quotes. For example:

    "vmware:/?filter=Displayname Contains 'vm1'"

-quotechar x
    Specifies the ASCII decimal value of an alternate quote character to be used in the nbdiscover output when you use the -noxmloutput option. The default quote character is a double quote (") or -quotechar 34.

-sched policy_schedule_type
    Specifies the schedule type of the policy when you use the -policy policy_name option.

**EXAMPLES**

Example 1 - List the virtual machines that either match or do not match the query in the policy pol1. Do not list explanations for the virtual machines that failed the query or that the query excluded.

    # nbdiscover -noxmloutput -policy pol1 -noreason
    + "grayvm3"
    + "grayvm5"
    + "grayvm7"
Example 2 - List the virtual machines that have display names that contain “vm”. Do not list virtual machines that do not have “vm” in the display names:

```
# nbdiscover -noxmloutput -includedonly "vmware://?filter=Displayname Contains 'vm'"
grayvm3
grayvm5
grayvm7
vladvm1
vladvm2
bodvm23
```

Example 3 - List the virtual machines by whether they are turned on.

```
# nbdiscover -noxmloutput "vmware://?filter=Powerstate Equal poweredOn"
+ "grayvm3"
+ "grayvm5"
+ "grayvm7"
- "vladvm1" "VM excluded by discovery filter, display name=[vladvm1], server=esx1.acme.com]."
+ "vladvm2"
+ "bodvm23"
+ "bittle4"
```

Example 4 - List the virtual machines by whether they are turned on and have "7" in their display name. Do not list explanations for the virtual machines that failed the query or that the query excluded.

```
# nbdiscover -noxmloutput "vmware://?filter=Powerstate Equal poweredOn / AND Displayname Contains '7'" -noreason
- "grayvm3"
- "grayvm5"
+ "grayvm7"
- "vladvm1"
- "vladvm2"
- "bodvm23"
- "bittle4"
```
Example 5 - Search all VM backups that have "test" in their vCloud vApp name. This example uses a query to search virtual machines in vCloud Director. nbdiscover must be run on the master server.

```
# nbdiscover -noxmloutput "vmsearch:/;reqType=search?filter=vCDvApp Contains 'test'
+ "demovm%20(8c879791-2917-4428-8213-bea7ec727717)"
+ "small_vm%20(61e85579-7246-411f-b2f9-9fb570546755)"
+ "small_vm_percent_%25%20(61e85579-7246-411f-b2f9-9fb570546755)"
```

Example 6 - Show the hierarchy of the vCloud environment that was backed up. The output of this command is in XML. This example uses a query to search virtual machines in vCloud Director. nbdiscover must be run on the master server.

```
# nbdiscover "vmsearch:/;reqType=browse;viewType=vcloud"
<?xml version="1.0" encoding="utf-8"?>
<Start Iteration="vmsearch:/;reqType=browse;viewType=vcloud">
  <VCDSERVER>
    <NBU>
      <NAME>hypervm1.acme.com</NAME>
    </NBU>
  </VCDSERVER>
  <VCDORG>
    <NBU>
      <NAME>Test_vCloud</NAME>
    </NBU>
    <VCDORGVDC>
      <NBU>
        <NAME>TestOrg</NAME>
      </NBU>
      <VCDVAPP>
        <NBU>
          <NAME>TestvApp</NAME>
        </NBU>
      </VCDVAPP>
    </VCDORGVDC>
  </VCDORG>
  <VCDSERVER>
    <StatusMsg NBUStatus="0" Severity="0"></StatusMsg>
  </VCDSERVER>
</Start>
```
nbdna

nbdna – run the utility that analyzes the NetBackup domain and its configuration

SYNOPSIS


On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/support

On Windows systems, the directory path to this command is install_path\NetBackup\bin\support

DESCRIPTION

The NetBackup Domain Network Analyzer (nbdna) command utility analyzes the NetBackup domain and its configuration for network issues, performance, and behavior. It addresses the host name lookup and connectivity between NetBackup hosts and their role within the NetBackup domain.

nbdna does the following:

■ Discovers and maps the NetBackup domain
■ Extracts the host name memberships by querying the configuration
■ Evaluates the host name lookup and the socket connectivity to these host names to validate their network relationship status according to their domain configuration

nbdna can be run on a NetBackup master server, media server, or client. It creates and identifies a compress archive that contains all generated reports. You can return the compress archive to Veritas upon request.

You must have administrator privileges to run this command.

Note: In the NBAC environment, authenticate before you execute the nbdna command.
OPTIONS

-discover
Performs host discovery on the NetBackup environment for the hosts in the host list that the -f option specifies.

Note: This option does not discover any other hosts in the NetBackup environment, but limits its discovery to only the hosts in the host list that -f specifies.

-discover must be used with the -f option and the -listonly option.

-dump
Does not run the test, but dumps server, client, and lookup test list to the specified file.

-f=hostlist
Reads the host names from the specified ASCII text file and adds them to the test lists. The format of the text file is the following:

SERVER hostname
CLIENT hostname-b
LOOKUP hostname-c

Lines that begin with SERVER are imported to the server test list.
Lines that begin with CLIENT are imported to the client test list.
Lines that begin with LOOKUP are imported to the lookup-only test list.

-imfile=bpimmage.out
Reads the host names from a file that contains the output from either the bpimagelist -l command or the bplmedia -l command.

-listonly
Runs the network tests only for the hosts in the host list that the -f option specifies. It does not search the NetBackup environment for other host names.

Note: This option does not discover the location of these hosts, nor does it analyze the NetBackup configuration for other hosts. To discover the listed hosts, include the -discover option.

-lookup
Runs the name lookup test only. This option cannot be run with the -server option.
-odir=override_output_directory

Overrides the output directory with the specified directory.

The default directory is the following:

- For UNIX:
  
  `/usr/openv/netbackup/bin/support/output/nbdna/YYYYMMDD.HHMMSS/

- For Windows:
  
  `install_path\NetBackup\bin\support\output\nbdna\YYYYMMDD.HHMMSS`

If the NetBackup path cannot be found, the default is changed to the same directory as the `nbdna` binary.

-phase= pn

Specifies the number (`pn`) of the test phase to be run.

The possible values of `pn` are the following:

- 0 - Phase 0 runs the name lookup test and the socket connection test. Phase 0 is the default mode.
- 1 - Phase 1 tests include phase 0 tests plus the basic NetBackup service test for the SERVER list.
- 2 - Phase 2 tests include phase 0 tests plus the basic NetBackup service test for the SERVER list and the CLIENT list.

-server

Runs the server test only. This option cannot be run with the -lookup option.

-sfo

Produces script friendly reports.

-temp=override_tmp_directory

Overrides the temporary directory. The default condition is the system temp directory.

-verbose

Displays progress to the standard out (on-screen). The same information is captured to the progress-trace log regardless of this switch. You do not need to capture verbose output to a file.

-version

Displays the version information then exits the utility.

FILES

`nbdna` creates up to five files:
The last three files that are listed are generated only if there are errors.

EXAMPLES

Example 1 - In this UNIX example, nbdna runs with report files written to an alternate directory:

```
# nbdna -odir=/user/home/winter/
```

Example 2 - Run nbdna with verbose output. It imports a host name list file (hostnames.txt) and evaluates only those hosts:

```
# nbdna -verbose -f=hostnames.txt -listonly
```

The host name file format is as follows:

```
SERVER dellpe2400
CLIENT 10.12.249.20
LOOKUP 10.82.108.136
```

SEE ALSO

See nbsu on page 867.

See nbcplogs on page 606.
nbemm

nbemm – run the NetBackup EMM daemon to manage volumes, volume pools, barcode rules, and devices

SYNOPSIS

nbemm [-console] [-terminate]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\

DESCRIPTION

The Enterprise Media Manager daemon or service manages volumes, volume pools, barcode rules, and devices. This daemon performs media, drive, drive path, and storage unit selection.

**Note:** The `nbemm` daemon or service must be active to change the volume configuration, device configuration, storage unit configuration, and for any tape mount activity.

To start `nbemm`, enter `nbemm`.

To stop `nbemm`, enter `nbemm -terminate`.

OPTIONS

- **-console**
  This option enables you to start NetBackup in console mode.

- **-terminate**
  This option enables you to stop the `nbemm` binary.

SEE ALSO

See `nbemmcmd` on page 678.
nbemmcmd – update and view information in the EMM database

SYNOPSIS

nbemmcmd [-addhost] [-changesetting] [-deletehost] [-errorsdb]
[-machinealias] [-renamehost] [-resethost] [-servercontrol]
[-setemmserver] [-updatehost]

nbemmcmd -addhost [-activenodename string] [-brief] [-clustername
string] [-displayname string] [-machinedescription string]
-machinename string -machinetype api | app_cluster | cluster | master
| media | ndmp [-masterserver string] [-netbackupversion
level[major_level[minor_level]]] [-operatingsystem hpux | linux |
rs6000 | solaris | windows] [-scanability unsigned_integer]

nbemmcmd -changesetting -machinename string
[-ALLOW_MULTIPLE_RETENTIONS_PER_MEDIA 0|1|no|yes] [-AUDIT DISABLED
| ENABLED] [-AUDIT_RETENTION_PERIOD number_of_days]
[-COMMON_SERVER_FOR_DUP default | preferred | required]
[-DISABLE_AUTOMATIC_HOST_NAME_ADD 0|1|no|yes]
[-DISABLE_BACKUPS_SPANNING_DISK 0|1|no|yes]
[-DISABLE_DISK_STU_JOB_THROTTLING 0|1|no|yes]
[-DISABLE_STANDALONE_DRIVE_EXTENSIONS 0|1|no|yes]
[-DISALLOW_NONNDMP_ON_NDMP_DRIVE 0|1|no|yes] [-DO_NOT_EJECT_STANDALONE
0|1|no|yes] [-DON'T_USE_SLAVE 0|1|no|yes] [-DRIVE_ERROR_THRESHOLD
unsigned_integer] [-DRIVE_NAME_SEED 0|1|no|yes] [-emmmname string]
[-emmmport unsigned_integer] [-MAX_REALLOC_TRIES unsigned_integer]
[-MEDIA_ERROR_THRESHOLD unsigned_integer] [-MEDIA_REQUEST_DELAY
unsigned_integer] [-MPMS_DISABLE_EVENTS 0|1|no|yes]
[-MPMS_DISABLE_RANK unsigned_integer] [-MUST_USE_LOCAL_DRIVE
0|1|no|yes] [-NBUFS_DESTINATION_DSU string] [-NBUFS_DUP_TSU_TO_DSU
0|1|no|yes] [-NBUFS_RETENTION_LEVEL unsigned_integer]
[-NON_ROBOTIC_MEDIA_ID_PREFIX string] [-PREFER_NDMP_PATH_FOR_RESTORE
0|1|no|yes] [-RETURN_UNASSIGNED_MEDIA_TO_SCRATCH_POOL 0|1|no|yes]
[-SCSI_PROTECTION NONE | SPR | SR] [-SHAREDISK_MOUNT_POINT string]
[-TIME_WINDOW unsigned_integer] [-UNRESTRICTED_SHARING 0|1|no|yes]
[-USE_POTENTIAL_FREESPACE_FOR_ALLOCATION 0|1|no|yes]
[-VALIDATE_HOST_NAME 0|1|no|yes] [-VAULT_CLEAR_MEDIA_DESC 0|1|no|yes]
nbemmcmd -deletealldevices [-allrecords] | [-machinename string] | [-machinetype api | app_cluster | appliance | client | cluster | disk_array | foreign_media | master | media | nbwss_endpoint | ndmp | remote_master | replication_host | virtual_machine] [-emmname string] [-emmport unsigned integer]

nbemmcmd -deletehost [-brief] -machinename string -machinetype api | app_cluster | cluster | master | media | ndmp | master | media | ndmp-mediaid string

nbemmcmd -errorsdb [-brief] [-prune [-days no_of_days] [-hours no_of_hours] [-minutes no_of_minutes]]

nbemmcmd -getemmserver [-masterserver string] [-timeout unsigned_integer]


nbemmcmd -listsettings -machinename string [-brief] [-emmname string] [-emmport unsigned_integer]


nbemmcmd -releasecache -machinename string [-brief] [-emmname string] [-emmport unsigned_integer]

nbemmcmd -renamehost [-brief] -machinename string -machinetype api | app_cluster | cluster | master | media | ndmp -newmachinename string

nbemmcmd -resethost -machinename string

nbemmcmd -servercontrol [-brief] [-resume] [-suspend]
The `nbemmcmd` command enables users to update a limited set of EMM database information. In addition, this command enables you to manage host entries, configuration options, and other miscellaneous items in the EMM database.

**OPTIONS**

The following commands contain a variety of options that enable you to manage the EMM database. The names of the options are purposely long to provide the user with a better understanding of how the options are to be used. Because of the option name length, you need only type the first letter or letters of the command that make it a unique option. For example, to use the `-changesetting` option, type `-c` because no other command option starts with the letter `c`.

**-addhost**

This option adds the specified host to the EMM database. The following entries can be adjusted by using this command option:

`-activenodename string`

 Identifies the active node in a cluster.
-brief
   Makes the output of the command less verbose.

-clustername string
   Identifies the cluster to which this computer belongs.

-displayname string
   Sets the display name of the computer.

-machinedescription string
   Describes the computer or system being used.

-machinename string
   Specifies the name of the computer to be updated.

-machinetype api | app_cluster | cluster | master | media | ndmp
   Defines how the computer is used.

-masterserver string
   Defines the host master server in a particular domain.

-netbackupversion level[major_level[minor_level]]
   Specifies the version that the added host is running. The level variable
   has a range of 0-99. The major_level and minor_level variables are optional
   single-digit fields. No spaces are allowed between the major_level and
   minor_level variables.

   For example, enter the following information to specify NetBackup 7.0:
   
   -netbackupversion 7.0 or -netbackupversion 7

-operatingsystem hpux | linux | rs6000 | solaris | windows
   Adds a host with a designated operating system.

-scanability unsigned_integer
   This option applies only to NetBackup Enterprise Servers that use the
   Shared Storage Option (SSO) feature.

   A scan ability factor can range from zero to 9, with a default value of 5.
   This factor allows the assignment of scan hosts to be prioritized if a drive's
   scan host changes. Scan hosts with higher scan ability factors are chosen
   first.
Caution: A drive is unavailable for use until a scan host can be assigned to it. If all hosts that register for a particular drive use \textit{scan\_factor} = 0, the drive is unusable. The drive remains unusable until a host with a non-zero \textit{scan\_factor} registers for the drive. If all hosts with a non-zero \textit{scan\_factor} have the drive DOWN, then again the drive becomes unavailable.

The decision to use a \textit{scan\_factor} of zero for a server reduces the level of resiliency in your SSO configuration. Be aware of the servers that can be a scan host for a drive. If a drive loses a scan host, it makes the drive unavailable to any server.

\textbf{-changesetting \ -machinename \ \textit{string}}

Changes the configuration setting for a specified host and adds the settings that did not previously exist.

To change these configuration options, use \textbf{-changesetting} with the option name and the enable designator (1 or yes) or the disable designator (0 or no). For example, the following command disables the ability of EMM to add a host name automatically:

```
# nbemmcmd -changesetting -DISABLE_AUTOMATIC_HOST_NAME_ADD no
```

\textbf{-ALLOW_MULTIPLE_RETENTIONS_PER_MEDIA \ 0 \ | \ 1 \ | \ no \ | \ yes}

Allows NetBackup to mix retention levels on media. The default condition is that each volume can contain backups of only a single retention level.

\textbf{-AUDIT \ [DISABLED \ | \ ENABLED]}

Enables and disables NetBackup auditing. An audit trail is a record of user-initiated actions in a NetBackup environment. Auditing gathers and records the information to help answer who changed what and when they changed it. The default condition is audit enabled.

\textbf{-AUDIT\_RETENTION\_PERIOD \ \textit{number\_of\_days}}

Specifies the number of days that user actions are to be retained for the audit report. If no retention period is indicated, the default audit retention period is 90 days. A value of 0 (zero) indicates that the records are never purged.

\textbf{-COMMON\_SERVER\_FOR\_DUP \ default \ | \ preferred \ | \ required}

Determines how NetBackup finds the desired media server(s) to duplicate the data.

The media server that is used to read the image is the 'read media server'. The media server that is used to write the image is the 'write media server'.

By default, when the source image is on a tape device, the read media...
server is the one that writes the backup image. Also, when the source image is on a disk pool with multiple media servers, any of those media servers can be the read media server. The choice for the write media server is limited to those that have access to the storage unit or storage unit group specified as the destination of the duplication operation.

The following are the possible settings of this option:

- **Default.** NetBackup does not perform an exhaustive search for possible common servers (same read and write media server). If the common media servers are busy or unavailable, NetBackup uses a different write media server than the read media server. Use this option when you don’t want an exhaustive search to affect the performance of the Resource Broker. This scenario can occur when a large job queue with duplication jobs waits for resources to become available.

- **Preferred.** Look for a common media server to use. If one or more common media servers are found, but their resources (for example, DSUs or tape drives) are busy, do the following: Run the duplication job anyway by using two separate media servers (sending images over the network).

- **Required.** NetBackup makes an exhaustive search to find a common server. If the common media servers are busy, NetBackup queues the resource request and waits for the resources to become available. NetBackup runs the job with two separate media servers, sending the images over the network, if the following is true: No common servers are in the NetBackup domain, or if a common server exists but is down.

- **DISABLE_AUTOMATIC_HOST_NAME_ADD 0|1|no|yes**
  Disables the ability of EMM to add a host name automatically if it appears to be valid. An example of an invalid host name is a name that duplicates another host.

- **DISABLE_BACKUPS_SPANNING_DISK 0|1|no|yes**
  Disables the ability of a backup operation to disk to continue when a file system full condition occurs on a disk storage unit volume. It disables by using image fragments on multiple storage unit volumes.

- **DISABLE_DISK_STU_JOB_THROTTLING 0|1|no|yes**
  Disables the disk storage unit job throttle action that occurs when disk storage units approach their high-water mark. Disk storage unit throttling limits the number of jobs that are started simultaneously to approach the high-water mark more accurately. Default: Throttle disk storage units that approach their high-water mark.
-DISABLE_STANDALONE_DRIVE_EXTENSIONS 0|1|no|yes
Disables the non-robotic drive operations. During a backup, NetBackup
does not automatically try to use whatever labeled or unlabeled media it
finds in a non-robotic drive. Default condition is that standalone drive
extensions are enabled.

-DISALLOW_NONNDMP_ON_NDMP_DRIVE 0|1|no|yes
The MDS logic on the EMM server reads this option. NetBackup tries to
use an available drive that is based on the type of request as follows:
For a non-NDMP request of any kind, NetBackup tries to find an available
non-NDMP drive. If a non-NDMP drive is not available and an NDMP drive
is available, the slower NDMP drive is used. Non-NDMP requests include
all type of requests apart from storage unit-related requests (backups and
write side of duplicates) and NDMP image restores.

-DO_NOT_EJECT_STANDALONE 0|1|no|yes
If this entry is enabled, tapes in standalone drives are not ejected when a
backup has completed on that host. (Tapes are ejected if end-of-media is
reached during a backup.) Use when you want to keep a standalone drive
ready after successful backups are performed.

-DONT_USE_SLAVE 0|1|no|yes
Deselects the use of drive name rules to assign names to drives
automatically.

-DRIVE_ERROR_THRESHOLD unsigned_integer
Changes the threshold or number of drive errors that can occur before
NetBackup changes the drive state to DOWN. Default: 2.

-DRIVE_NAME_SEED 0|1|no|yes
Selects the use of drive name rules to assign names to drives
automatically.

-emmname string
Specifies the name of the EMM database server. This server contains the
database that stores the media information and device configuration
information.

-emmport unsigned_integer
Specifies the EMM port.

-machinename string
Names the computer whose settings are changed.
-MAX_REALLOC_TRIES unsigned_integer
   Specifies the maximum number of tries that NetBackup attempts to
   reallocate the media for future backups.

-MEDIA_ERROR_THRESHOLD unsigned_integer
   Changes the threshold or number of media errors that can occur before
   the media is frozen. Default: 2.

-MEDIA_REQUEST_DELAY unsigned_integer
   Specifies the number of seconds that NetBackup waits for a drive to
   become ready. Applies only to non-robotic drives. Default: 0 seconds. For
   example, assume that the delay is 150 seconds:

      MEDIA_REQUEST_DELAY = 150

   Add this information to the bp.conf file on NetBackup servers or enter a
   value for Media Request Delay in the Media host properties.

-MPMS_DISABLE_EVENTS 0|1|no|yes, -MPMS_DISABLE_RANK 0|1|no|yes,
- MUST_USE_LOCAL_DRIVE 0|1|no|yes
   If the client is also a master server and this option is active, backups for
   this client must occur on a local drive. If the client is not a master server,
   this entry has no effect.

   Add this option to the bp.conf file on master servers. Or check the Must
   Use Local Drive setting in the General Server host properties dialog box.

-NBUFS_DESTINATION_DSU string, -NBUFS_DUP_TSU_TO_DSU 0|1|no|yes,
- NBUFS_RETENTION_LEVEL unsigned_integer,
- NON_ROBOTIC_MEDIA_ID_PREFIX string
   Specifies the media ID prefix that is used for creating non-robotic media.
   It applies to the host that the -machinename option specifies. The media
   ID prefix is an alphanumeric string of characters from one to three
   characters in length.

-PREFER_NDMP_PATH_FOR_RESTORE 0|1|no|yes (default value is 1 or
no)
   Used to specify how NetBackup selects drives for NDMP restores. By
   default, NetBackup selects drives in the order shown:

   - NetBackup looks for an NDMP tape server that is local to the NDMP
     file system set to receive the restore data.
   - NetBackup looks for any NDMP tape server, including those that are
     not local to the restore client.
   - NetBackup looks for any NetBackup media server to act as an NDMP
     tape server.
If you specify `-PREFER_NDMP_PATH_FOR_RESTORE 0` or `-PREFER_NDMP_PATH_FOR_RESTORE yes`, the order NetBackup uses is:

- NetBackup looks for an NDMP tape server that is local to the NDMP file system set to receive the restore data.
- NetBackup looks for any NetBackup media server to act as an NDMP tape server.
- NetBackup looks for any NDMP tape server, including those that are not local to the restore client.

```bash
-RETURN_UNASSIGNED_MEDIA_TO_SCRATCH_POOL 0|1|no|yes
```

This EMM global option applies to every host that uses the EMM server. It is not a host option.

YES: The Media Manager automatically returns the expired and unassigned media that originated in the scratch volume pool to the scratch volume pool.

NO: Disables the automatic behavior of returning media to the scratch pool. Use one of the Media Manager administration interfaces to move media.

```bash
-SCSI_PROTECTION NONE | SPR | SR
```

Allows the exclusive access protection for tape drives. With access protection, other host bus adaptors cannot issue commands to control the drives during the reservation. The three possible settings for this option are:

- NONE - No protection
- SPR - SCSI persistent reserve
- SR - SPC-2 SCSI reserve (default condition)

```bash
-TIME_WINDOW unsigned_integer
```

Enables you to set a value that is equal to the amount of time in which errors can be tracked. You can use this value with an error threshold (for example, `media_error_threshold`) to monitor the number of media errors that occur within the time window. The default setting is 12 hours.

```bash
-UNRESTRICTED_SHARING 0|1|no|yes
```

Enables the unrestricted media sharing for all media servers.

```bash
-USE_POTENTIAL_FREESPACE_FOR_ALLOCATION 0|1|no|yes
```

Allows the memory allocation of the available free space. The High Water Mark normally triggers image cleanup on BasicDisk storage units and disk pools. When the High water mark is reached in a storage lifecycle policy, it can prevent the use of any more memory space.
For example, the **High water mark** is 90%, but the potential free space is 50%. When the free space that is left on disk is only available past the **High water mark**, the backup fails. Turn on this parameter (1) to allow the use of the 40% free space between the potential free space and the **High water mark**.

The default setting is no (0).

```-VALIDATE_HOST_NAME 0|1|no|yes```

Enables the host name character validation according to NetBackup standard. If this option is disabled, you can use a name like "_host1", which does not follow the standard.

```-VAULT_CLEAR_MEDIA_DESC 0|1|no|yes```

This option is an EMM global option that applies to every host that uses the EMM server. It is not a host option. When NetBackup media is returned from the off-site vault during a typical tape rotation, it is expired and is ready for reuse by new backups. To avoid confusion, it may be helpful to clear the old media description information when an expired tape is returned to the robot. If this entry is specified, the media description field is cleared when other Vault information is cleared from the Media Manager volume database.

```-deletealldevices```

Deletes all tape devices.

```-allrecords```

Deletes all tape devices across all computers. You cannot use this option with the `-machinename` option.

```-emmname string```

Name of the EMM server.

```-emmport unsigned_integer```

Port number for the EMM server.

```-machinename string```

Deletes all tape devices that are attached to the specified media server. You cannot use this option with the `-allrecords` option.

```-machinetype api | app_cluster | appliance | client | cluster | disk_array | foreign_media | master | media | nbwss_endpoint | ndmp | remote_master | replication_host | virtual_machine```

Specifies the type of the computer name. You cannot use this option with the `-allrecords` option.
-deletehost

Deletes an EMM computer record by using the required computer name and computer type.

-brief

Generates a less verbose output of the command.

-machinename string

Removes the specified host from the EMM database.

-Machinetype api | app_cluster | cluster | master | media | ndmp

Identifies by type the computer to be removed.

-errorsdb

-brief

Generates a less verbose output of the command.

-prune [-days no_of_days] [-hours no_of_hours] [-minutes no_of_minutes]

Removes the entries from the error database. The optional days, hours, and minutes arguments determine which database entries to delete. It removes any entries older than the specified time.

-getemmsserver

Displays the information on all the hosts in a particular EMM domain. Use this command to ensure a level of consistency in a newly installed domain or modified domain.

-brief

Generates a less verbose output of the command.

-masterserver string

Specifies a name of a master server for an EMM domain. If you omit this option when you use this command, the current computer is assumed.

-timeout unsigned integer

Specifies a temporary timeout value in seconds to be used during the duration of this command.

-help

Displays usage information for the specified command by entering the following:

nbemmcmd -help command

-listhosts

This option dumps the table structure for each known host.
-display_server  -machinename string  -machinetype string
     Displays only the specified computer by the computer name and computer
     type.

-list_app_clusters  -masterserver string
     Lists all of the application clusters of the specified master server.

-list_snap_vault_fileers  -machinename string
     Lists all of the SnapVault filers of the specified computer name See the
     -machinename option description that follows.

-list_snap_vault_media_servers  -masterserver string
     Lists all of the SnapVault media servers of the specified master server.

-list_sts_hosts  -machinename string
     Lists all OpenStorage hosts connected to the specified computer name.

-list_sts_media_servers  -masterserver string
     Lists all OpenStorage media servers that are connected to the specified
     master server.

-machinename api  |  app_cluster  |  cluster  |  master  |  media  |  ndmp
     Defines the type of computer to list.

-nbservers  -masterserver string
     Displays only the media servers and master servers. The default for
     -listhosts is to display all servers.

-netbackupversion level[.major_level[minor_level]]
     Specifies the computer version. The level variable has a range of 0-99.
     The major_level and minor_level variables are optional single-digit fields.
     There should be no spaces between major_level and minor_level.
     For example, enter the following information to specify NetBackup 7.0:
     -netbackupversion 7.0 or -netbackupversion 7

-servers_in_emm_cluster  -clustername string
     Lists all servers in the specified cluster.

-server_in_app_cluster  -clustername string
     Lists all of the application cluster servers of the specified cluster.

-brief
     Makes the output of the command less verbose.

-parsable
     Makes the output of the command parsable.
-verbose
Controls how host information is displayed. Multiple lines of output are printed, one for each parameter of a host.

-listmedia

-allrecords
Displays all media records.

-mediaid string
Specifies the media ID of the EMM media record.

-mediatype unsigned integer
Queries the volumes by media type.
Valid media types for NetBackup Enterprise Server are:
4mm, 8mm, 8mm2, 8mm3, dlt, dlt2, dlt3, dlt, hcart, hcart2, hcart3, qcrt, 4mm_clean, 8mm_clean, 8mm2_clean, 8mm3_clean, dlt_clean, dlt2_clean, dlt3_clean, dlt_clean, hcart_clean, hcart2_clean, hcart3_clean.

Valid media types for a NetBackup server are:
4mm, 8mm, dlt, hcart, qcrt, 4mm_clean, 8mm_clean, dlt_clean, hcart_clean.

-poolname string
Queries the volumes by pool number, an index into the volume pool. Use `vmpool -listall` to determine the index for a given pool name.

-robotnumber unsigned_integer
Queries the volumes by robot number. A robot number is a unique, logical identification number for the robot where the volume is located.

-vaultcontainer string
Lists the volumes that are stored in the container. The `string` variable is the `vault_container_id`, a string of up to 29 alphanumeric characters.

-listsettings

-machinename string
Specifies which computer to list settings for.

-brief
Generates a less verbose output of the command.

-emmname string
Specifies the host name of the pertinent EMM server. If `-emmname` is not specified, the default name is located in the `bp.conf` file.
-emmport unsigned_integer
   Specifies the port number of the EMM server to where calls are made. If
   -emmport is not specified, the default port is specified in the bp.conf file.

-machinealias
   The following parameters are used to maintain the alias list for a particular
   computer. Use them to view current aliases, add new aliases, or delete current
   aliases for an identified computer.

   -addalias -alias alias -machinename name -machinetype type
   Adds an alias name to a computer. Identify the computer name that is to
   receive the alias as well as the computer type.

   For example, to create a media server with the alias name blue, use the
   following command:

   machinealias -machinename 10.10.10.1 -machinetype media
   -addalias -alias blue

   -deletealias -alias name -machinetype type
   Deletes an alias name from the database. This operation requires that
   you identify the alias to be deleted by using the -alias string command
   and computer type with this option.

   -deleteallaliases -alias name -machinetype type
   Deletes all aliases for a particular computer. To perform this operation you
   must identify the computer name and the computer type.

   -getaliases
   Retrieves all aliases for a particular computer. To perform this operation
   you must identify the computer name and the computer type.

   -alias string
   Specifies the string that identifies the alias name of a computer.

   -machinename string
   Specifies the name of a computer.

   -Machinetype api | app_cluster | cluster | master | media | ndmp
   Defines what the computer is used as.

   -releasecache
   Release cache memory that the EMM server has used.

   -brief
   Generates a less verbose output of the command.
-emmname string
  Specifies the host name of the pertinent EMM server. If -emmname is not
  specified, the default name is located in the bp.conf file.

-emmport unsigned_integer
  Specifies the port number of the EMM server to where calls are made. If
  -emmport is not specified, the default port is specified in the bp.conf file.

-renamehost
  This command, with the required computer name and new computer name
  options, renames the current computer name to a new computer name.

  -machinename string
    Defines the current computer name.

  -newmachinename string
    Defines the new computer name.

-resethost
  Use this command to reset the Host Properties for an updated host. The Host
  Properties section displays the additional information that the host web service
  collects.

  Run this command if you have downgraded the NetBackup version on a
  computer or removed a host from your NetBackup environment. You only need
  to run this command if you downgrade to NetBackup 8.0 or earlier. You may
  need to restart the NetBackup Administration Console for the changes to take
  effect.

  Before you run the nbemmcmd -resethost command, you must run the bpnbat
  -login -loginType WEB command. This command authenticates your web
  services login. After you successfully run the bpnbat command, run the
  nbemmcmd -resethost command.

  -machinename string
    Defines the name of the computer that was downgraded or removed from
    the NetBackup environment.

-servercontrol
  This command suspends and resumes control of a specified server. You can
  perform database maintenance without the corruption of existing data because
  a job began to run during this time.

  -resume
    Resumes the control of a specified server.

  -suspend
    Suspends the control of a specified server.
-setemmsserver

This command changes the EMM server name for certain hosts in the domain whose name matches the old EMM server name. This command has the following options:

-emmsservername string

Specifies the EMM server name to be changed.

-newemmsservername string

Specifies the new, or replacement, value for the EMM server.

-masterserver string

Specifies a name of a master server for an EMM domain. If you omit this option when you use this command, the current computer is assumed.

-timeout unsigned integer

Specifies a temporary timeout value in seconds to use for the duration of this command.

-updatehost -machinename string

This command, when used with the following options, enables you to change a computer record that was specified by using the required -machinename option.

-add_server_to_app_cluster

This option designates that the computer should be added to the application cluster that is specified in the -clusternname option.

-activenodename string

Identifies the active node in a cluster.

-clusternname string

Identifies a cluster to which this computer belongs.

-delete_server_from_app_cluster

Designates that the computer should be removed from the application cluster that is specified in the -clusternname option.

-displayname string

Displays the assigned name of a computer that is equivalent to the numbered identifier for that computer.

-machinename string

Specifies the computer name to update.
-machinestateop clr_admin_pause | clr_admin_pause_and_set_active | clr_disk_active | clr_ltid_restart | clr_master_server_connectivity | clr_tape_active | reset_all | set_admin_pause | set_disk_active | set_master_server_connectivity | set_tape_active

Sets or clears the specified computer state.

-Machinetype api | app_cluster | cluster | master | media | ndmp

Defines what the computer is used as.

-masterserver string

Defines the host's master server in the domain.

-netbackupversion level[.major_level[minor_level]]

Adds a host and specifies the version it is running. The level variable as a range of 0-99. The major_level and minor_level variables are optional single-digit fields. There should be no spaces between the major_level and minor_level variables.

For example, enter the following to specify NetBackup 7.0:
-netbackupversion 7.0

-operatingsystem hpux | linux | rs6000 | solaris | windows

This option enables you to update the operating system of the computer.

EXAMPLES

Example 1 - Display the information on all the hosts in a particular EMM domain.

# nbemmcmd -getemmsserver
These hosts were found in this domain: throttle, upwords
Checking with host: throttle...
Checking with host: upwords...
Server Type Host Version Host Name EMM Server
MEDIA UNKNOWN RELEASE (0) throttle throttle
MASTER 7.6 upwords upwords

One or more hosts had mismatched EMM Servers.
Run-time failure: The consistency check either failed or was incomplete. Command did not complete successfully.

Example 2 - Change the EMM server name for certain hosts in the domain whose name matches the old EMM server name.

# nbemmcmd -setemmserver -emmservename throttle -newemmm upwords
These hosts were found in this domain: throttle, upwords
Checking with host: throttle...
Checking with host: upwords...

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Host Version</th>
<th>Host Name</th>
<th>EMM Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEDIA</td>
<td>UNKNOWN RELEASE (0)</td>
<td>throttle</td>
<td>throttle</td>
</tr>
</tbody>
</table>

EMM server name was changed.

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Host Version</th>
<th>Host Name</th>
<th>EMM Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>MASTER</td>
<td>7.6</td>
<td>upwords</td>
<td>upwords</td>
</tr>
</tbody>
</table>

One media hosts had EMM Server name changed. Command was completed successfully.

**Example 3 - List the settings for computer name** orbitvml.

```
# nbemmcmd -listsettings -machinename orbitvml

NBEMMCDM, Version:7.1

The following configuration settings were found:
ALLOW_MULTIPLE_RETENTIONS_PER_MEDIA="no"
DISABLE_DISK_STU_JOB_THROTTLING="no"
DISABLE_STANDALONE_DRIVE_EXTENSIONS="no"
MEDIA_REQUEST_DELAY="0"
MUST_USE_LOCAL_DRIVE="no"
NON_ROBOTIC_MEDIA_ID_PREFIX="A"
MAX_REALLOC_TRIES="1000"
DISABLE_BACKUPS_SPANNING_DISK="no"
DISALLOW_NONNDMP_ON_NDMP_DRIVE="no"
DO_NOT_EJECT_STANDALONE="no"
PREFER_NDMP_PATH_FOR_RESTORE="yes"
DONT_USE_SLAVE="no"
DRIVE_ERROR_THRESHOLD="2"
MEDIA_ERROR_THRESHOLD="2"
TIME_WINDOW="12"
SCSI_PROTECTION="SR"
NBUFS_DUP_TSU_TO_DSU="no"
NBUFS_DESTINATION_DSU="NONE"
NBUFS_RETENTION_LEVEL="0"
MPMS_DISABLE_RANK="0"
MPMS_DISABLE_EVENTS="no"
UNRESTRICTED_SHARING="no"
FATPIPE_USAGE_PREFERENCE="Preferred"
FATPIPE_WAIT_PERIOD="15"
FATPIPE_RESTORE_WAIT_PERIOD="5"
FT_MAX_CLIENT_PORTS_PER_SERVER="2"
FT_MAX_CLIENTS_PER_PORT="2"
SHARDDISK_MOUNT_POINT="/nbusharedisk"
AUDIT="ENABLED"
AUDIT_RETENTION_PERIOD="90"
```
RETURN_UNASSIGNED_MEDIA_TO_SCRATCH_POOL="yes"
VAULT_CLEAR_MEDIA_DESC="no"
SCSI_PERSISTENT_RESERVE="0"
Command completed successfully.
nbfindfile

nbfindfile – search files or folders based on simple search criteria

SYNOPSIS


On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The nbfindfile command lets you search files or folders based on simple search criteria like file name and path including wildcard and backup date range. Users can specify a set of clients, possibly belonging to different master servers, for which backups are to be searched. You can specify advanced search criteria including policy type, schedule type, policy name, policy associated keywords, file extensions, file modification date range, and file size.

OPTIONS

-atime

When used with the -l option, -atime displays the last access time in place of the last modification time.

-atime_max mm/dd/yyyy [hh:mm:ss]

Specifies the maximum last access time of objects to be returned. The default is infinite.
-atime_min mm/dd/yyyy [hh:mm:ss]
   Specifies the minimum last access time of objects to be returned. The default is 01/01/1970 00:00:00.

-backupid backup_id
   The backup ID of the backup image that should be searched.

-c client_name[, ...]
   Specifies the names of the NetBackup clients whose backups need to be searched. The client names must be specified as they appear in the NetBackup configuration. Multiple clients can be specified as a list that is separated by commas.

-case_sen
   Performs case sensitive matching.

-ctime
   When used with the -l option, -ctime displays the last change time in place of the last modification time.

-ctime_max mm/dd/yyyy [hh:mm:ss]
   Specifies the maximum last change time of objects to be returned. The default is infinite.

-ctime_min mm/dd/yyyy [hh:mm:ss]
   Specifies the minimum last change time of objects to be returned. The default is 01/01/1970 00:00:00.

-e mm/dd/yyyy [hh:mm:ss] | -e_ut unix_time
   Specifies the end date for the search. Backups that occurred at or before the specified date and time are searched. The default is the current date and time.

-extn file_extn[, ...]
   Returns only the files with the specified extensions. For example, -extn txt,do*,jp?.

-h | -help
   Displays usage information.

-kb_max max_size_kb
   Specifies the maximum size in kilobytes (1024 bytes) of files to be returned. The default is infinite.

-kb_min min_size_kb
   Specifies the minimum size in kilobytes (1024 bytes) of files to be returned. The default is 0 (zero).
-keyword "keyword_phrase"
  Searches only the backup images that contain a matching keyword phrase are searched. The keyword phrase can contain wildcards (*, ?) and square bracket expressions. Examples are [Kk]ey*, [a-z]e?, and [!K]ey.

-l
  Displays output in long list format. The default condition is the last modification time of objects.

-max_results number
  Specifies the maximum number of results to be displayed. The default is infinite.

-mtime_max mm/dd/yyyy [hh:mm:ss]
  Specifies the maximum last modification time of objects to be returned. The default is infinite.

-mtime_min mm/dd/yyyy [hh:mm:ss]
  Specifies the minimum last modification time of objects to be returned. The default is 01/01/1970 00:00:00.

-only_dirs | -only_files
  Specifies the type of objects to be returned.

-p search_pattern
  Specifies the search pattern. File and directory entries matching this pattern are displayed.

-policy policy_name
  Searches only the backup images that are created using the specified policy.

-pt policy_type
  Searches only the backups with the specified policy type. Valid values for policy_type: Any, Standard, FlashBackup, MS-Windows, NDMP, FlashBackup-Windows.

-r
  Displays raw output.

-s mm/dd/yyyy [hh:mm:ss] | -s_ut unix_time
  Specifies the start date for the search. Backups that occurred at or after the specified date and time are searched. The default is 30 days before the end date.

-st sched_type
  Specifies a schedule type for the image selection. The default is any schedule type. Valid values, in either uppercase or lowercase, are as follows:
  - ANY
- FULL (full backup)
- INCR (differential-incremental backup)
- CINC (cumulative-incremental backup)
- UBAK (user backup)
- UARC (user archive)
- SCHED
- USER (user backup and user archive)
- NOT_ARCHIVE (all backups except user archive)
nbfirescan

nbfirescan — scan for SCSI disk devices and print out report

SYNOPSIS

nbfirescan

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\Common Files\Symantec Shared\VxFI\4\Bin\n
DESCRIPTION

The Frozen Image Rescan (nbfirescan) utility scans for SCSI disk devices and prints what it finds. It is available on all media servers and is used to triage import problems.

Before you run the command, add the NetBackup bin directory in the PATH statement. For example, setx path "%path%;C:\Program Files\Veritas\NetBackup\bin" for Windows or export PATH=$PATH:/usr/openv/netbackup/bin for UNIX or Linux.

Only authorized users can run this command.

For more information about NetBackup authorization, refer to the NetBackup Security and Encryption Guide.

EXAMPLES

The following applies to Windows systems only; it is a sample output from the local host SCSI bus scan:

C:\Program Files\Common Files\Veritas\VxFI\4\Bin>nbfirescan.exe

nbfirescan v4.4.1 - Copyright (c) 2005-2010 Veritas Technologies LLC.
Rescanning
devices..................................................Complete.
Device count: 48
DevicePath Vendor Product ID EnclosureId
DeviceId [Ctl,Bus,Tgt,Lun]
------------------------------------------------------
\\.\PHYSICALDRIVE0  SEAGATE  ST336607LW  -
\\.\PHYSICALDRIVE1  SEAGATE  ST336607LW  -
\\.\PHYSICALDRIVE2  COMPAQ  HSV111 (C)COMPAQ  5000-1FE1-5004-5660
6005-08B4-0010-120F-0000-7000-0956-0000  \[00,04,00,01]\]
\\.\PHYSICALDRIVE3  COMPAQ  HSV111 (C)COMPAQ  5000-1FE1-5004-5660
6005-08B4-0010-4E39-0000-4000-0010-0000  \[00,04,00,02]\]
nbftadm

nbftadm – start menu interface for managing the Fibre Transport (FT)

SYNOPSIS

/usr/openv/netbackup/bin/nbftadm

DESCRIPTION

This command operates only on UNIX systems.

nbftadm has a menu interface that an administrator can use to configure and manage the fiber transport between NetBackup media servers and SAN clients. nbftadm requires administrator privileges. This interface can be used from any character-based terminal (or terminal emulation window) for which the administrator has a termcap or a terminfo definition.

See the NetBackup Administrator’s Guide and the nbftadm online Help for detailed operating instructions.

FILES

/usr/openv/netbackup/help/nbftadm/*
/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/bin/initbprd
/usr/openv/netbackup/bp.conf

SEE ALSO

See bprd on page 377.
nbftconfig

nbftconfig – configure the attributes that are associated with Fibre Transport (FT) servers and SAN clients

SYNOPSIS


nbftconfig -[ac]addclient -C client_name [-M master_server] [-ftpref preferred | always | never] [-ftwait minutes] [-ftrwait minutes]

nbftconfig -[dc]deleteclient -C client_name


nbftconfig -[rc]rescanclient client_name

nbftconfig -[ra]rescanallclients

nbftconfig -[lc]listclients [-verbose] [-C client_name | -Me media_server | -M master_server]

nbftconfig -[ds]deleteserver -Me media_server

nbftconfig -[cs]changeserver -Me media_server [-l connection_limit] [-state active | disabled]

nbftconfig -[ls]listservers [-Me media_server | -M master_server] [-verbose]

nbftconfig -[la]listactive [-C client_name | -Me media_server] [-verbose]

nbftconfig -[lt]listtargets [-Me media_server] [-verbose]


nbftconfig -getconfig [-M master_server] [-verbose]

nbftconfig -option -help
On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\

DESCRIPTION

nbftconfig is a NetBackup utility that modifies the attributes that are associated with the Fibre Transport (FT) server. It also creates the SAN client entities in the EMM database.

nbftconfig performs the following operations:

- Add a new SAN client and its attributes to the EMM database.
- Modify an existing SAN client record.
- Delete a SAN client.
- Add a new FT server.
- Modify the attributes of an existing FT server record.
- List SAN clients that are defined within the database.
- List FT servers that are defined within the database.
- List by all active Fibre Channel connections.
- List the target port configuration information for FT media servers.

OPTIONS

-addclient

Adds the specified SAN client to the EMM database. SAN clients are normally automatically discovered when the SAN client code is installed on the client. However, if the notification from the client to the EMM server is lost, use this command to manually add the client. The following attributes can be set by using this command option:

-\C client_name
  Specifies the name of the SAN client that is to be added to the database.

-\M master_server
  Specifies the master server that is associated with the designated client. If this option is omitted, the local client’s master server is used.
-ftpref preferred | always | fail | never

Determines if the Fibre Channel connections to the media server are preferred (default condition), must always be used, or should never be used. If preferences are not provided, master server defaults are used. This value is set by default according to the global defined for the EMM server. The following describes the possible -ftpref values:

- Preferred. Use an FT device if one is available within the configured wait period in minutes. If an FT device is not available after the wait period elapses, NetBackup uses a LAN connection for the operation. If you select this option, also specify the wait period for backups and for restores.

- Always. NetBackup always uses an FT device for backups and restores of SAN clients, and waits until an FT device is available before it begins the operation.

- Fail. NetBackup fails the job if an FT device is not up and online. If the FT devices are online but busy, NetBackup waits until a device is available and assigns the next job to the device. An FT device may not exist because none is active, none have been configured, or the SAN Client license expired.

- Never. NetBackup never uses an FT pipe for backups and restores of SAN clients and uses a LAN connection for the backups and restores. If you specify Never for the master server, Fibre Transport is disabled in the NetBackup environment, and you can configure FT usage on a per-client basis. If you specify Never for a media server, Fibre Transport is disabled for the media server. If you specify Never for a SAN client, Fibre Transport is disabled for the client.

-ftrwait minutes

Defines the number of minutes that a restore job should wait for an available Fibre Channel connection before it uses a standard network connection. This option is only valid when the ftpref type is set to preferred.

-ftwait minutes

Defines the number of minutes that a backup job should wait for an available Fibre Channel connection before it uses a standard network connection. This option is valid only when the ftpref type is set to preferred.
-np number_of_ports

Defines the maximum number of client ports that can be simultaneously used on a single media server. If the maximum number of client ports is set to 0, then all ports are used. The default number of client ports is 2.

-deleteclient

Deletes the specified client from the EMM database. The following attribute may be included with this option.

-C client_name

Specifies the name of the SAN client that is to be deleted from the database.

-changeclient

Changes the options that are associated with a specific SAN. The following attributes can be set by using this command option:

-C client_name

Specifies the name of the SAN client that is to be added to the database.

-ftpref preferred | always | never

Determines if the Fibre Channel connections to the media server are preferred, must always be used, or should never be used. If preferences are not provided, master server defaults are used. This value is set by default according to the global defined for the EMM server.

-ftwait minutes

Defines the number of minutes that a backup job should wait for an available Fibre Channel connection before it uses a standard network connection. This option is valid only when the ftpref type is set to preferred.

-ftrwait minutes

Defines the number of minutes that a restore job should wait for an available Fibre Channel connection before it uses a standard network connection. This option is only valid when the ftpref type is set to preferred.

-rescanallclients

Scans all clients for new FT devices, up to five clients at a time.

-rescanclient

Scans the specified client for new FT devices. The following attribute can be set by using this command option:

client_name

Specifies the name of the SAN client to scan.
-listclients
Displays the list of SAN clients and attributes that are associated with the clients. By default all SAN clients are listed with a subset of attributes. The information output by the listclients operation depends on whether all clients are listed or the attributes associated with a specific SAN client.

The following attributes can be set by using this command option:

-C client_name
 Specifies the name of the SAN client whose information you want listed. If this attribute is omitted, listclients lists the information for all clients that are attached to the designated media server or master server.

-Me media_server
 Specifies the name of the FT server for whose attached clients you want the information listed.

-M master_server
 Specifies the master server that is associated with the FT servers. If this option is omitted, all FT servers are returned.

-verbose
 The output can be displayed in verbose mode and non-verbose mode (by default). When all clients are listed (including all clients by master or media server), the information appears for multi-client, verbose mode output.

The following information appears in verbose mode for the client record:
SAN client name
Version — Client NetBackup software version
State - SAN client state
Master server name
Number of FT servers to which the SAN client can connect
Usage preferences (see addclient)
Usage preference wait period (See addclient)

If a specific SAN client is included in the listclients command, then the information is displayed for that client (single client output):
The following information appears in verbose mode for the client device records:
SAN client device state
Media server name
Media server state
Media server HBA port number on which a device was discovered

Media server HBA port mode

LUN — The LUN that is associated with the HBA Port

The default condition is non-verbose mode output. The output information is the same as for verbose mode in space-separated text format. Client records start with the letter "c" and device records start with the letter "d".

-deleteserver

Deletes the specified client from the EMM database. The following attribute can be set by using this command option:

-M media_server

Specifies the name of the FT server to be deleted.

-changeserver

Changes the attributes that are associated with an FT server. The following attributes can be set by using this command option:

-M media_server

Specifies the name of the FT server to be changed.

-M master_server

Specifies the master server that is associated with the designated media server.

-l connection_limit

Specifies the maximum number of connections that the FT server supports. This number is the total for the server and not per LUN or HBA. If this option is omitted, the FT server’s default connection limit is used.

-state [active | disabled]

Identifies the assigned state of the FT server. The possible values are Active and Disabled.

-listservers

This operation is used to display the list of FT servers and attributes that are associated with the servers. By default all FT servers are listed:

The following options are associated with the listservers command:

-M media_server

Specifies the name of the media server whose attached FT servers are to be listed.

-M master_server

Specifies the name of the master server whose attached FT servers are to be listed.
-verbose

Specifies a detailed output for the server information.

The output can be displayed in verbose mode and non-verbose mode (by default). When all clients are listed (including all clients by master or media server), the information appears for multi-client, verbose mode output.

The following output information appears in verbose mode for the server record:

SAN client name
FT Server name
Version — Server NetBackup software version
State -FT Server state
Connection limit

If a specific SAN client is included in the listclients command, then the information is displayed for that client (single client output):

The following output information appears in verbose mode for the client device records:

FT Server HBA port
FT Server HBA port mode
FT Server device state
Associated LUN
FT Connections — number of active FT Connections on the specific HBA/LUN

The default condition is non-verbose mode output. The output information is the same as for verbose mode in space-separated text format. Media server records start with the letter "d" and device records start with the letter "d". Each HBA port number on each server gets a separate line entry in the output.

-listtargets

This operation is used to display the list of specifics on all the target ports on FT media servers. By default all FT servers are listed.

The following options are associated with the listtargets command:

- Me media_server

Specifies the name of the media server whose target port configurations are to be listed. If no media server is specified, the target port information is listed for all FT media servers.
-verbose
   Specifies a detailed output for the server information.
   The output can be displayed in verbose mode and non-verbose mode (by
default). When all clients are listed, the information appears for multi-client,
verbose mode output. The default condition is non-verbose mode output.
The output information is the same as for verbose mode in space-separated
text format.
   EXAMPLE 2 shows the use of the nbftconfig -listtargets -verbose
command and the output data categories.

-getconfig
   Retrieves the default configuration parameters for the FT server and SAN client
attributes.
   The following options are associated with the -getconfig command:
   -M master_server
      Specifies the master server that is associated with the FT server. If this
option is omitted, the master server of the local machine is used.
   -verbose
      Specifies a detailed output for the configuration information.

-setconfig
   Sets the configuration parameters for the FT server and SAN client attributes.
   These attributes can be set by using this command option:
   -ftpref preferred | always | never
      Determines if the Fibre Channel connections to the media server are preferred,
must always be used, or should never be used. This value is set by default
according to the global defined for the EMM server.
   Usage of -ftpref and -np or -ncp is mutually exclusive.
   -ftwait minutes
      Defines the number of minutes that a backup job should wait for an
available Fibre Channel connection before it uses a standard network
connection. This option is required only when the ftpref type is set to
preferred.
   -ftrwait minutes
      Defines the number of minutes that a restore job should wait for an
available Fibre Channel connection before it uses a standard network
connection. This option is required only when the ftpref type is set to
preferred.
-ncp number_of_clients_per_target_port
  Specifies the maximum number of clients per target port that are allowed on any FT media server.

-np number_of_ports
  Specifies the number of initiator ports on a client that can be used with one FT media server.

-listactive
  Lists the active FT connections. At a minimum, the following information should be obtainable from this command for each FT connection:
  
  SAN Client Name
  Client HBA Number
  FT Server Name
  Server HBA number
  FT Channel - Number of the FT Channel
  LUN
  Direction
  Job Number
  
The following options are associated with the listactive command:

  -C client_name
    Specifies the name of the SAN client whose active FT connections you want listed. If this attribute and the media server attribute are omitted, -listactive lists the information for the local machine’s master server.

  -Me media_server
    Specifies the name of the FT server from whose attached clients you want the FT connections listed.

  -verbose
    Specifies a detailed output for the FT connection information.

EXAMPLES

Example 1 - List FT configuration values for master server wendigo in verbose mode. These values are set in the nbftconfig -getconfig command.

  # nbftconfig -getconfig -verbose
  Master Server : wendigo.example.com
  Client Ports/Server: 2
Clients/Target port: 2
FT Preference : preferred
Backup Wait Time : 15
Restore Wait Time : 5

Example 2 - Show how the -listtargets option lists the configuration specifics for all the target ports on FT media server wendigo in verbose mode.

# nbftconfig -listtargets -verbose
FT Server Name : wendigo.example.com
FT Server HBA Port : 1
FT Server Port WWN : 21:00:00:E0:8B:8F:CC:79
FT Server Port Mode : PTP
FT Server Port Model : QLA234x Series FC Hba
FT Server Port Vendor: Qlogic
FT Server Device State : active
Associated LUN : 0
Active Connections on LUN: 0
FT Server Device State : active
Associated LUN : 1
Active Connections on LUN: 0
FT Server HBA Port : 0
FT Server Port WWN : 21:01:00:E0:8B:AF:CC:79
FT Server Port Mode : DISCONNECTED
FT Server Port Model : QLA234x Series FC Hba
FT Server Port Vendor: Qlogic
FT Server Device State : active
Associated LUN : 0
Active Connections on LUN: 0
FT Server Device State : active
Associated LUN : 1
Active Connections on LUN: 0
nbgetconfig

nbgetconfig  – helper program to obtain configuration information

SYNOPSIS

nbgetconfig  -M host [-x | -X | -d | -D] [config_item ...]

nbgetconfig  [-u | -h] [-x | -X | -d | -D] [config_item ...]

nbgetconfig  -private_exld_list

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

The nbgetconfig command is available for all NetBackup host platforms. It displays the configuration information of a specified host in various formats.

You must have administrator privileges to run this command.

OPTIONS

-D | -d

The -D option returns a listing of configuration entry names, the existing configuration values in brackets, and the default configuration values in parentheses. This operation can be performed locally or remotely. The remote machine with an identical version of netbackup is installed. The -D and -d options may be combined with the -M, -h, and -u options.

The following is part of a listing that the -D option returns:

...  
REQUEST_DELIVERY_TIMEOUT       [300]    (300)
DISABLE_SCSI_RESERVE            [NO]     (NO)
Time_Overlap                    [60]     (60)
Buffer_Size                     [16]     (16)
Use_Archive_Bit                 [YES]    (YES)
Perform_Default_Search          [YES]    (YES)
Accumulate_Files  [NO]  (NO)
...

The \(-d\) option functions like the \(-D\), except \(-d\) displays only the entries changed from the configuration defaults. The following is an example display:

```
.. PEM_VERBOSE [-1] (0)
                 JM_VERBOSE [-1] (0)
                 RB_VERBOSE [-1] (0)
                CONN_OPTIONS [**configured**] ()
                Exclude [**configured**] ()
                 Browser [teburi.min.vrts.com] ()
           AUTHENTICATION_DOMAIN [**not configured**] ()
               VXSS_NETWORK [**not configured**] ()
            PREFERRED_NETWORK [**not configured**] ()
...
```

More information on many of the configuration items are described in the NetBackup Administrator’s Guide, Volume I.

\(-H\) \(\text{config\_item}\)

Displays the valid configuration items.

\(-h\)

Displays the default local host configuration.

\(-M\) \(\text{host}\)

Specifies the NetBackup host or client whose configuration appears.

\(-\text{private\_exld\_list}\)

Lists all the directories and files that are excluded by default from a backup.

\(-u\)

Displays the current user configuration.

\(-X\)

Lists all configuration items by default. The \(-x\) and \(-X\) options may be combined with the \(-M\), \(-h\), and \(-u\) options. The \(-x\) and \(-X\) options have no effect if one or more configuration items are specified on the command line.

If \(\text{config\_item}\) is specified, it appears on the specified configuration items.

\(-x\)

Excludes the items not explicitly listed in the configuration.
EXAMPLES

Example 1 - Retrieve the VERSIONINFO option setting from the bp.conf file.

# nbgetconfig VERSIONINFO
VERSIONINFO = "Windows2008" "6" "win_x64" "NetBackup" "7.6" 760000

Example 2 - Retrieve the list of directories and files that are excluded by default from a backup.

#nbgetconfig -private_exld_list

Total Number of Entries in Exclude List : 24
/usr/openv/var/global/vxss/
/usr/openv/var/global/wsl/credentials/
/usr/openv/var/session/
/usr/openv/var/vxss/at/
/usr/openv/var/vxss/credentials/
/usr/openv/var/vxss/crl/
/usr/openv/var/websvcccreds/
/usr/openv/var/global/wmc/cloud/*.pem
/usr/openv/var/global/webrootcert.pem
/usr/openv/var/global/.yekcnedwssap
/usr/openv/var/global/jkskey
/usr/openv/var/keyfile.dat
/opt/VRTSnbu/var/global/vxss/
/opt/VRTSnbu/var/global/wsl/credentials/
/opt/VRTSnbu/var/session/
/opt/VRTSnbu/var/vxss/at/
/opt/VRTSnbu/var/vxss/credentials/
/opt/VRTSnbu/var/vxss/crl/
/opt/VRTSnbu/var/websvcccreds/
/opt/VRTSnbu/var/global/wmc/cloud/*.pem
/opt/VRTSnbu/var/global/webrootcert.pem
/opt/VRTSnbu/var/global/.yekcnedwssap
/opt/VRTSnbu/var/global/jkskey
/opt/VRTSnbu/var/keyfile.dat

SEE ALSO

See nbsetconfig on page 831.
See bpgetconfig on page 158.
See bpsetconfig on page 416.
**nbhba**

nbhba – run the utility to modify an HBA cards device ID

**SYNOPSIS**

```
nbhba -modify -wwn string [ -wwn wwn_string ... ] -mode target | initiator
nbhba -l | -L
```

The directory path to this command is

```
/usr/openv/netbackup/bin/admincmd
```

**DESCRIPTION**

This command operates only on UNIX systems.

nbhba enables an administrator to set the mode of the HBA cards in the system. The HBA cards can respond as either target mode or initiator mode devices. To change the mode of the HBA card for use with the SAN Client, change the device ID of the QLogic card. The device ID changes from its standard designation to a special designation that allows only the target mode driver to be loaded.

**OPTIONS**

- `-l, -L`

- `-l` lists the drivers of all HBA cards that are installed in the system. `-L` also lists information about the cards. The following information appears for each HBA port:
  - Linux systems only: The first line of data lists the number of ports recognized, the number of target mode ports, and the driver mode (e.g., `nbhba installed`).
  - HBA index - a relative number of the HBA card in the system. This number is valid until the system restarts.
  - Device ID - the device ID as read from the card.
  - World Wide Name - the world-wide name that is read from the card.
  - Model Name - the physical slot in which the card is installed in the system.
  - Port - the port on the HBA card. Possible values are 0 or 1.
- **Mode** - the mode of the card, target, or initiator.

  **-modify**
  
  Modifies the mode of the HBA card. Specify the HBA card to be changed through the World Wide Name (wwn).

  The mode of the card can be target or initiator. Target mode is used as the terminus for a SAN Client. Initiator mode connects the media server disk resources. Optionally, the administrator can input the specific QLogic device ID for either the target mode or initiator mode driver.

  **-wwn string**
  
  Specifies the World Wide Name of the HBA card. These required selection criteria are used to specify which card and port to mark.

  **-mode target | initiator**
  
  Sets the mode of the specified HBA card. Target mode uses the HBA as the target for a SAN Client. Do not set an existing card to initiator mode unless it had been previously set to target mode.

**EXAMPLES**

Example 1 - Set the HBA port with worldwide name "123456789ABCDEF0" to target mode:

```
# nbhba -modify -wwn 123456789ABCDEF0 -mode target
```

Example 2 - List information on all HBA cards that are installed on a Linux system (see the first line of the output). Note that Card #2 uses both ports.

```
nbhba -L
4 ports recognized; 3 target mode ports; mode : driver in nbhba mode

Card #1
HBA Index #1
  Device ID = 2312
  World Wide Name = 21:00:00:E0:8B:8F:E6:45
  Model Name = "QLA2340 "
  Port = 0
  Mode = initiator (designated for other use)(100)

Card #2
HBA Index #2
  Device ID = 2312
  World Wide Name = 21:00:00:E0:8B:9A:22:3D
  Model Name = "QLA2342 "
```
Port = 0
Mode = target (designated for FT Server)(8101)  HBA Index #3
Device ID = 2312
World Wide Name = 21:01:00:E0:8B:BA:22:3D
Model Name = "QLA2342"
Port = 1
Mode = target (designated for FT Server)(8101)

Card #3
HBA Index #4
Device ID = 2422
World Wide Name = 21:00:00:E0:8B:9B:28:89
Model Name = "QLA2460"
Port = 0
Mode = target (designated for FT Server)(8133)

Example 3 - This example is the short list type (-l) counterpart of Example 2 (long
list type -L). It lists only the drivers of all the HBA cards that are installed on the
system. Note that the first line of the output (4 ports recognized...) displays only
on a Linux system.

# nbhba -l
4 ports recognized; 3 target mode ports; mode : driver in nbhba mode

1 2312 21:00:00:E0:8B:B6:E6:45 "QLA2340" 0 0 100
2 2312 21:00:00:E0:8B:9A:22:3D "QLA2342" 0 1 8101
3 2312 21:01:00:E0:8B:BA:22:3D "QLA2342" 1 1 8101
4 2422 21:00:00:E0:8B:9B:28:89 "QLA2460" 0 1 8133
nbholdutil

nbholdutil – run the utility that places and removes holds on backup images

SYNOPSIS

nbholdutil -create -holdname hold_name [-reason "string"] -filepath filepath | -backupid backup_ID -primarycopy | -allcopy

nbholdutil -add -holdid hold_id | -holdname hold_name [-reason "string"] -filepath filepath | -backupid backup_ID -primarycopy | -allcopy

nbholdutil -list [-holdid hold_id] | [-holdname hold_name] | [-backupid backup_ID -primarycopy | -allcopy] [-U [-include_extended_info]]

nbholdutil -list -holdname hold_name -U -include_extended_info > bid.txt

nbholdutil -delete -holdid hold_id] | -holdname hold_name [-force] [-reason "string"]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/goodies

On Windows systems, the directory path to this command is install_path\NetBackup\bin\goodies

DESCRIPTION

The nbholdutil utility places holds on backup images. The holds provide a mechanism to override existing retention levels. These holds ensure that backup images and associated media are retained until the holds are released.

nbholdutil performs the following operations:

- **-create** creates a hold on one or more holds for backup images.
- **-add** adds one or more images to an existing hold.
- **-list** outputs a list of all holds. This operation also creates the backup ID (BID) file.
- **-delete** deletes one or more holds.

Only authorized users can run this command.
nbholdutil cannot hold an incremental backup image with zero files. If either a differential or cumulative incremental backup has zero (0) files in the backup image, nbholdutil fails with EXIT STATUS = 1401.

OPTIONS

-allcopy
   Includes all copies of the specified backup image.
-backupid backup_ID
   Specifies the backup ID of the backup image.
-filepath filepath | -primarycopy | -allcopy
   Specifies the file path to the backup image.
-force
   Bypasses a prompt to confirm the release of the hold. This option is useful in a script because it allows the release operations to continue without waiting for a response to the prompt.
-holdname hold_name
   Specifies a unique name for the hold.
-include_extended_info > bid.txt
   Provides more details regarding the images on hold and creates a backup (BID) in which to store the information.
-primarycopy
   Includes only the primary copy of the specified backup image.
-reason "string"
   Indicates the reason for performing this command action. The reason text string that you enter is captured and appears in the audit report. Enclose the string with double quotes ("...") and the string cannot exceed 512 characters. It cannot begin with a dash character (-) nor contain a single quotation mark (').
-U
   Reports in user format which includes additional user information.

EXAMPLES

Example 1 - Create a hold that is called legal_case1. The backup image ID is win81.sky.com_1307425938. The -allcopy option indicates that the hold includes all copies of the selected backup image. If this option is not included, this operation holds only the primary copy of the selected backup image.
# nbholdutil -create -holdname legal_case1 -backupid win81.sky.com_1307425938 -allcopy
nbhostidentity

nbhostidentity imports the NetBackup master server identity after a disaster.

SYNOPSIS

nbhostidentity -import -infile file_path [-altdir directory_path [-noacls]] [-mapuser domain1\user1:domain2\user2 [,domain3\user3:domain4\user4]

nbhostidentity -testpassphrase -infile file_path

nbhostidentity [-import | -testpassphrase] -help

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd

DESCRIPTION

The nbhostidentity command is used to import the master server identity after a disaster. You need to provide the file path and the file name of the disaster recovery package for the master server identity you want to restore.

Disaster recovery packages store the master server identity and are created during catalog backups. NetBackup requires the disaster recovery package to restore the master server identity after a disaster.

Note: Do not run the nbhostidentity command if you selected the disaster recovery mode during installation. In this scenario, the master server identity is automatically imported during the installation.

Run the nbhostidentity command on the master server after you install NetBackup to manually import the master server identity after a disaster.

The warning message that is shown is displayed when you run the command:

If new certificates are deployed on the media servers or clients after NetBackup master server installation, certificates on those hosts should be redeployed. To identify the hosts that need
certificate redeployment, go to NetBackup Administration Console > Host Properties > Clients.
This process requires you to restart the NetBackup services.
Are you sure you want to proceed (y/n)?
Read the warning message carefully and then specify the option.
Press N to terminate the command execution. Press Y to run the \texttt{nbhostidentity} command and restart the NetBackup services.
After you enter Y, you must provide the appropriate passphrase to decrypt the specified disaster recovery package. The host identity import operation fails if the passphrase does not match the one that you have set earlier.

\textbf{Note:} Ensure that the passphrase is same as what you set at the time of the catalog backup. The passphrase must be the same as the one that is associated with the specified disaster recovery package.

\section*{OPTIONS}

\texttt{-altdir directory_path}

The \texttt{-altdir} parameter specifies the alternate directory location where you want to restore the disaster recovery package.

\texttt{-import}

Specifies the path name and the file name of the disaster recovery package for the master server identity you want to restore.

The disaster recovery packages are stored in the same location as the disaster recovery files. This location is specified during the catalog backup policy configuration. The disaster recovery package name is same as disaster recovery file name. The extension for the disaster recovery package is \texttt{.drpkg}. You must use the \texttt{inifile} parameter with the \texttt{-import} option.

To run the \texttt{nbhostidentity -import} command, you must be an authorized user with system administrator or superuser privileges.

\texttt{-import -help}

Displays the command usage statement for the \texttt{-import} option.

\texttt{-inifile file_path}

The path name and the file name for the disaster recovery package you want to validate or import. This parameter is required for the \texttt{-import} and the \texttt{-testpassphrase} option. If you want to use a network share, you must specify a path to a subfolder on that share.
-mapuser
Maps the users or groups that are referenced in the disaster recovery package to the existing users or groups on the system. You can map more than one user or group.

This option must not be used along with the -noacls option.

-noacls
Lets you restore files without setting the Access Control List (ACL). This option is available only in case of the disaster recovery package restore to an alternate path.

testpassphrase
Used to confirm that the passphrase for a disaster recovery package is correct. You must be an authorized user with system administrator or superuser privileges to run the nbhostidentity -testpassphrase command.

Use of this option begins an interactive session where you are prompted to enter the passphrase for the specified disaster recovery package. The nbhostidentity command confirms the passphrase that is entered matches the one associated with the disaster recovery package. You must use the infile parameter with the -testpassphrase option.

testpassphrase -help
Displays the command usage statement for the -testpassphrase option.

-help
Displays the command usage statement for the nbhostidentity command.

EXAMPLES

Example of the nbhostidentity command to recovery a master server identity.

# nbhostidentity -import -infile /dr/nbu_dr_file/
cat_backup_1438271286_INCR.drpkg

Example of the -testpassphrase option with an invalid passphrase.

# ./nbhostidentity -testpassphrase -infile /test2.drpkg
Specify the passphrase that is associated with the disaster recovery package.
Passphrase:
The specified passphrase is not valid for the disaster recovery package - /test2.drpkg.
nbhostidentity command failed.

Example of the -testpassphrase option with a valid passphrase.
# ./nbhostidentity -testpassphrase -infile /test2.drpkg
Specify the passphrase that is associated with the disaster recovery package.
Passphrase:
The specified passphrase is valid for the disaster recovery package - /test2.drpkg.
Command is successfully carried out.

SEE ALSO

See nbseccmd on page 822.
nbhostmgmt

nbhostmgmt – used to manage host ID to host name mappings

SYNOPSIS

nbhostmgmt -add -hostid hostid | -host host -mappingname mappingname
[-isshared] [-reason reason] [-server master_server]

nbhostmgmt -addhost -host host [-reason reason] [-server master_server]

nbhostmgmt -allowautoreissuecert -hostid hostid | -host host
-autoreissue 0|1 [-reason reason] [-server master_server]

nbhostmgmt -delete -hostid hostid | -host host -mappingname
mappingname [-reason reason] [-server master_server]

nbhostmgmt -list [-short | -json | -json_compact] [-hostid hostid | -host host
| -approved | -pending | -conflict] [-server master_server]

nbhostmgmt -addcomment -hostid hostid | -host host -comment comment
[-server master_server]

nbhostmgmt -deletecomment -hostid hostid | -host host [-server master_server]

nbhostmgmt -updatehost -hostid hostid | -host host -newhostname
newhostname [-reason reason] [-server master_server]

nbhostmgmt -help

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The nbhostmgmt command is used to manage the host ID to host names or IP
addresses mappings. You can identify a host with alternate names. Use this
command to map these alternate names to the respective host IDs. Use the
command to add, delete, and list the mappings. Only the root user can run this
command.
Before you run the `nbhostmgmt` command, you must run the `bpnbat -login -loginType WEB` command. The `bpnbat` command authenticates your web services logon.

**OPTIONS**

`-add | -a`

Use this option to add and approve the host ID to host name or IP address mapping for the specified host.

**Note:** Use `-add` without the `-isshared` option to add the first share. Add all additional shares with the `-isshared` option.

`-addcomment | -ac`

Use this option to add a comment for the primary host. You can view the comment using the `nbhostmgmt -list` option. The added comment is only associated with the primary host and not with the alternate mapped host name. You cannot edit comments. You can only overwrite or delete the existing comment.

`-ah | -addhost`

Use this option to add a host in the host database.

The option lets you add the host entry so that the NetBackup administrator can set the `autoreissue` parameter. The `autoreissue` parameter lets you deploy certificate on the host without requiring a reissue token. During a Bare Metal Restore in an Auto Image Replication (AIR) setup, a host entry must be added in the host database of the target domain.

Veritas does not recommend manually adding a host except for specific scenarios like a Bare Metal Restore AIR setup.

`-aa | -allowautoreissuecert`

Use this option to set the `autoreissue` parameter for the specified host or host ID. The `autoreissue` parameter lets you deploy certificate on the host without requiring a reissue token. The `autoreissue` parameter is only associated with the primary host name and not with the alternate mapped name.

`-approved | -ap`

Use this option to list the mapped host names or IP addresses that are approved.

`-comment | -c`

Use this option to specify the content of the comment you want added to the primary host. You must specify either the host or the host ID to add a comment.
If the comment contains a space, you must enclose the comment in double quotation marks ("..."). The comment field is limited to 2048 characters.

- **conflict | -cf**  
  Use this option to list the mapped host names or IP addresses whose entries conflict with other mappings.

- **delete | -d**  
  Use this option to remove host ID to host name or IP address mapping.

- **deletecomment | -dc**  
  Use this option to remove a comment for the specified host or host ID. This option removes the comment that is associated with the primary host.

  If you attempt to delete a non-existent comment for a host with the `nbhostmgmt-deletecomment` option, the `nbauditreport` displays a corresponding entry for a successful update.

- **help | -h**  
  Displays the command-line usage message.

- **host | -n**  
  Specifies the primary host name or alternate mapped host name or IP address. For the add and the delete operation, ensure that the alternate mapped host name or IP address is associated with a single host ID.

- **hostid | -i**  
  Specifies the NetBackup host ID.

- **isshared | -is**  
  Indicates that you want to add the mapping name as shared.

---

**Note:** Use `-add` without the `-isshared` option to add the first share. Add all additional shares with the `-isshared` option.

---

- **json | -j**  
  This option generates the data in json format and spans multiple lines.

- **json compact | -jc**  
  This option generates the data in json format on a single line

- **list | -li**  
  Use this option to list mapped host names or IP addresses based on different filters. You can list based on approved, pending for approval, and conflicting names or addresses.
-mappingname | -hm
    Specifies the host name or the IP address you want to add or delete.

-newhostname | -nh
    Specifies the new primary host name for the host to be updated.

-pending | -p
    Use this option to list the mapped host names or IP addresses pending approval.

-reason | -r
    Use this option to specify the reason for the command action. The string that you enter is captured and appears in the audit report. Enclose this string with double quotes ("..."). The reason field is limited to 512 characters. It cannot begin with a dash character (-) and it cannot contain the single quotation mark (‘) character.

-server | -s
    Indicates the name of NetBackup Master server with which communication needs to be established. The default value for the -server option is the first server name listed in the bp.conf file.

-short | -l
    Use this option to list the host ID and mapped host names only.

-updatehost | -uh
    Use this option to update the primary host name of a host.

EXAMPLES

Example 1: Add a host ID to host name mapping.

```
# nbhostmgmt -add -hostid 0a0aa0a0-0000-0aa0-aa00-000a0a00a0a0
    -mappingname testhost1
testhost1 is successfully mapped to 0a0aa0a0-0000-0aa0-aa00-000a0a00a0a0.
```

Example 2: Add a host ID to host name mapping with the host name.

```
# nbhostmgmt -add -host testhost1 -mappingname testhost2
testhost2 is successfully mapped to 0a0aa0a0-0000-0aa0-aa00-000a0a00a0a0.
```

Example 3: Approve a pending mapping. This example shows the approval of the mapping of testhost3 for mapped host name host3.
#nbhostmgmt -add -host host3 -mappingname testhost3
testhost3 is successfully updated.

Example 4: Delete a host ID from the host name mapping with a host ID.

#nbhostmgmt -delete -hostid 0a0aa0a0-0000-0aa0-aa00-000a0a00a0a0 -mappingname testhost1
Mapping between testhost1 and 0a0aa0a0-0000-0aa0-aa00-000a0a00a0a0 is removed.

Example 5: Delete a host ID from the host name mapping with a host.

#nbhostmgmt -delete -host fs001 -mappingname testhost4
Mapping between testhost4 and 0a0aa0a0-0000-0aa0-aa00-000a0a00a0a0 is removed.

Example 6: Delete a host ID from the host name mapping with a host from the specified master server.

#nbhostmgmt -delete -server nbmaster01 -host fs001 -mappingname testhost3
Mapping between testhost3 and 0a0aa0a0-0000-0aa0-aa00-000a0a00a0a0 is removed.

SEE ALSO

See bpnbat on page 242.
nbhypervtool

nbhypervtool – NetBackup tool for Hyper-V

SYNOPSIS


On Windows systems, the directory path to this command is 
install_path\NetBackup\bin\

DESCRIPTION

The nbhypervtool utility removes orphaned NetBackup WMI checkpoints (snapshots) of a Hyper-V virtual machine on Windows 2016 or later.

This command operates only on Windows systems.

---

**Note:** For NetBackup 8.0: If a virtual machine checkpoint exists that NetBackup created for a previous WMI backup, NetBackup aborts the next WMI backup job for that virtual machine.

---

**Note:** This command does not apply to VSS snapshots.

---

OPTIONS

- **-d, -debug**
  Enables debug logging.

- **deleteNbuCheckpoints**
  Deletes the existing NetBackup WMI checkpoints of the virtual machine.

- **-h, -help**
  Displays the available options for nbhypervtool.

- **listNbuCheckpoints**
  Lists the existing NetBackup WMI checkpoints of the virtual machine.

- **-server Hyper-V_server_name**
  The name of the Hyper-V server. The default is the local host.
-version
   Displays the nbhypervtool version and exits.

-vmguid VM_guid
   The globally unique identifier (GUID) of the virtual machine.

-vmname VM_display_name
   The display name of the virtual machine.

EXAMPLES

Example 1 - List the existing NetBackup WMI checkpoints for a virtual machine by its display name:

nbhypervtool.exe listNbuCheckpoints -vmname VM1

Example 2 - List the existing NetBackup WMI checkpoints for a virtual machine by its GUID:

nbhypervtool.exe listNbuCheckpoints -vmguid 4c080c63-72b4-462b-b4b3-372e0f4cab04

Example 3 - Delete NetBackup WMI checkpoints for a virtual machine by its display name:

nbhypervtool.exe deleteNbuCheckpoints -vmname VM1

Example 4 - Delete NetBackup WMI checkpoints for a virtual machine by its GUID:

nbhypervtool.exe deleteNbuCheckpoints -vmguid 4c080c63-72b4-462b-b4b3-372e0f4cab04
nbidpcmd

nbidpcmd – configure an identity provider (IDP) on the NetBackup master server to use with the Single Sign-On (SSO) method.

SYNOPSIS

nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file [-t SAML2] [-e true | false] [-u IDP user field] [-g IDP user group field] [-M master_server]
nbidpcmd -dc -n IDP configuration name [-M master_server]
nbidpcmd -sc -n IDP configuration name [-M master_server]
nbidpcmd -scl [-M master_server]
nbidpcmd -uc -n IDP configuration name { -mxp IDP XML metadata file | -e true | false} [-M master_server]
nbidpcmd -v [-M master_server]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

The nbidpcmd command can add, modify, list, and delete the configuration for identity providers on the NetBackup master server.

OPTIONS

-ac

Adds a configuration for an identity provider. Use the -e option to enable an IDP configuration.

-dc

Deletes the configuration of the identity provider with the specified ID.
-e true | false

Enables or disables the identity provider configuration. An IDP must be available and enabled otherwise users cannot sign in with the Single Sign-On (SSO) option.

- true = Enable
- false = Disable

-M master_server

The master server to which you want to add or modify the identity provider configuration. The default is the NetBackup server master where you run the command.

-n IDP configuration name

The unique name of the identity provider.

-mxp IDP XML metadata file

The metadata file that contains configuration details for the identity provider, in Base64-encoded format.

-sc

Display the details for the configured identity provider with the specified ID. If the ID is not provided the details of all the configured identity providers are listed. Or, use -scl to display a specific identity provider.

-scl

Display the details for all the configured identity providers. Use -sc -n to display a specific identity provider.

-t SAML2

Indicates the type of protocol that the identity provider supports. The following types are supported: SAML2.

-u IDP user field, -g IDP user group field

Retrieves the fields from the SAML assertion that are the primary keys for the user and the user group. You can specify these fields together or individually.

-uc

Updates the details for the configured identity provider with the specified ID. In addition to the -n option, you must use the -mxp or the -e option, or both options.

-v

Shows the version of the nbidpcmd utility.
nbimageshare

nbimageshare – use this command to import the VM images and recover the VMs from one NetBackup domain to the Amazon Web Service.

SYNOPSIS

nbimageshare -login username password
nbimageshare -listimage
nbimageshare -singleimport client_name policy_name backupID
nbimageshare -batchimport image_list_file_path
nbimageshare -recovervm client_name policy_name backupID

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

This command is not available on Windows systems.

DESCRIPTION

The nbimageshare command is part of the automated disaster recovery solution that lets you import and restore backups images and turn on the VM images instantly.

OPTIONS

-batchimport image_list_file_path
  Import information about more than one backup images to NetBackup. The maximum number that is allowed is 64.

-listimage
  List the images from the Amazon Web Service (AWS) S3 bucket.

-login user_name password
  Enter the NetBackup logon credentials.

-recovervm client_name policy_name backupID
  Recover the virtual machine to an Amazon Machine Image (AMI) in AWS.

-singleimport client_name policy_name backupID
  Import a single backup image information to NetBackup.
nbinstallcmd

nbinstallcmd – used to create deployment jobs

SYNOPSIS

nbinstallcmd -policy policy_name -schedule schedule [-master_server hostname]  
[[-hosts hostname1,hostname2,... | -host_filelist path]]

nbinstallcmd -operation_type {precheck | stage | install} -package package_name  
[-master_server hostname] [-media_server hostname]  
{[-hosts hostname1,hostname2,... | -host_filelist path] [-limit_jobs max_concurrent_jobs]  
-use_existing_certs [-components javagui_jre=(include|exclude|match)]}

nbinstallcmd -operation_type {precheck | stage | install} -package package_name  
[-master_server hostname] [-media_server hostname]  
{[-hosts hostname1,hostname2,... | -host_filelist path] [-limit_jobs max_concurrent_jobs]  
-unix_eca_cert_path path -unix_eca_crl_check_level {use_cdp | use_path | disabled}  
-unix_eca_trust_store_path path -unix_eca_private_key_path path  
[-unix_eca_key_passphrasefile path] [-unix_eca_crl_path path]  
[-components javagui_jre=(include|exclude|match)]}

nbinstallcmd -operation_type {precheck | stage | install} -package package_name  
[-master_server hostname] [-media_server hostname]  
{[-hosts hostname1,hostname2,... | -host_filelist path] [-limit_jobs max_concurrent_jobs]  
-win_eca_cert_store path -win_eca_crl_check_level {use_cdp | use_path | disabled} [-win_eca_crl_path path]  
[-components javagui_jre=(include|exclude|match)]}

nbinstallcmd -operation_type {precheck | stage | install} -package package_name  
[-master_server hostname] [-media_server hostname]  
{[-hosts hostname1,hostname2,... | -host_filelist path] [-limit_jobs max_concurrent_jobs]  
-win_eca_cert_path path -win_eca_crl_check_level {use_cdp | use_path | disabled} [-win_eca_crl_path path]  
[-components javagui_jre=(include|exclude|match)]}

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin
DESCRIPTION

Use the nbinstallcmd command to create VxUpdate jobs. VxUpdate supports updates for clients and media servers. If you launch the job from a master server, it may target any client or any media server the master server knows. If you launch the job from a client or a media server, only that client or media server is targeted.

Use the -policy and -schedule options to base a job off an existing deployment policy. If the -hosts or -host_filelist switches are used with -policy, the job is limited to a subset of the target hosts configured in the deployment policy. If -hosts and -host_filelist are not used, the job is executed against all target hosts configured in the deployment policy.

Use the -operation_type and -package options to launch a job without a deployment policy. This form of the command requires you to provide information regarding security configuration. The command requires you specify how VxUpdate handles security:

- Configure external security certificates for UNIX and Linux hosts during the upgrade using a file-based certificate.
- Configure external security certificates for Windows hosts during the upgrade using a certificate from a certificate store.
- Configure external security certificates for Windows hosts during the upgrade using a file-based certificate.
- Do not modify the security, as it is configured correctly.

See the NetBackup Installation Guide and the NetBackup Security and Encryption Guide for more details on these security options.

Logs for the nbinstallcmd command are located in the legacy logging directory. For UNIX and Linux, the logs are found in /usr/openv/netbackup/logs. On Windows, the logs are in install_path\NetBackup\logs.

Note: Please use shell-specific annotations if any of the file paths in the arguments contain spaces or special characters that must be escaped.
OPTIONS

-components javagui_jre={include | exclude | match}

Use this option to specify if the Java GUI and JRE should be present on the target systems after the deployment job runs.

A value of include indicates that you want these components to be installed or upgraded on the target systems.

A value of exclude indicates that you do not want the components on the target systems. Any preexisting Java GUI and JRE components are removed.

A value of match indicates that you want to preserve the current state of the Java GUI and JRE components. The components are upgraded if they are present on the pre-upgraded system. The components are not installed if they are not present on the pre-upgraded system.

-hosts [host1,host2,...]

A comma-separated list of host names with no spaces between the entries. You cannot use this option with -host_filelist. If -policy is specified, the hosts that are listed must be included in the policy. If -policy is not specified and the command is executed on the master server, hosts specified must be known to the master server. If -policy is not specified and the command is executed on the target host, this value must match the name of the target host. You cannot specify a mixture of clients and media servers in a single job. All hosts that are listed in a job must either be all clients or all media servers.

-host_filelist [path]

Path to a file with the host names specified on individual lines. You cannot use this option with -hosts. If -policy is specified, the hosts that are specified must be included in the policy. If -policy is not specified and the command is executed on the master server, the hosts that are specified must be known to the master server. If -policy is not specified and the command is executed on the target host, this value must match the name of the target host. You cannot specify a mixture of clients and media servers in a single job. All hosts that are listed in the file must either be all clients or all media servers.

-limit_jobs [max_concurrent_jobs]

The maximum number of concurrent jobs allowed. This option applies only when -policy is not specified. If unspecified, the default value is unlimited.

-master_server hostname

The host name of the master server where the VxUpdate repository exists. This option is not required.
-media_server hostname

The host name of the staging server with which the client communicates. This server must be a media server. This option applies only when -policy is not specified. If unspecified, the master server acts as the staging server. When a media server is used for staging, the packages are cached to it so that it can serve these packages in VxUpdate operations. This option helps optimize the efficiency of the NetBackup master server.

-operation_type {precheck | stage | install}

The type of deployment operation to launch. Required if -policy is not specified. Valid options are:

- precheck: Performs the various precheck operations, including confirming there is sufficient space on the host for the update.
- stage: Moves the update package to the host, but does not install it. Also performs the precheck operation.
- install: Installs the specified package. Also performs the precheck and the stage operations. If you already performed the stage operation, the install command does not move the package again.

-package item

The name of the package you want installed. Required if -policy is not specified. The package must be present in the repository. Use the nbrepo command to view and manage packages.

-policy policy_name

The name of an existing deployment policy. This option is required if -operation_type isn’t specified.

-schedule schedule_name

The deployment policy’s schedule to execute. Required if -policy is specified.

-unix_eca_cert_path path

Use this option to specify the path to the certificate file for UNIX and Linux hosts. This option applies when:

- -policy and -use_existing_certs are not specified.
- The master server supports external security certificates.
- The target hosts do not yet have external security certificates configured.
- You want the configuration to occur during the upgrade.

-unix_eca_crl_check_level {use_cdp | use_path | disabled}

Specifies how you want to handle the Certificate Revocation List on UNIX and Linux hosts. Specify use_cdp to use the CRL defined in the certificate. Specify
use_path to specify the path to the CRL. Specify disabled to not use a CRL.

Applies when:

- `-policy` and `-use_existing_certs` are not specified.
- The master server supports external security certificates.
- Your target hosts do not yet have external security certificates configured.
- You want that configuration to occur during the upgrade.

`-unix_eca_crl_path path`

Use this option to specify the path to the external certificate authority file for UNIX and Linux hosts. This option is required if you use `-unix_eca_crl_check_level use_path`. If you attempt to use this option without `-unix_eca_crl_check_level use_path`, the job fails.

- `-policy` and `-use_existing_certs` are not specified.
- The master server supports external security certificates.
- Your target hosts do not yet have external security certificates configured.
- You want that configuration to occur during the upgrade.

`-unix_eca_key_passphrasefile path`

Use this option to provide the path to the passphrase file on UNIX and Linux hosts. This option is not required. This option applies when:

- `-policy` and `-use_existing_certs` are not specified
- The master server supports external security certificates
- Your target hosts do not yet have external security certificates configured.
- You want that configuration to occur during the upgrade.

`-unix_eca_private_key_path path`

Use this option to specify the path to the private key file and the private key file name on UNIX and Linux hosts. This option applies when:

- `-policy` and `-use_existing_certs` are not specified
- The master server supports external security certificates.
- Your target hosts do not yet have external security certificates configured.
- You want that configuration to occur during the upgrade.

`-unix_eca_trust_store_path path`

Use this option to specify the path to the trust store file on UNIX and Linux hosts. This option applies when:

- `-policy` and `-use_existing_certs` are not specified
-use_existing_certs

Specify this option when you want the job to use the existing security certificates. This option only applies when -policy is not specified. You cannot use this option with any *eca* option. Specify this option if:

- The target hosts have existing external certificates.
- The target hosts have existing NetBackup security certificates you want to continue to use.

-win_eca_cert_path path

Use this option to specify the path to the certificate file for Windows hosts. You cannot use this option with -win_eca_cert_store_path. This option applies when:

- -policy and -use_existing_certs are not specified
- The master server supports external security certificates.
- Your target hosts do not yet have external security certificates configured.
- You want that configuration to occur during the upgrade.

-win_eca_cert_store path

Use this option to specify the path to the Windows certificate store. You cannot use this option with -win_eca_cert_path, -win_eca_key_passphrasepath, -win_eca_private_key_path, and -win_eca_trust_store_path. You must enter the certificate location as Certificate_Store_Name\Issuer_Distinguished_Name\Subject_Distinguished_Name. This option applies when:

- -policy and -use_existing_certs are not specified
- The master server supports external security certificates.
- Your target hosts do not yet have external security certificates configured.
- You want that configuration to occur during the upgrade.

-win_eca_crl_check_level {use_cdp | use_path | disabled}

Specifies how you want to handle the Certificate Revocation List on Windows hosts. Specify use_cdp to use the CRL defined in the certificate. Specify use_path to specify the path to the CRL. Specify disabled to not use a CRL. This option applies when:
-policy and -use_existing_certs are not specified
- The master server supports external security certificates.
- Your target hosts do not yet have external security certificates configured.
- You want that configuration to occur during the upgrade.

-win_eca_crl_path path
Use this option to specify the path to the external certificate authority file for Windows hosts. This option is required if you use -windows_eca_crl_check_level use_path. If you attempt to use this option without -windows_eca_crl_check_level use_path, the job fails.

-win_eca_key_passphrasefile path
Use this option to provide the path to the passphrase file on Windows hosts. This option is not required. You cannot use this option with -win_eca_cert_store. This option applies when:
- -policy and -use_existing_certs are not specified
- The master server supports external security certificates.
- Your target hosts do not yet have external security certificates configured.
- You want that configuration to occur during the upgrade.

-win_eca_private_key_path path
Use this option to specify the path to the private key file and the private key file name on Windows hosts. You cannot use this option with -win_eca_cert_store. This option applies when:
- -policy and -use_existing_certs are not specified
- The master server supports external security certificates.
- Your target hosts do not yet have external security certificates configured.
- You want that configuration to occur during the upgrade.

-win_eca_trust_store_path path
This option lets you specify the path to the trust store and the trust store file name on Windows hosts. You cannot use this option with -win_eca_cert_store. This option applies when:
- -policy and -use_existing_certs are not specified
- The master server supports external security certificates.
- Your target hosts do not yet have external security certificates configured.
- You want that configuration to occur during the upgrade.
EXAMPLES

Example 1: Initiate a precheck operation for all hosts that are configured in the specified policy.

```plaintext
nbinstallcmd -policy policy-deployment20 -schedule sched-precheck -master_server master.domain.com
```

Example 2: From the master server, initiate a staging job that is not based on a deployment policy. The job should: stage the NetBackup 8.2 client, target several hosts, use a separate media server as the staging server, and not include any security certificate configuration.

```plaintext
nbinstallcmd -operation_type stage -package nbclient_8.2 -master_server master.domain.com -media_server media_staging.domain.com -hosts client01.domain.com,client02.domain.com -use_existing_certs
```

Example 3: From the target host, initiate an install operation that is not based on a deployment policy. The operation upgrades the host to NetBackup 8.3 with instructions to configure external security certificates as part of the upgrade.

```plaintext
nbinstallcmd -operation_type install -package nbserver_8.3 -master_server master.domain.com -hosts media01.domain.com -unix_eca_cert_path /usr/home/cert.pem -unix_eca_trust_store_path /usr/home/cacert.pem -unix_eca_private_key_path /usr/home/private_key.pem -unix_eca_key_passphrasefile /usr/home/passphrase_file -unix_eca_crl_check_level use_path -unix_eca_crl_path /usr/home/crl_dir
```

Example 4: From the target host, initiate an install operation not based on a deployment policy. The operation upgrades the host to NetBackup 8.3 using a separate media server as the staging server. It also includes instructions to configure external security certificates originating from a certificate store.

```plaintext
nbinstallcmd -operation_type install -package nbclient_8.3 -master_server master.domain.com -media_server media_staging.domain.com -hosts client01.domain.com -win_eca_cert_store MyCertStore\MyIssuer\MyClient -win_eca_crl_check_level use_cdp
```

Example 5: From the master server, initiate an install operation not based on a deployment policy. The operation applies a NetBackup 8.2 Windows EEB and targets several hosts. The job uses the master server as the staging server and does not include any security certificate configuration.

```plaintext
nbinstallcmd -operation_type install -package nbclient_8.3 -master_server master.domain.com -hosts client01.domain.com -win_eca_cert_store MyCertStore\MyIssuer\MyClient -win_eca_crl_check_level use_cdp
```
nbinstallcmd -operation_type install -package nbeeb_1234567.1_8.2 -master_server master.domain.com -host_filelist path_to_file.txt -use_existing_certs

**SEE ALSO**

See nbrepo on page 800.
nbjm

nbjm – run NetBackup Job Manager to submit jobs and acquire resources to start jobs

SYNOPSIS

```
nbjm [-console] [-terminate]
```

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\

DESCRIPTION

The NetBackup Job Manager binary (`nbjm`) service starts when NetBackup is started, and it remains active. The primary function of this binary is to accept the jobs that `nbpem` submitted, acquire the resources to run them, and then start the job. This service then waits for the completion of a job and sends a signal to `nbpem` when a job completes. This service also handles all IRM communications to `bpjobd` for Activity Monitor information, external resource requests, and it writes to the progress log.

OPTIONS

- **-console**

  This option enables you to start NetBackup in console mode.

- **-terminate**

  This option accepts an option parameter, which is the number of seconds to wait for jobs to finish before it terminates. The default is 60 seconds. If you enter a value of 0, `nbjm` waits until all jobs complete before it terminates. If a limit is placed on the termination, after that limit is reached, `nbjm` terminates without waiting for the completion of jobs.

SEE ALSO

See `nbpem` on page 774.

See `nbrb` on page 788.
**nbkmiputil**

nbkmiputil – executes the various external KMS server operations.

**SYNOPSIS**

```
```

```
```

```
nbkmiputil -setAttribute -kmsServer kms_server_name -port kms_server_port -trustStorePath CA_certificate_file_path -certPath certificate_file_path -privateKeyPath private_key_file_path -keyId key_ID -attributeName attributeName -attributeValue attribute_value [-passphrasePath private_key_passphrase_file_path] [-crlCheckLevel LEAF | CHAIN | DISABLE] [-connectTimeout time_in_seconds] [-requestTimeout time_in_seconds] [-kmipVersion version] [-jsonCompact]
```

```
```
nbkmiputil -ekmsCheckCompat -kmsServer kms_server_name -port kms_server_port -trustStorePath CA_certificate_file_path -certPath certificate_file_path -privateKeyPath private_key_file_path [-passphrasePath private_key_passphrase_file_path] [-crlCheckLevel LEAF | CHAIN | DISABLE] [-kmipVersion version] [-jsonCompact]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/goodies/
On Windows systems, the directory path to this command is install_path\NetBackup\bin\goodies\

DESCRIPTION

The nbkmiputil executes the various external KMS server operations like retrieving keys, listing key IDs, setting key attributes, and validating KMS servers.

The command supports the following operations:

-ekmsCheckCompat Use -ekmsCheckCompat to determine if NetBackup is compatible with the specified external KMS server. You can also use this option to determine if the following KMIP operations are supported on the external KMS server: Discover supported versions; create, get, or locate keys; and get, set, modify, or delete attributes.

-getKey Fetches the NetBackup keys from the external KMS server.

-listKeyIDs Lists NetBackup key IDs that are present in the external KMS server as per the specified options.

-setAttribute Sets the custom attribute for the given key in the external KMS server. Supported attribute names are x-application, x-keygroup, and x-comment.

-validate Validates the related functionality with the external KMS server. The functionality that is validated includes:
  - Connecting to the external KMS server.
  - Listing NetBackup key IDs present in the external KMS server.
  - Fetch the key for any active NetBackup key ID.
  - Fetch and set the attributes on any NetBackup key ID.
OPTIONS

- activeKey
  Specifies whether to list only active NetBackup keys.

- attributeName
  Specifies the custom attribute name to be set. Supported attribute names are
  x-application, x-keygroup, and x-comment.

- attributeValue
  Specifies the custom attribute value to be set. Supported attribute value for
  attribute x-application : NetBackup.

- certPath
  Specifies the path of the PEM-encoded certificate that is to be used for
  authentication with the external KMS server.

- connectTimeout
  Specifies the time-out value to connect to the external KMS server in seconds.
  The default value is 120 seconds.

- crlCheckLevel
  Specifies the CRL check level. The possible values are: LEAF, CHAIN, and
  DISABLE. The default value is LEAF.
  ■ LEAF - Revocation status of peer's leaf certificate is checked.
  ■ CHAIN - Revocation status of full chain of peer certificate is checked.
  ■ DISABLE - Revocation status of peer certificate is not checked.

- getDetails
  Displays the additional key attributes details for the NetBackup keys.

- jsonCompact
  Specifies whether to display the output in JSON compact form.

- kad
  Specifies the key associated data (KAD) of the NetBackup key to be fetched
  from the external KMS server.

- kadLength
  Specifies the length up to which KAD of a NetBackup key is to be generated.

- keyId
  If -keyId is used with the -getKey option, it specifies the key ID of the
  NetBackup key to be fetched from the external KMS server. If it is used with
  the -setAttribute option, it specifies the key ID of the key for which a custom
  attribute is to be set.
-kmsServer
  Specifies the external KMS server name with which you want to connect.

-kmipVersion version
  Specifies the KMIP version to be used. Supported KMIP versions: 1.0, 1.1, 1.2, 1.3, 1.4, and 2.0.

-maxItems
  Specifies the maximum number of key IDs to be listed.

-nbKeyGroup
  If it is used with the -getKey option, it specifies the key group name whose active and latest key is to be fetched from the external KMS server. If it is used with the -listKeyIDs option, it specifies the key group name for which keys are to be listed.

-offset
  Specifies the offset number of the key ID from where the list of key IDs starts. The default value is 0.

-passphrasePath
  Specifies the path of the file containing the passphrase that is required to access the keystore for authentication with the external KMS server.

-port
  The port number in use by the external KMS server.

-privateKeyPath
  Specifies the path of the private key that is to be used for authentication with the external KMS server.

-requestTimeout
  Specifies the time-out value for the given request to external KMS server in seconds. Default value is 300 seconds.

-trustStorePath
  Specifies the path of the PEM-encoded CA certificate that is to be used for authentication with the external KMS server.

EXAMPLES

Example 1: Set custom attributes for the external KMS.

nbkmiputil -setAttribute -kmsServer example.veritas.com -port 5696 -certPath /usr/cert.pem -privateKeyPath /usr/key.pem -trustStorePath /usr/ca.pem -keyId EFF18E49-DBBF-4F84-BF94-13F4A6B6E32B -attributeName x-keygroup -attributeValue msdp
nbkmscmd

nbkmscmd – configures the key management service (KMS) in NetBackup.

SYNOPSIS

nbkmscmd -configureCredential -credName credential_name -certPath certificate_file_path -privateKeyPath private_key_file_path -trustStorePath CA_certificate_file_path [-passphrasePath private_key_passphrase_file_path] [-crlCheckLevel LEAF | CHAIN | DISABLE] [-server master_server_name] [-description description] [-force]

To configure NetBackup KMS (NBKMS):

nbkmscmd -configureKMS -name configuration_name -type NBKMS -hmkId host_master_key_ID_to_identify_HMK_passphrase -kpkId key_protection_key_ID_to_identify_KPK_passphrase [-useRandomPassphrase 0 | 1] [-enabledForBackup 0 | 1] [-priority priority_of_KMS_server] [-server master_server_name] [-description description]

To configure external KMS:

nbkmscmd -configureKMS -name configuration_name -type KMIP -port port_to_connect_to_external_KMS_server -kmsServerName network_name_of_external_KMS_server -credId credential_ID | -credName credential_name [-enabledForBackup 0 | 1] [-priority priority_of_KMS_server] [-server master_server_name] [-description description]

nbkmscmd -createKey -name configuration_name -keyName name_of_the_key_to_be_created -keyGroupName key_group_name [-algorithm key_algorithm] [-comment comment_about_the_key] [-keyPassphraseFilePath file_path_of_the_key_passphrase] [-reason reason] [-server master_server_name]

nbkmscmd -deleteCredential -credName credential_name | -credId credential_ID [-force] [-server master_server_name]

nbkmscmd -deleteKMSConfig -name configuration_name [-server master_server_name] [-reason reason_for_deleting] [-force]

nbkmscmd -discoverNBKMS

nbkmscmd -listCredential [-credName credential_name | -credId credential_ID] [-server master_server_name] [-jsonCompact] [-jsonRaw]
To update NetBackup KMS (NBKMS) configuration:

```
nbkmscmd -updateKMSConfig -name configuration_name [-server master_server_name] [-priority priority_of_KMS_server] [-enabledForBackup 0 | 1] [-description description]
```

To update external KMS configuration:

```
```

```
nbkmscmd -validateKMSConfig -name configuration_name [-jsonRaw]
```
On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\

DESCRIPTION

The nbkmscmd command is used to configure KMS. You can also create KMS credentials and keys. All of these commands require NetBackup administrator privileges to run. Additionally, these operations require a bpnbat web log-on (bpnbat -login -loginType WEB) using an account that has NetBackup administrator privileges.

The nbkmscmd supports the following operations:

-configCredential  Adds the KMS configuration credential in the NetBackup database. The credential ID and its credential name are added in the database. These credentials are used to connect to external KMS.

-configureKMS  Adds an entry for the KMS configuration in the NetBackup database.

-createKey  Creates an active NetBackup key in the KMS server that is associated with the provided configuration name. To create key, KMS server should allow NetBackup to create key and to set NetBackup attributes on that key.

For NetBackup KMS (NBKMS), If the specified key-group name does not exist then the key-group is created with specified algorithm.

-deleteCredential  Deletes the specified KMS configuration credential from the NetBackup database.

-deleteKMSConfig  Deletes the KMS configuration entry from the NetBackup database.

-discoverNBKMS  Discovers whether the NetBackup KMS (NBKMS) is configured and running and adds it to NetBackup database.

-listCredential  Lists the details of the specified KMS configuration credential in JSON format. If the credential name or ID is not specified, credential details for all KMS configurations are listed.

-listKeys  Lists the NetBackup keys from the specified KMS configuration in JSON format.
-listKMSConfig Lists the details of the specified KMS configuration in JSON format. If the configuration name is not provided, this operation lists the configuration details of all KMS.

-precheckKMSConfig Performs a dry run of KMS configuration operations to validate the required connections and setup.

-updateCredential Updates the specified KMS configuration credential.

-updateKMSConfig Updates the specified KMS configuration in the NetBackup database.

-validateKMSConfig Validates the functionality with the specified KMS configuration and ensures that backup and restore functionality works.

OPTIONS

-algorithm algorithm
   Specifies the encryption algorithm for the key created.

-certPath certificate_file_path
   Specifies the path of the certificate that is used to connect to the remote server.

-comment comment
   Specifies a comment about the key.

-credId credential_ID
   Specifies the credential ID of the KMS configuration.

-credName credential_name
   Specifies the credential name of the KMS configuration.

-crlCheckLevel LEAF | CHAIN | DISABLE
   Specifies the revocation check level for certificates of the external KMS server. The default value is LEAF.

   Accepted values for CRL check level are:
   DISABLE: Revocation check is disabled. The revocation status of the certificate is not validated against the CRL during host communication.
   LEAF: The revocation status of the leaf certificate is validated against the CRL.
   CHAIN: The revocation status of all the certificates from the certificate chain are validated against the CRL.

-description description
   Used to provide further information about the current operation.
-enabledForBackup 0 | 1
   Specifies whether keys from this KMS should be used for backup or not. The default value is 1.
   Provide 0 if the keys from this KMS should not be used for backup.

-force
   Suppresses the confirmation prompts and performs the specified operation.

-hmkId host_master_key_ID_to_identify_HMK_passphrase
   Specifies the host master key (HMK) ID to identify HMK passphrase. This option is only applicable if the KMS type is NBKMS.

-jsonCompact
   Generates output data in a compacted JSON format.

-jsonRaw
   Displays the JSON response of the web server.

-keyGroupName key_group_name
   Specifies the name of the key group that is used to retrieve or set keys.

-keyName key_name
   Specifies the name of the key.

-keyPassphraseFilePath file_path_of_the_key_passphrase
   Specifies the file path that has the passphrase that is used to create the key. Not all KMS types support key passphrase.

-kmsServerName network_name_of_external_KMS_server
   Specifies the network name for the KMS server. If there are multiple network names for the KMS server, separate the names with a comma (,). This option is only applicable if the KMS type is KMIP.

-kpkId key_protection_key_ID_to_identify_KPK_passphrase
   Specifies the key protection key (KPK) ID to identify KPK passphrase. This option is only applicable if KMS type is NBKMS.

-name configuration_name
   Specifies a unique name for the KMS configuration.

-pageLimit number_of_records_to_be_listed after_offset
   Specifies the number of records to be listed after the offset. Valid values for -pageLimit are 1 to 100. The default value is 100.

-pageOffset record_number
   Specifies the record number from where the records start listing. The default value is 0.
-passphrasePath private_key_passphrase_file_path
  Specifies the file path of the passphrase that is used to encrypt the certificate private key.

-port port_to_connect_to_external_KMS_server
  Specifies the port number to be used to connect to external KMS server. This option is only applicable if KMS type is KMIP.

-priority priority_of_KMS_server
  Specifies the KMS server to be used when NetBackup checks for keys during encryption or decryption. By default, the KMS server priority is set to 0. A KMS server with the highest value gets the first priority to be used during encryption or decryption.

-privateKeyPath private_key_file_path
  Specifies the file path for the certificate private key.

-reason reason
  Specifies the reason to perform the current operation.

-server master_server_name
  Specifies an alternate master server. By default, this command uses the first server entry in the NetBackup configuration file.

-trustStorePath CA_certificate_file_path
  Specifies the file path for the CA certificate that is used to verify the remote server.

-type NBKMS | KMIP
  Specifies the KMS type. NBKMS and KMIP are the valid KMS types.

-useRandomPassphrase 0|1
  Specifies whether random passphrases should be used or not. The default value is 0. Provide 1 if random passphrases should be used for KMS configuration.

EXAMPLES

Example 1: Configure credential for External KMS

nbkmscmd -configureCredential -credName ExtKMS_Credential -certPath /EKMS_creds/cert_chain.pem -privateKeyPath /EKMS_creds/key.pem -trustStorePath /EKMS_creds/cacerts.pem -description "Configuring credential for external KMS"

Example 2: Configure external KMS.
nbkmscmd -configureKMS -name ExtKMS -type KMIP
-kmsServerName extkms.veritas.com -port 5696
-credName ExtKMS_Credential -priority 1 -description
"Configuring external KMS with configuration name ExtKMS"
nbkmsutil

nbkmsutil – run the NetBackup Key Management Service utility

SYNOPSIS

[-recoverkey] [-unquiescedb]

nbkmsutil -createkey [ -nophrase ] -kgname key_group_name -keyname
key_name [ -activate ] [ -desc description ]

nbkmsutil -createkg -kgname key_group_name [ -cipher type ] [ -desc
description ]

nbkmsutil -deletekey -keyname key_name -kgname key_group_name

nbkmsutil -deletekg -kgname key_group_name

nbkmsutil -export -path secure_key_container [-key_groups
key_group_name_1 ... | -key_file key_file_name]

nbkmsutil -gethmkid

nbkmsutil -getkpkid

nbkmsutil -import -path secure_key_container [-preserve_kgname] [-desc
description] [-preview]

nbkmsutil -ksstats [-noverbose]

nbkmsutil -listkeys -kgname key_group_name [ -keyname key_name | -activekey ] [ -verbose ]

nbkmsutil -listkgs [ -kgname key_group_name | -cipher type | -emptykgs | -noactive ] [ -verbose ]

nbkmsutil -modifyhmk [ -nophrase ]

nbkmsutil -modifykey -keyname key_name -kgname key_group_name [ -state
new_state | -activate ] [ -name new_keyname ] [ -desc new_description ]

nbkmsutil -modifykg -kgname key_group_name [ -name new_key_group_name ] [ -desc new_description ]

nbkmsutil -modifykpk [ -nophrase ]
nbkmsutil -quiescedb

nbkmsutil -recoverkey -keyname key_name -kgnamekey_group_name -tag key_tag [-desc description]

nbkmsutil -unquiescedb

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd

DESCRIPTION

The nbkmsutil command performs the following operations:

-creakey
Create a new key. The default state of the new key is Prelive.

-createkg
Create a new key group. The default cipher of the new key group is AES_256.

-deletekey
Delete a key. Only keys in Prelive and Terminated states can be deleted.

-deletekg
Delete an empty key group.

To force the delete of a key group that is not empty, use the -force option.

# nbkmsutil -deletekg -kgname key_group_name -force

-export
Exports keys and key groups across domains

-gethmkid
Return the current HMK ID.

-getkpkid
Returns the current KPK ID.

-import
Imports keys and key groups across domains

To preview the results of the import option, use -preview.

# nbkmsutil -import -path secure_key_container -preview

-ksstats
Returns the keystore statistics. The statistics consist of the number of key groups, the total number of keys, and the outstanding quiesce calls.
-listkeys
Get the details of keys.

-listkgs
Get the details of the key groups. If no option is specified, retrieve the details of all the key groups.

-modifyhmk
Modify the host master key (HMK). HMK is used to encrypt the keystore. To modify the HMK, provide an optional seed (passphrase) and an HMK ID which can remind the user of the specified passphrase. The passphrase and the HMK ID are both read interactively.

-modifykey
Modify key attributes.

-modifykg
Modify key group attributes.

-modifykpk
Modify the key protection key (KPK). KPK is used to encrypt KMS keys. KPK is per keystore. To modify the KPK, provide an optional seed (passphrase) and a KPK ID which can remind the user of the specified passphrase. The passphrase and the KPK ID are both read interactively.

-quiescedb
Sends a quiesce request to KMS. If the command succeeds, the current outstanding quiesce count is returned (as multiple backup jobs might quiesce the KMS DB to back it up)

-recoverkey
Restore could fail if a key used in encrypting the backup data is lost. Such Keys can be recovered (re-created) with the knowledge of the original Key's attributes (tag and passphrase).

-unquiescedb
Sends an unquiesce request to KMS. If the command succeeds, the current outstanding quiesce count is returned. A count of zero (0) means that the KMS database is completely unquiesced.

OPTIONS

The nbkmsutil command uses the following options:

-activate
Sets the state of the specified key to active. The default state is prelive.

-activekey
Retrieves the details of a specific key group's active key.

-cipher
The type of cipher that the key group supports. All keys that belong to a key group support the same cipher type. Supported cipher types are BLOW, AES_128, AES_192, and AES_256 (default cipher).
-emptykgs  Retrieves the details of all the key groups with zero keys in it.

-keyname  key_name specifies the name of a key. This name should be unique within a key group. The key group name and key name uniquely identify a key in the keystore.

-kgname  key_group_name specifies the name of a key group. Within a keystore, the key group name uniquely identifies the key group.

-name  Specifies the new name of the key group when used with -modifykg or the new name of the key when used with -modifykey. The new key group name must not conflict with other names in the keystore.

-noactive  Retrieves the details of all the key groups in which there are no active keys.

-nophrase  Disables the utility function that prompts you for a pass phrase. Instead, the utility creates the key. The default condition is the use of the pass phrase to create a key with a seed. A lengthy seed and a strong seed results in a strong key.

-noverbose  Disables verbosity. The default condition is verbosity, which prints the details in readable format.

-state  new_state specifies the new state of the Key. Possible states are Prelive, Active, Inactive, Deprecated, and Terminated.

Key states can be changed only in the following ways:

- Prelive to Active
- Transition between Active and Inactive
- Transition between Inactive and Deprecated
- Transition between Deprecated and Terminated

-tag  key_tag specifies a random unique identifier that is created for the key record that the utility creates. The listkey option can display this tag. If you need to recover (recreate) the key record, you need to use the original tag value, hence the –tag option for these recovery options.
**nboraadm**

**nboraadm** – set up instances and instance groups as part of an Oracle backup policy

**SYNOPSIS**

```
nboraadm [-S master_server] -list_rac_dbs [{-rac_dbid dbid
-rac_db_unique_name name} [-rac_type type] [-scan_name name]
[-service_name name] [-port number] [-active | -inactive] [-registered
| -unregistered]
```

```
nboraadm [-S master_server] -list_rac_instances [instance_name]
[{-rac_dbid dbid -rac_db_unique_name name}] [-host name] [-backup_host
name] [-os Unix | Windows] [-active | -inactive] [-registered
| -unregistered]
```

```
nboraadm [-S master_server] -add_rac_db -rac_dbid dbid
-rac_db_unique_name name -rac_type type -scan_name name -service_name
name -port number [-load_balanced_node_count number]
```

```
nboraadm [-S master_server] -add_rac_instance instance_name -rac_dbid
dbid -rac_db_unique_name name -host name -oracle_home oracle_home
[-backup_priority priority] [-backup_host name]
```

```
nboraadm [-S master_server] -delete_rac_db -rac_db_unique_name name
[-rac_dbid dbid] [-scan_name name]
```

```
nboraadm [-S master_server] -delete_rac_instance instance_name [-host
name] [-backup_host name] [-rac_dbid dbid] [-rac_db_unique_name name]
[-oracle_home oracle_home]
```

```
nboraadm [-S master_server] -modify_rac_db -rac_dbid dbid
-rac_db_unique_name name [-new_scan_name name] [-rac_type type]
[-load_balanced_node_count number] [-port number] [-scan_name name]
[-service_name name] {{-oracle_auth user [-oracle_TNS tns] | 
-disable_oracle_auth] | [-wallet_path path [-wallet_rman_TNS tns | 
-disable_rman_catalog] | -disable_wallet_auth] [-rman_catalog_user
name [-rman_catalog_TNS tns] | -disable_rman_catalog] [-active
| -inactive] [-force] [-no_warnings]
```

```
nboraadm [-S master_server] -register_rac_db -rac_db_unique_name name
[-scan_name name] [-rac_dbid dbid] {-oracle_auth user | -wallet_path
path [-wallet_rman_TNS tns]} [-rman_catalog_user name
[-rman_catalog_TNS tns]] [-add_rac_dbid dbid] [-force] [-no_warnings]
```
nboraadm [-S master_server] -modify_rac_instance instance_name
  -rac_dbid dbid -rac_db_unique_name name [-new_instance instance_name]

nboraadm [-S master_server] -list_instance_aliases [instance_name]
  [-host name] [-oracle_home oracle_home]

nboraadm [-S master_server] -add_instance_alias instance_name -alias alias_name [-host name] [-oracle_home oracle_home]

nboraadm [-S master_server] -delete_instance_alias instance_name
  -alias alias_name [-host name] [-oracle_home oracle_home]

nboraadm [-S master_server] -list_instances [instance_name]
  [-instance_group name] [-host name] [-os Unix | Windows] [-active | -inactive] [-registered | -unregistered]

nboraadm [-S master_server] -add_instance_instance_name -host name
  -oracle_home oracle_home [-tns_admin tns_admin] {[-instance_group name] | [-os_user name [-os_domain name]] | [-oracle_auth user [-oracle_TNS tns]] | [-wallet_path path -wallet_TNS tns [-wallet_rman_TNS tns]]} [-rman_catalog_user name [-rman_catalog_TNS tns]] [-force]

nboraadm [-S master_server] -register_instance instance_name [-host name]
  [-oracle_home oracle_home] {[-instance_group name] | [-os_user name [-os_domain name]]} [-oracle_auth user [-oracle_TNS tns] | -wallet_path path -wallet_TNS tns [-wallet_rman_TNS tns]]
  [-rman_catalog_user name [-rman_catalog_TNS tns]] [-no_warnings] [-force]

nboraadm [-S master_server] -delete_instance instance_name [-host name] [-oracle_home oracle_home] [-no_warnings]

nboraadm [-S master_server] -modify_instance instance_name
  [-new_instance instance_name] [-host name] [-new_host name]
nboraadm [-S master_server] -remove_from_instance_group instance_name
[-instance_group name] [-host name] [-oracle_home oracle_home]
[-no_warnings]

nboraadm [-S master_server] -list_instance_groups
[instance_group_name]

nboraadm [-S master_server] -add_instance_group instance_group_name
{{-unix_os_user name AND/OR -windows_os_user name -os_domain name}
| [-oracle_auth user [-oracle_TNS tns]] | [-wallet_path path
-wallet_TNS tns [-wallet_rman_TNS tns]]} [-rman_catalog_user name
[-rman_catalog_TNS tns]]

nboraadm [-S master_server] -delete_instance_group instance_group_name

nboraadm [-S master_server] -modify_instance_group instance_group_name
[-new_instance_group instance_group_name] {{[-unix_os_user name]
[-windows_os_user name -os_domain name] | -disable_os_user]
[-oracle_auth user [-oracle_TNS tns] | -disable_oracle_auth] | 
[-wallet_path path -wallet_TNS tns [-wallet_rman_TNS tns | 
-disable_wallet_auth]] [-rman_catalog_user name [-rman_catalog_TNS tns] | -disable_rman_catalog] [-validate]

nboraadm [-S master_server] -auto_registration instance_group_name
[-unix_tns_admin tns_admin] [-windows_tns_admin tns_admin]

nboraadm [-S master_server] -disable_auto_registration

nboraadm [-S master_server] -list_dbas

nboraadm [-S master_server] -add_dba client_name user_name

nboraadm [-S master_server] -delete_dba client_name user_name

nboraadm [-S master_server] -immediate -policy policy [-schedule
schedule] {{-instance instance | {-rac_dbid dbid -rac_db_unique_name
name}} [-w[hh:mm:ss]]}

nboraadm [-S master_server] -list_jobs [count] [-utc]

nboraadm [-S master_server] -list_job_details -jobid jobid [-utc]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\
DESCRIPTION

The nboraadm command can add, modify, list, and remove RAC databases, instances, and instance groups as part of an Oracle backup policy. If you modify an instance that is not local to the host where you ran nboraadm, a prompt asks you if you want to change the instance. The nboraadm command performs the following operations:

- `list_instances` lists all Oracle instances in the repository.
- `add_instance` adds an instance to the repository.
- `register_instance` registers credentials for an instance or an instance group.
- `delete_instance` deletes an instance.
- `modify_instance` changes the attributes of the specified instance.
- `list_instance_groups` lists all Oracle instance groups that have been created.
- `add_instance_group` adds an instance group to the repository.
- `delete_instance_group` deletes an instance group from the repository.
- `modify_instance_group` changes the attributes of the specified instance group.
- `auto_registration` automatically registers newly discovered instances into the specified instance group name.
- `disable_auto_registration` disables automatic registration of newly discovered instances.
- `list_dbas` displays a list of all DBAs able to use nboraadm on a specified client.
- `add_dba` allows the NetBackup Administrator to give a database administrator (DBA) the ability to use the nboraadm command on a specific client.
- `delete_dba` removes the ability of the specified DBA to use nboraadm on the specified client.
- `list_jobs` displays job information for the Oracle jobs that contain RMAN output.
- `list_job_details` displays the RMAN output for a specified job.
- `list_rac_dbs` lists all the databases that NetBackup can identify as Oracle RAC.
- `add_rac_db` lets you manually add an Oracle RAC database to NetBackup.
- `register_rac_db` lets you register the Oracle RAC credentials with NetBackup.
-modify_rac_db modifies an existing Oracle RAC database in NetBackup.

-delete_rac_db lets you delete the Oracle RAC database and any associated instances from NetBackup.

-list_rac_instances lists all the instances that NetBackup can identify as Oracle RAC.

-add_rac_instance lets you manually add an Oracle RAC instance to NetBackup. You cannot add instance without a database.

-modify_rac_instance modifies an existing Oracle RAC instance in NetBackup.

-delete_rac_instance lets you delete an Oracle RAC instance from NetBackup.

-list_instance_aliases lists all the aliases that are associated with the Oracle instance.

-add_instance_alias adds an alias that is associated with the Oracle instance.

-delete_instance_alias deletes an alias that is associated with the Oracle instance.

**OPTIONS**

-active | -inactive

When used with the -list_instances operation, you can narrow the list to only the active instances or the inactive instances. The default condition is to list all instances.

When used with the -modify_instance operation, you can change the status of an instance from active to inactive or vice versa.

When used with -modify_rac_instance, this option adds or removes the instance from the pool of available nodes for backup. When the option is used with -modify_rac_db, you can change the status of a database from active to inactive or vice versa.

-add_rac_dbid id

Used to add an Oracle RAC database ID. Used only with -register_rac_db when the database ID is not discovered.

-alias name

Used with -add_instance_alias or -delete_instance_alias to add or delete an alias that is associated with the database instance.

-backup_host name

Used to specify an alternate network host for transport of backup data. This option only applies to -add_rac_instance and -modify_rac_instance.
-disable_backup_host
Disables the use of a backup host name. This option only applies to
-modify_rac_instance.

-backup_priority number
An integer that defines the order in which to use RAC instances for protection.
Valid values are any integer. If two instances of a RAC share the same priority,
instances are selected in alphabetical order. As NetBackup tests the credentials
for the highest priority instance, if the instance is unavailable, NetBackup does
not test credentials on any other instances. Use -force to skip validation.

-client_name user_name
Specifies a client name and the user name of a database administrator (DBA)
to enable or disable the use the nboraadm command. These options are used
only with the -add_dba operation and the -delete_dba operation.

-disable_oracle_auth
Disables the use of Oracle authentication.

-disable_os_user
Disables the use of operating system authentication.

-disable_rman_catalog
Disables the use of Oracle RMAN Recovery Catalog Credentials as well as
Wallet RMAN recovery catalog credentials.

-disable_wallet_auth
Disables the use of Wallet authentication.

-force
Forces the instance or RAC database to be added to the repository despite a
validation failure. Unregistered instances or RAC databases cannot be protected
using a NetBackup for Oracle policy.

-host name
Specifies the name of the host where the Oracle database resides

-immediate
Allows the Oracle DBA to start an immediate backup from the Oracle client.
The Oracle DBA can start the backup instead of waiting for the backup to be
initiated based on the NetBackup schedule. When -immediate is used, the
-policy option is required. Additional, you must specify either the -instance
option or the -rac_dbid and -rac_db_unique_name options. The Oracle DBA
can use this option for the immediate backup of a RAC database.
-instance_group name
   Specifies that you want the new or the changed instance to be part of the instance group with the specified name.

-instance_name
   Names the instance that is created or changed.

-list_job_details -jobid jobid [-utc]
   Displays the RMAN output that is contained in the LOG messages from Job Details for the specified Oracle job that the parameter -jobid defines. Use the nboraadm -list_jobs command to determine the specified jobid you want RMAN details about. The optional -utc parameter displays each Job Details message timestamp in UTC format instead of the default UNIX time format.

-list_jobs [count] [-utc]
   Displays the Oracle jobs that contain RMAN output where the count parameter specifies the number of the most recent Oracle jobs to list. Displays the following job information for each Oracle job in JSON format: Jobid, JobType, Status, State, Policy, ScheduleType, Schedule, Started, and Ended. The valid range of values for the count parameter is 1 to 1024. If the optional count parameter is not specified the default is 128. The optional -utc parameter displays all Job Details message timestamps (i.e. Started and Ended fields) in UTC format instead of the default UNIX time format.

-load_balanced_node_count number
   An integer that defines the maximum number of nodes NetBackup uses for backup. Backups proceed with a lower number, if the number of nodes that is specified is not available. If you specify 0 (zero) NetBackup uses all the available nodes.

-new_scan_name name
   Used to change the SCAN (single client access name) name of the Oracle RAC database. Used with the -modify_rac_db option.

-no_warnings
   NetBackup warns the user if you change an instance that is not local to the host where you ran the command. NetBackup prompts to ask if you want to change the instance. Use this option to prevent the display of this warning.

-oracle_auth user [-oracle_TNS tns]
   Specifies the user name and the Net Service Name (TNS alias) of the Oracle authentication credentials.

-oracle_home oracle_home
   Specifies the file path of the Oracle home directory where the instance resides.
-os Unix | Windows
  Specifies if the operating system type for the instance is UNIX or Windows.

-os_user name [-os_domain name]
  Specifies the user name and the domain of the operating system credentials.

-port number
  The grid service listener port. The behavior of this option varies based on the operation specified.

-rac_db_unique_name name
  The unique database name for the Oracle RAC database. Once this name is discovered or manually added, it cannot be changed. The behavior of this option varies based on the operation specified.

-rac_dbid id
  The database ID for the Oracle RAC database. You cannot change the database ID once it is added. The behavior of this option varies based on the operation specified.

-rac_type values
  The type of Oracle RAC database communicating with NetBackup. Accepted values are RAC and RACOneNode.

-registered | -unregistered
  Specifies all instances that are registered and all instances that are not registered due to incorrect credentials.

-rman_catalog_user name [-rman_catalog_TNS tns]
  Specifies the user name and the Net Service Name (TNS alias) of the Oracle RMAN Recovery Catalog credentials.

-S master_server
  Specifies the master server that contains the instance to be added or changed.

-scan_name name
  The database SCAN name for the Oracle RAC database. The behavior of this option varies based on the operation specified.

-service_name name
  The service name for the Oracle RAC database. The behavior of this option varies based on the operation specified.

-unix_os_user name -windows_os_user name
  Specifies the user name for UNIX and/or Windows OS credentials for an instance group.
-unix_tns_admin tns_admin and -windows_tns_admin tns_admin
    Used to override default UNIX TNS_ADMIN or Windows TNS_ADMIN path.

-wallet_path
    Specifies the path to the Oracle wallet that contains the credentials for use with
    the instance or RAC database.

-wallet_tns
    Specifies the wallet connect descriptor to use to look up the credentials within
    the Oracle wallet. You cannot use this option with a RAC database.

-wallet_rman_TNS
    Specifies the RMAN Net Service Name of the Oracle RMAN recovery catalog
    credentials that are stored in the Oracle wallet. This option is used with both
    instances and RAC databases.
nbora

nbora – Manage Oracle Copilot images and instant recovery point operations.

SYNOPSIS

nbora -list_images [-client name] [-server master] [-s mm/dd/yyyy [hh:mm:ss]] [-e mm/dd/yyyy [hh:mm:ss]]
nbora -list_images -X [-client name] [-server master] [-s unixtime] [-e unixtime]
nbora -list_files -backupid backup_id [-server master] [-verbose]
nbora -create_recovery_point -backupid backup_id -dest_client name [-export_options options] [-server master] [-verbose]
nbora -list_recovery_points -appliance appliance_name [-server master]
nbora -delete_recovery_point -appliance appliance_name -export_path export_path [-server master]
nbora -validate -backupid backup_id -mount_path mount_path [-verbose] [-server master]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/
On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

The nbora command can determine if an image is available for Oracle Copilot instant recovery. The command lists files from a backup ID, creates and deletes recovery points, lists recovery points from an appliance, and validates a snapshot for use. Some of the nbora options can only be run from the master server. The nbora command performs the following operations:

- list_images lists backup images compatible with Oracle Copilot instant recovery. This option can be run from the master server or the client.
- list_files  lists the backup files information, from a given backup ID, for use with Oracle Copilot instant recovery. This option can be run from the master server or the client.

- create_recovery_point  creates a recovery point on a NetBackup appliance for instant recovery. This option can only be run from the master server.

- list_recovery_points  lists the recovery points available on the NetBackup appliance. This option can only be run from the master server.

- delete_recovery_point  deletes the recovery point on the requested NetBackup appliance. This option can only be run from the master server.

- validate  validates the snapshot for use with the recovery point that is created. This option can be run from the master server or the client.

---

Note: The environment variable ORACLE_HOME is required to be set when the -validate operation is used in a Windows environment.

---

**OPTIONS**

- appliance  appliance_name
  
  The NetBackup appliance where the instant recovery point is located.

- backupid  backup_id
  
  The backup image that is used in instant recovery point operations.

- client  name
  
  Specifies a client name to use for Oracle Copilot instant recovery. By default, nborair searches for all clients where the command was run.

- dest_client  name
  
  The client the instant recovery point is exported to.

- e  mm/dd/yyyy [hh:mm:ss] or unixtime
  
  The end date that is used to filter backup images. Use mm/dd/yyyy [hh:mm:ss] or pass unixtime with the –x parameter.

- export_options  options
  
  Allows the user to set the NFS export options of the newly created instant recovery point. It takes as arguments a comma separated list of options.

  See the NetBackup Appliance Administrator’s Guide for the list of NFS export options.

- export_path  export_path
  
  The export path for the instant recovery point.
-mount_path mount_path
   The mount path of the instant recovery point on the destination client.

-s mm/dd/yyyy [hh:mm:ss] or unixtime
   The start date that is used to filter backup images. Use mm/dd/yyyy [hh:mm:ss]
   or pass unixtime with the -x parameter.

-server master_server
   Master server to use.

-verbose
   Provides more information about the associated operation.

-x
   Interpret the -s and -e parameters as UNIX time.
**nb pem**

nb pem – run NetBackup Policy Execution Manager to schedule and submit the jobs that are due

**SYNOPSIS**

nb pem [-console] [-terminate]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\

**DESCRIPTION**

The NetBackup Policy Execution Manager (nb pem) is a service that starts when NetBackup is started and remains active until NetBackup stops.

The nb pem command does the following:

- Determines which jobs are due based on defined policies and the previous backup images.
- Creates Policy/Client tasks and determines when jobs are due to run.
- If a policy is modified or if an image expires, it is notified and the appropriate Policy/Client tasks are updated.
- Determines a policy’s priority that is based on how overdue the job is.
- Ensures that the policies are scheduled within the windows in which they are supposed to run.
- Cancels the policies that are queued, late, or outside the parameters of the scheduled window.
- Handles any policy changes and then updates the policies that are due to run.
- Initiates more attempts if a particular job stops part way through the backup.

**OPTIONS**

- -console
  Enables you to start NetBackup in console mode.
-terminate

Enables you to stop the NetBackup policy execution manager.

SEE ALSO

See nbjm on page 746.
See nbrb on page 788.
See nbpemreq on page 776.
nb pemreq

nb pemreq – run NetBackup Policy Execution Manager (PEM) Requisition to schedule the jobs that are due and capture PEM information

SYNOPSIS

nb pemreq -due -date mm/dd/yyyy hh:mm:ss [-unixtime] [-legacy] [-client_filter client...] [-policy_filter policy...]
nb pemreq -due -dateu unixtime [-unixtime] [-legacy] [-client_filter client...] [-policy_filter policy...]
nb pemreq -jobs [screen] [-depth value] [all | job_id...]
nb pemreq -M servername...
nb pemreq -persisted [screen] [-depth value]
nb pemreq -policies [screen] [-depth value] [policy...]
nb pemreq -predict -date mm/dd/yyyy hh:mm:ss [-unixtime] [-legacy] [-client_filter client...] [-policy_filter policy...]
nb pemreq -predict -dateu unixtime [-unixtime] [-legacy] [-client_filter client...] [-policy_filter policy...]
nb pemreq -predict_all -date mm/dd/yyyy hh:mm:ss [-legacy] [-client_filter client...] [-policy_filter policy...]
nb pemreq -predict_all -dateu unixtime [-legacy] [-client_filter client...] [-policy_filter policy...]
nb pemreq -resume_scheduling
nb pemreq -subsystems [screen] [list | all | subsystem_id...]
nb pemreq -suspend_scheduling
nb pemreq -updatepolicies

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is \install_path\NetBackup\bin\admincmd\
DESCRIPTION

The NetBackup Policy Execution Manager Requisition (nb pemreq) determines which jobs are due in the near future. It also reads in all entered policy updates that are in a pending state. Finally, nb pemreq gathers the pertinent nb pem information that is placed in the nb pem log file and optionally displayed to stdout.

This command can also instruct nb pem to process policy updates immediately.

When the nb pemreq command runs, nb pem is affected, which slows down policy processing. Because the nb pemreq output may change from release to release, Veritas does not recommend using nb pemreq in scripts.

OPERATIONS

-due

Provides data about the clients or policies that are scheduled to run by the time specified. The data that is displayed is based on the current time and a future date. Time is indicated by yymm/dd/yyyy hh:mm:ss or by a UNIX timestamp.

-jobs

Provides nb pem information about the state of current jobs and jobs that have run in the previous 30 minutes. nb pem manages all running jobs and keeps history on each job for 30 minutes after the job completes.

-M servername...

Allows nb pemreq to be executed on one or more master servers. The command is executed on each master sequentially in the order that is listed on the command line. When -M is not specified, the default value is the local host.

-persisted

Provides internal information about the contents of the nb pem persistence database file, which contains information about the jobs that are currently running. If nb pem is interrupted, NetBackup knows which jobs to run when nb pem restarts.

-policies

Provides nb pem internal data about the specified policies that includes static data from the policy definition and dynamic information about job scheduling.

-predict | -predict_all

Helps determine when a policy is to be run. The displayed information is based on the current time and a future date. Time is indicated by yymm/dd/yyyy hh:mm:ss or by a UNIX timestamp.
This option also helps determine why a policy has not run. The difference between the options is the output format and the amount of data presented. It shows the backups that are eligible to run, but it does not indicate which jobs are to run at a specific time. It checks for an open window for the backup, but does not reflect any of the exclude dates that might be set for the schedule.

-resume_scheduling

Resumes the nbpemreq the scheduling activity that a -suspend_scheduling option has interrupted.

-subsystems

Provides nb pem internal information about the internal subsystem operations. The amount of information that is presented for each subsystem depends on the specified depth. Each subsystem contains varying layers of information.

-suspend_scheduling

Suspends the nbpemreq scheduling activity. You can use this option to suspend scheduled backups.

-updatepolicies

Instructs nb pem to reread the existing policy configuration. Normally, nb pem checks for changes based on the policy update interval that is part of the Global Attributes host properties. The default is 10 minutes. After you run this command, the prompt is simply returned.

OPTIONS

all | job_id...

Lists all jobs or the job that job_id specifies.

-client_filter client...

Filters on the name of a specific client or clients.

-depth [ list | all | subsystem_id...]

Specifies the level of detail to be produced for the various output options. Depth is an integer value starting at zero (least amount of output) and goes up (more output). The maximum depth value and the specific content of each depth level varies from output option to output option. The information differs from the information that is presented by using the -subsystems option.

-depth value

Displays all 36 subsystems, or the specified subsystems. Separate the subsystems with spaces, not commas. For example:

# nbpemreq depth 3 8 12
-policy_filter policy...
    Filters on the name of a specific policy or policies.

screen
    Sends the output to stdout. Command output is always directed to the log files even if the screen option is not used. A maximum of 1 MB of data can be written to stdout.

-unixtime
    Specifies the number of seconds elapsed since midnight Coordinated Universal Time (UTC) of January 1, 1970, not counting leap seconds.

SEE ALSO

See nbpem on page 774.
nbmlb

nbmlb – migrates the sign-in banner for the NetBackup Administration Console to the NetBackup Web UI.

SYNOPSIS

nbmlb -migrate file [-force]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\

DESCRIPTION

The nbmlb command migrates the contents of the sign-in banner file for the NetBackup Administration Console to the database. Then the same sign-in banner is used in the NetBackup Web UI.

OPTIONS

-force
   Forces an update even when the sign-in banner exists in the NetBackup Web UI. This option is not required.

-migrate file
   Where file is the location of the sign-in banner file. On UNIX the location is /usr/openv/var/LoginBanner.conf. On Windows the location is install_path\NetBackup\var\LoginBanner.conf.
nbperfchk

nbperfchk – measures a disk array’s read and write speeds.

SYNOPSIS

nbperfchk -i inputpath -o outputpath [-s filesize] [-syncend] [-bs buffersize]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/support/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\support\n
DESCRIPTION

The nbperfchk command measures the read speed and write speed of a disk array. You can use this command to test the read speed and the write speed of the disks that host deduplicated data. For example, you can measure the speeds of the disks that host deduplicated data.

In a NetBackup media server deduplication pool (MSDP), use this command to measure the speed of the disks attached to the media server. The media server can be running any operating system that Veritas supports for media servers and MSDPs.

Note: Veritas recommends that you work with a Veritas technical support staff member when you run this command and interpret its results. Veritas recommends a minimum disk performance level of 130 MB/sec for deduplicated read and write operations.

The nbperfchk utility enables you to write a test file to a disk, read back that test file, and observe the read speeds attained during the read operation. You can use the results from nbperfchk to make sure that the ReadBufferSize parameter is set appropriately in your backup environment. The ReadBufferSize parameter resides in the [CRDataStore] section of the contentrouter.cfg file. You can use this command as follows:

- Use the following command to write data to the disks:
  nbperfchk -i inputpath -o outputpath -s filesize -syncend
Use the following command to read data from the disks:
```
nbperfchk -i inputpath -o outputpath -bs buffersize
```

**OPTIONS**

- **-i inputpath**
  
  For *inputpath*, specify the full path to an input file. The `nbperfchk` command reads this file and generates information about the read speed when this file is read to disk.

  For example, you can specify the following to read in a file that contains all zero characters (0x00) from the `/dev/zero`:

- **-o outputpath**
  
  For *outputpath*, specify the full path to an output file. The `nbperfchk` command creates this file.

  For example, on writes, specify the path to the output file that you want to create. On reads, specify `-o NULL` to discard all the output as it is generated.

- **-s filesize**
  
  For *filesize*, specify a file size that is equal to or larger than the combined memory size of your computer plus the amount in the disk array. A file of this size ensures that the data is written to disk and not to a buffer.

- **-syncend**
  
  The `syncend` parameter flushes the buffer and writes all data to disk.

- **-bs buffersize**
  
  For *buffersize*, specify the read buffer size to use when `nbperfchk` runs. For example, 64k or 128k.

**PROCEDURES**

To analyze `nbperfchk` results and adjust the ReadBufferSize parameter setting

1. Log in as the root user (UNIX) or the administrator (Windows) on the computer that hosts the content router.
   
   In NetBackup environments, log into the media server.

2. Change to a test directory.
Type the `nbperfchk` command in the following format to write a large test file to the content router:

```
nbperfchk -i inputpath -o outputpath -s filesize -syncend
```

For example, the following command writes a 64 GB data file that contains all zeros to the e drive:

```
nbperfchk -i zero: -o e:\data1 -s 64g -syncend
```

Type the `nbperfchk` command in the following format to read the test file and observe the read speeds in the `nbperfchk` output:

```
nbperfchk -i inputpath -o NULL -bs buffersize
```

Example 1. To observe several read speeds, with several buffer sizes, type the following series of commands:

```
nbperfchk -i e:\data1 -bs 64k -o NULL
nbperfchk -i e:\data1 -bs 128k -o NULL
nbperfchk -i e:\data1 -bs 256k -o NULL
```

Example 2. The following `nbperfchk` command reads back the data in file `data1` and uses a buffer size of 1024 K:

```
C:\Users\administrator.mymediaserver\Desktop>nbperfchk -i e:\data1 -bs 1024k -o NULL
195 MB @ 65.3 MB/sec, 194 MB @ 64.9 MB/sec
295 MB @ 49.4 MB/sec, 100 MB @ 33.5 MB/sec
403 MB @ 44.8 MB/sec, 108 MB @ 35.8 MB/sec
505 MB @ 42.1 MB/sec, 102 MB @ 34.1 MB/sec
599 MB @ 40.0 MB/sec, 94 MB @ 31.3 MB/sec
705 MB @ 39.2 MB/sec, 106 MB @ 35.5 MB/sec
821 MB @ 39.2 MB/sec, 116 MB @ 38.8 MB/sec
943 MB @ 39.4 MB/sec, 122 MB @ 40.8 MB/sec
1024 MB @ 40.1 MB/sec
```

Observe the following when you analyze the data:

- The left two columns show the amount of data read and the average read speed.
- The final line shows the overall read speed. This is the most important line in this output because it shows you how fast the total read occurred with the buffer size you specified.
- The right two columns show the average read speed in the last 3 seconds of each read. Unless these numbers vary drastically from read to read, you can disregard the right two columns.

5. Analyze your read speeds and adjust the **ReadBufferSize** parameter if necessary.

Your operating system, your disk speeds, and the **ReadBufferSize** parameter setting all affect restore and rehydration performance.

Veritas recommends that you type several `nbperfchk` commands and increase the size of the argument to the `-bs` parameter each time. Example 1 in step 4 shows this method. If you can enter ever-increasing arguments to the `-bs` parameter, you can probably increase the size of the **ReadBufferSize** parameter in the `[CRDataStore]` section of the `contentrouter.cfg` file.

By default, **ReadBufferSize=65536**, which is 64K. Veritas testing shows that **ReadBufferSize=1048576**, which is 1024 X 1024, or 1M, offers good performance on most Windows systems. On most UNIX systems, Veritas testing shows that **ReadBufferSize=65536** (the default) offers good performance.

For information about how to edit NetBackup configuration files, see the NetBackup documentation.
nbplupgrade

nbplupgrade – upgrade policy type from FlashBackup-Windows to VMware or Hyper-V

SYNOPSIS

```
```

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The nbplupgrade utility (CLI) upgrades FlashBackup-Windows policies that were created for VMware or Hyper-V backup. To successfully convert a policy, note the following requirements:

- The current policy must not specify a NetBackup pre-7.5 media server or pre-7.5 VMware backup host.
- The current policy must not specify any option that requires VMware VCB.

To convert the policy even when the above requirements are not satisfied, use the -vm_force option. This option may require further editing of the converted policy.

During conversion, the nbplupgrade utility converts the policy type from FlashBackup-Windows to VMware or Hyper-V as appropriate. It also converts the snapshot method to the new VMware or Hyper-V type as required by the new policy. It retains all other attributes from the original policy and converts them as needed to the new 7.5 policy layout.

This upgrade is necessary only if you want the policy to use the new VMware or Hyper-V features in NetBackup 7.5.

OPTIONS

- **-allpolicies**
  Upgrades all FlashBackup-Windows policies that were created for VMware or Hyper-V backup.
Lists usage information on the nbplupgrade command.

`policy_name`
Performs the upgrade only on the specified policy.

`-verbose`
Helps you track the progress of the utility script.

`-vm_force`
Before the conversion, the utility checks for incompatibilities such as a policy that is tied to an old media server or an old client. If an incompatibility exists, the utility issues a warning and exits or moves to the next policy if `-allpolicies` is selected. However, when the `-vm_force` option is specified, the policy converts despite the compatibility check failure. Use this option with care, because it can cause backup failures for the migrated policy.

`-vm_report`
Performs the compatibility checks and reports the results. Note that it does not perform the actual policy conversion. This option is designed to be used only as a migration dry run before you attempt the actual conversion.

`-vm_force` and `-vm_report` cannot be used together in the same command.

**EXAMPLES**

Example 1 - Perform compatibility checks on the `mypolicy` policy and report the results. This action is only a dry run of an actual conversion to be run later.

```bash
# nbplupgrade mypolicy -vm_report
```

Example 2 - Perform compatibility checks on all the FlashBackup-Windows policies and report the results. This action is only a dry run of an actual conversion to be run later.

```bash
# nbplupgrade -allpolicies -vm_report
```

Example 3 - Upgrade the policy named `mypolicy`.

```bash
# nbplupgrade mypolicy
```

Example 4 - Upgrade all the FlashBackup-Windows policies that were created for VMware or Hyper-V backup.

```bash
# nbplupgrade -allpolicies
```

Example 5 - Upgrade the policy named `mypolicy` even if the compatibility check fails.
# nbplupgrade mypolicy -vm_force

Example 6 - Upgrade all the FlashBackup-Windows policies that were created for VMware or Hyper-V backup. even if the compatibility check fails.

# nbplupgrade -allpolicies -vm_force
**nbrb**

nbrb – run NetBackup Resource Broker

**SYNOPSIS**

```bash
nbrb [-console] [-terminate]
```

On UNIX systems, the directory path to this command is `/usr/openv/netbackup/bin/`

On Windows systems, the directory path to this command is `install_path\NetBackup\bin`

**DESCRIPTION**

The NetBackup Resource Broker binary (`nbrb`) is a service that starts when NetBackup starts and remains active. This service makes the allocations for such things as storage units, tape drives, and client reservations. This service works closely with the EMM to obtain physical and logical the resources that a job requires to run. Physical resources can be storage units, tape drives, and media IDs. Logical resources can be named resources, max jobs per client, max jobs per policy, and multiplexed groups as resources that `nbjm` uses.

**OPTIONS**

- **-console**
  
  Enables you to start NetBackup in console mode.

- **-terminate**
  
  Enables you to stop the nbrb.

**SEE ALSO**

See `nbjm` on page 746.

See `nbpem` on page 774.
nbrbutil

nbrbutil – configures the NetBackup Resource Broker (nbrb)

SYNOPSIS

nbrbutil [-cancel GUID] [-changePriority requestID]
[-changePriorityClass requestID] [-changesettings name=value
[,
name=value],... ] [-deleteSetting settingname] [-disablePerfMon]
[-dump] [-dumptables -f filename] [-enablePerfMon] [-listActiveJobs]
[-listActiveDriveJobs] [-listActiveMediaJobs] [-listActivePoolJobs]
[-listActiveStuJobs] [-listOrphanedDrives] [-listOrphanedMedia]
[-listOrphanedPipes] [-listOrphanedStus] [-listSettings] [-release
GUID] [-resetAll] [-releaseAllocHolds] [-releaseDrive drive]
[-releaseMDS ID] [-releaseMedia mediaID] [-releaseOrphanedDrive
drivekey] [-releaseOrphanedMedia mediakey] [-releaseOrphanedPipes]
[-releaseOrphanedStu name] [-resetMediaServer mediaserver]
[-reportInconsistentAllocations] [-resume] [-setDriveGroupUnjoinable]
[-setMediaGroupUnjoinable] [-suspend] [-syncAllocations]

nbrbutil -listPipes [-verbose] [-jobid jobid][-pipe pipeid][-pipeState
PIPE_AVAILABLE | PIPE_UNALLOCATED | PIPE_CLIENT_ORPHANED |
PIPE_SERVER_ORPHANED | PIPE_ORPHANED | PIPE_ACTIVE |
PIPE_SHUTDOWN_REQUEST | PIPE_SHUTDOWN_READ | PIPE_SHUTDOWN_WRITE]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The NetBackup Resource Broker utility sets up the following Resource Broker
functionality:

- List the allocations that the Resource Broker has handed out.
- Release an allocation.
- View the list of orphaned resources.
- Display the jobs that use a particular resource (drive, media, storage unit)
- Cancel a request that has not been allocated.
- Set the Resource Broker tuning parameters.
- Suspend and resume the process.
- List all Fibre Transport pipes.

**OPTIONS**

- `cancel GUID`  
  Cancels the allocation request within the given identifier.

- `changePriority requestID -priority priority`  
  Changes the request priority.

- `changePriorityClass requestID -priorityClass priorityClass`  
  Changes the request priority class.

- `changesettings name=value [,name=value]...`  
  Adds or changes the nbrb configuration settings.

The following describes all the `changesettings` parameters:

- **RB_DO_INTERMITTENT_UNLOADS** - When this parameter is set to true (default), nbrb initiates unloads of the drives that have exceeded the media unload delay. Drives become available more quickly to jobs that require different media servers or different media than the job that last used the drive. However, the loaded media or drive pair may not be available for jobs with less priority in the prioritized evaluation queue that can use the drive or media without unload.

- **RB_ENABLE_OPTIMIZATION** - When this parameter is set to true, it serves as a performance tuning parameter for the Intelligent Resource Manager. This entry instructs NBRB to cache states of resource requests.

- **RB_RESPECT_REQUEST_PRIORITY** - Possible values for this parameter are true or false.  
  When RB_RESPECT_REQUEST_PRIORITY is set to false (default), nbrb continues to evaluate jobs in the prioritized job queue. As a result, a job is likely to reuse a drive more quickly after the drive has been released. However, some lower priority jobs may receive drives before higher priority jobs.  
  When the parameter is set to true, nbrb restarts its evaluation queue at the top of the prioritized job queue after resources have been released.

- **RB_BREAK_EVAL_ON_DEMAND** - When a high priority request appears, nbrb immediately interrupts the evaluation cycle. The request can be a tape
span request, a subsequent request for a synthetic or a duplication job, or a read request for an optimized duplication. If required, \texttt{nbrb} releases and unloads drives before the evaluation cycle begins again.

If the \texttt{RB\_BREAK\_EVAL\_ON\_DEMAND} parameter is set to true (default), interruptions of high priority jobs are not allowed and the evaluation cycle continues.

- **\texttt{RB\_MAX\_HIGH\_PRIORITY\_QUEUE\_SIZE}** - Spanning requests and additional resources for an active duplication job are put in a special queue for priority processing. The \texttt{RB\_MAX\_HIGH\_PRIORITY\_QUEUE\_SIZE} parameter sets the maximum number of requests that NetBackup allows in that queue. (Default: 100 requests.)

- **\texttt{RB\_RELEASE\_PERIOD}** - This parameter indicates the interval that NetBackup waits before it releases a resource. (Default: 180 seconds.)

- **\texttt{RB\_CLEANUP\_OBSOLETE\_DBINFO}** - This parameter indicates the number of seconds that can elapse between the cleanup of obsolete information in the \texttt{nbrb} database. (Default: 60 seconds.)

- **\texttt{RB\_MPX\_GROUP\_UNLOAD\_DELAY}** - This parameter indicates the number of seconds that \texttt{nbrb} waits for a new job to appear before a tape is unloaded. (Default: 10 seconds.)
  
  This setting can help avoid unnecessary reloading of tapes and applies to all backup jobs. During user backups, \texttt{nbrb} uses the maximum value of \texttt{RB\_MPX\_GROUP\_UNLOAD\_DELAY} and the Media mount timeout host property setting when \texttt{nbrb} unmounts the tape.

- **\texttt{RB\_RETRY\_DELAY\_AFTER\_EMM\_ERR}** - This parameter indicates how long NetBackup waits after an EMM error before it tries again. The error must be one where a retry is possible. For example, if a media server is down. (Default: 60 seconds.)

- **\texttt{RB\_REEVAL\_PENDING}** - This parameter indicates the number of seconds that can elapse between evaluations of the pending request queue. For example, a pending request queue can include, jobs awaiting resources. (Default: 60 seconds.)

- **\texttt{RB\_REEVAL\_PERIOD}** - This parameter indicates the time between evaluations if an outstanding request is not satisfied, and if no other requests or resources have been released. (Default: Five minutes must pass before the initial request is reevaluated.)

\texttt{-deleteSetting settingname}

Deletes the \texttt{nbrb} configuration setting identified by the \texttt{settingname} value.
-disablePerfMon
   Disables the Performance Monitoring.

-dump
   Dumps all nbrb allocation and request lists.

-dumptables -f filename
   Enables the Resource Broker (nbrb) to log its internal state in the specified filename.

-enablePerfMon
   Enables the Performance Monitoring.

-jobid jobid
   Restricts the output listing of Fibre Transport pipes to only those used for the specified jobid.

-listActiveJobs
   Lists all the active jobs.

-listActiveDriveJobs
   Lists all the active jobs for a drive.

-listActiveMediaJobs
   Lists all the active jobs for a media ID (disk or tape).

-listActivePoolJobs
   Lists all the active jobs for a volume pool.

-listActiveStuJobs
   Lists all the active jobs for a storage unit or a storage unit group.

-listOrphanedDrives
   Lists the drives that are reserved in EMM but have no corresponding allocation in the Resource Broker.

-listOrphanedMedia
   Lists the media that is reserved in EMM but has no corresponding allocation in the Resource Broker.

-listOrphanedPipes
   Lists the orphaned Fibre Transport pipes.

-listOrphanedStus
   Lists the storage units that are reserved in EMM but have no corresponding allocation in the Resource Broker.
-listPipes
   Lists the information about Fibre Transport pipes.

-listSettings
   Lists the NBRB configuration settings.

-pipe pipeID
   Restricts the output of Fibre Transport pipes to only those with the matching pipeID value.

-pipeState state
   Restricts the output listing of Fibre Transport pipes to only the pipes in specified state.

-release GUID
   Releases the allocation with the given identifier.

-resetAll
   Resets all nbrb allocations, requests, and persisted states.

-releaseAllocHolds
   Releases allocation holds caused by allocation errors for drives and media.

-releaseDrive drive
   Releases all allocations for the specified drive.

-releaseMDS ID
   Releases the EMM and the MDS allocations that are allocated by the MDS with the specified identifier.

-releaseMedia mediaID
   Releases all allocations for the specified volume.

-releaseOrphanedDrive drivekey
   Releases drives that are reserved in EMM but have no corresponding allocation in the Resource Broker.

-releaseOrphanedMedia mediakey
   Releases media that are reserved in EMM but have no corresponding allocation in the Resource Broker.

-releaseOrphanedPipes
   Releases the orphaned Fibre Transport pipes.

-releaseOrphanedStu name
   Releases the storage units that are reserved in EMM but have no corresponding allocation in the Resource Broker.
-resetMediaServer mediasever
    Resets all nbrb EMM and MDS allocations that are related to ltid on the media server.

-reportInconsistentAllocations
    Reports inconsistent allocation between the Resource Broker and MDS.

-resume
    Resumes the Resource Broker (nbrb) processing.

-setDriveGroupUnjoinable
    Disables the future job from joining the group for this drive.

-setMediaGroupUnjoinable
    Disables the future job from joining the group for this media.

-suspend
    Suspends the Resource Broker (nbrb) processing.

-syncAllocations
    Syncs up any allocation difference between the Resource Broker and MDS.

-verbose
    Provides a more detailed information for Fibre Transport pipes.

SEE ALSO

See nbjm on page 746.
See nbpem on page 774.
nbregopsc

nbregopsc – register OpsCenter

SYNOPSIS

nbregopsc -add | -addopscenter | -addnb OpsCenter_server_name

nbregopsc -preferred_network OpsCenter_server_IPAddress

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The NetBackup installation procedure asks if you want to register an existing OpsCenter with NetBackup. You need to enter the full pathname to execute the OpsCenter server name as a command line option. The nbregopsc -add command first adds the OpsCenter server name to bp.conf (CONFIG registry entry on Windows) with a new entry OPS_CENTER_SERVER_NAME = Opscenter_server_name. Later, the NetBackup master server name is registered with the OpsCenter server. This command can be run after the NetBackup installation to register OpsCenter and NetBackup servers with each other.

You can use the -addopscenter option to register OpsCenter with NetBackup without registering NetBackup with OpsCenter. You can also use the -addnb option to register NetBackup with OpsCenter without registering OpsCenter with NetBackup.

The command does not allow multiple OPS_CENTER_SERVER_NAME entries in bp.conf (or the registry), because NetBackup is limited in its ability to monitor multiple OpsCenter center servers. If you run this command with a different name, the new name overwrites the existing entry of OPS_CENTER_SERVER_NAME.

In an OpsCenter cluster setup, the virtual server name is added to bp.conf (or the registry).

OPTIONS

- add OpsCenter_server_name
  Registers NetBackup with the specified OpsCenter server and registers the OpsCenter server with NetBackup.
-addopscenter OpsCenter_server_name
   Registers the OpsCenter server with NetBackup.

-addnb OpsCenter_server_name
   Registers NetBackup with the specified OpsCenter server.

-preferred_network OpsCenter_server_IPAddress
   Specifies an optional OpsCenter server IP. -preferrednetwork applies only
to -add and -addnb. It applies mainly for multiple network interface cards (NICs)
on the OpsCenter host. The default value for this option is localhost/127.0.0.1.
nbreplicate

nbreplicate – initiate replication on a storage device

SYNOPSIS

nbreplicate -backupid backup_id -Bidfile file_name -cn copy_number 
-rcn replicate_copy_number -slp_name policy_name [-altreadhost 
hostname] [-priority number] [-v] [-target_sts target_sts] 
[-target_user target_sts_username] [-target_pwd target_sts_password]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The nbreplicate command allows a copy of a backup to be replicated to a 
NetBackup storage device in another domain. To duplicate an image in the same 
NetBackup domain, please see bpduplicate.

The nbreplicate command creates a copy of a specified backup based on the 
configuration on the supported replication targets of the storage server. This 
command is part of the automated Storage Lifecycle Policy (SLP) process of Remote 
Master Replication operations.

This command is not intended to circumvent normal NBSTSERV processing for 
Storage Lifecycle Policy controlled images. This command exists to redo previously 
successful replications. It is distinctly different from bpduplicate.

This command can be run only on the master server.

OPTIONS

-altreadhost hostname

Specify an alternate host from which to read the media. The default condition 
is that bpreplicate reads the source media from the host that performed the 
backup.
-backupid backup_id
    Specifies the backup ID of a single backup to replicate or for which you can change the primary copy.

-Bidfile file_name
    file_name specifies a file that contains a list of backup IDs to be duplicated. List one backup ID per line in the file. If this parameter is specified, other selection criteria are ignored.

    Also, file_name is removed during the execution of that command line interface (CLI) because the NetBackup GUIs commonly use this parameter. They expect the command-line interface to remove the temporary file that was used for the -Bidfile option upon completion. Direct command-line interface users can also use the option; however, it removes the file.

-cn copy_number
    Determines the copy number to duplicate. Valid values are 1 through 10. The default is 1.

    -primary means to search or duplicate the primary copy.

-priority number
    Sets a backup policy to run at a lesser or a higher priority than disk staging duplication.

-target_pwd target_sts_password
    Specifies the target storage server password if credentials are required to access the device.

-target_sts target_sts
    Specifies the target storage server to receive a copy of the replicated backup.

-target_user target_sts_username
    Specifies the target storage server user name if credentials are required to access the device.

-rcn replicate_copy_number
    Specifies the copy number of the replication copy. The copy number is the operation index value of the storage lifecycle policy replication operation plus 100.

    -primary means to search or duplicate the primary copy.

-slp_name policy_name
    Specifies the SLP name of the duplicated file.
Selects the verbose mode. When you specify the debug logs or progress logs, it includes more information.

**EXAMPLE**

Re-replicate an image according to the SLP parameters of an image that was previously successfully replicated, but needs to be replicated again due to disaster recovery.

```
# nbreplicate -backupid bu789 -rcn 102 -cn 1 -priority 0 -slp_name slp1
```

**FILES**

**UNIX systems:**

```
/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/db/images/*
```

**Windows systems:**

```
install_path\NetBackup\db\images/*
install_path\NetBackup\logs\admin/*
```

**SEE ALSO**

See `bpduplicate` on page 121.
nbrepo

nbrepo – used to manage the NetBackup package repository.

SYNOPSIS

nbrepo -a package_path
nbrepo -d package_identifier
nbrepo -l
nbrepo -p package_identifier
nbrepo -h

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\

DESCRIPTION

The nbrepo command is used to manage packages in the NetBackup repository. You can add new packages or delete existing packages from the repository. You can also list all the packages that currently exist in the repository. You can use this command to retrieve the package metadata.

OPTIONS

-a | -add package_path
  Add packages to the repository. The package identifier the repository generates is returned.

-d | -delete package_identifier
  Delete packages from the repository. Specify the package identifier for the command to delete.

-h | -help
  Show the command usage statement.

-l | -list
  Returns a list of all packages which have been added to the repository.
-p | -pkgDetails package_identifier

Returns the package metadata for the specified package.

EXAMPLES

Example 1: Adding a package to the NetBackup repository.

nbrepo -add C:\temp\vxupdate_nbclient_8.1.2_windows_x64.sja

Successfully added deployment package ID: 6 to the repository.

Example 2: Use the nbrepo command to determine the Installables field for use in the nbinstallcmd -package command. Note the File Name field is truncated in the nbrepo -l output. Bold is added for clarity.

nbrepo -l

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Version</th>
<th>OS</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>server+client</td>
<td>8.2</td>
<td>redhat_x64</td>
<td>vxupdate_nb_8.2_redhat_x64.sja</td>
</tr>
<tr>
<td>6</td>
<td>client</td>
<td>8.2</td>
<td>redhat_x64</td>
<td>nbeeb.client_3977539.1_8.2_re</td>
</tr>
<tr>
<td>7</td>
<td>server</td>
<td>8.2</td>
<td>redhat_x64</td>
<td>nbeeb.server_3977539.1_8.2_re</td>
</tr>
<tr>
<td>8</td>
<td>eeb</td>
<td>8.2</td>
<td>windows_x64</td>
<td>nbeeb_3977539.1_8.2_windows_x</td>
</tr>
<tr>
<td>9</td>
<td>client</td>
<td>8.2</td>
<td>suse_ppc64le</td>
<td>vxupdate_nbclient_8.2_suse_pp</td>
</tr>
</tbody>
</table>

nbrepo -p 1

Package ID: 1
Package File Name: vxupdate_nb_8.2_redhat_x64.sja
Package Type: server+client
Operating System: redhat_x64
Release Version: 8.2
Installables: nbclient_8.2
            nbserver_8.2
Package Size: 1.26 GB
Created Date/Time (UTC): 2019-05-15 09:04:28

SEE ALSO

See nbinstallcmd on page 737.
nbrestorevm

nbrestorevm – restore VMware or Hyper-V virtual machines

SYNOPSIS

For VSphere Restore:

```
nbrestorevm -vmw -C vm_client [-S master_server] [-O] [-R rename_file]
[-L progress_log [-en]] [-k "keyword phrase"] [-s mm/dd/yyyy
[hh:mm:ss]] [-e mm/dd/yyyy [hh:mm:ss]] [-w [hh:mm:ss]] [-vmtm
vm_transport_mode] [-vmserver vm_server] [-vmproxy vm_proxy] [-vmpo]
[-vdclfree] [-vcdremv] [-vmst] [-copy copy_number]
```

For VMware Selective VMDK Restore:

```
nbrestorevm -vmw -C vm_client -S master_server -s mm/dd/yyyy hh:mm:ss
-e mm/dd/yyyy hh:mm:ss | -backupid value -restorespecout filename
```

```
nbrestorevm [-validate] -restorespec filename
```

```
nbrestorevm -restorespec filename [-L progress_log] [-w [hh:mm:ss]]
```

For Hyper-V VM Restore:

```
nbrestorevm {-vmhv | -vmhvnew | -vmhvstage | -vmncf} -C vm_client
[-S master_server] [-O] [-R rename_file] [-L progress_log [-en]] [-k
"keyword phrase"] [-s mm/dd/yyyy [hh:mm:ss]] [-e mm/dd/yyyy
[hh:mm:ss]] [-w [hh:mm:ss]] [-vmtm vm_transport_mode] [-vmserver
vm_server]
```

For BMR VM Conversion:

```
vm_server -vmproxy vm_proxy -veconfig config_filepath [-config
bmr_config_name] [-vmpo] [-vmname] [-systemOnly]
```

For VMware Instant Recovery:

---

802NetBackup Commands

nbrestorevm
The `nbrestorevm` command restores VMware virtual machines (`-vmw` option) or Hyper-V virtual machines (`-vmhv` option). You can run `nbrestorevm` on a client to restore VMs only if you specify the client as a peer of the master server for the purpose of specific VM restoration. This restriction also applies to media servers if the media server is installed on different machine than the master server.

This command covers a wide range of functionality:

- The `-vmw` option restores a VMware virtual machine.
- The `-vmhv`, `-vmhvnew`, `-vmhvstage`, and `-vmncf` options restore a Hyper-V virtual machine.
- The `-bmr -vmw` option creates a VMware virtual machine from a client backup.
- The `-restorespec` option restores one or more virtual machine disks into a new VM.
- The `-ir_activate` option starts the instant recovery of a specified virtual machine. A set of related instant recovery options (`-ir_listvm`, `-ir_deactivate`, `-ir_done`, `-ir_reactivate`, and `-ir_reactivate_all`) perform other functions on the instant recovery of a virtual machine.
You can run this command on the master server and on all clients.

**OPTIONS**

Several of the options are common to all restores (VSphere, Hyper-V, BMR VM conversion, and IR) and others are specific to a subset of these restores. All options that begin "-ir" are Instant Recovery only (for example, -ir_list). Options that begin "-vcd" are VSphere only (for example, -vcdred). Other options that apply to only a subset of functions, are noted in the option description.

- **-backupid value**
  The ID of the backup image to use to create the parameters file to restore a VMware virtual machine disk or disks, in `clientname_backuptime` format. The `backuptime` is the decimal number of seconds since January 1, 1970.

  Use this option with the `-restorespecout` option. Do not combine it with the `-s` or `-e` option.

- **-bmr**
  Contacts the BMR server to carry out tasks related to virtual machine creation from client backup.

- **-C vm_client**
  The name of the virtual machine as identified in the backup. For example, if the policy backed up the virtual machine by its host name, specify that host name.

  To restore to a different location, use the `-vmserver` and `-R` options.

- **-config bmr_config_name**
  Specifies the BMR configuration name. The default name is `current`. Applies only to the BMR VM conversion.

- **-copy copy_number**
  Specifies the copy number to restore from for a vSphere Restore operation. This option allows a restore from a copy other than the primary copy. For example, `-copy 3` restores copy 3 of the backup image.

  This option is only supported for a full backup of a VMware virtual machine. If the specified copy number does not exist, the primary copy is used.

- **-disk_media_server media_server**
  Specifies which media server performs the Instant Recovery.

  This option is useful if NetBackup storage is configured over several media servers, such as for load balancing. Without the `-disk_media_server` option, the Instant Recovery job may select any of the available media servers to do
the restore. If only one of the media servers is configured for Instant Recovery, specify that server with the -disk_media_server option.

-force
  Suppresses the confirmation prompts.

-ir_activate
  Starts the Instant Recovery of the specified virtual machine. For VMware, the command mounts the backup image as an NFS datastore. The virtual machine is instantly recovered when the virtual machine data is accessible on the VM host.

-ir_deactivate ir_identifier [-force]
  Deletes the specified restored virtual machine from the ESX host and releases the NetBackup media server resources. The -force option suppresses the confirmation prompts.

-ir_done ir_identifier
  Completes the virtual machine instant recovery job after the data is migrated. It removes the NetBackup storage and releases the media server resources. The NetBackup storage is the datastore that is mounted on the ESX host.

-ir_listvm
  Lists details about the virtual machines that are activated by instant recovery.

-ir_reactivate ir_identifier [-force]
  Reactivates a restored virtual machine by remounting the NetBackup NFS datastore. It also registers the restored virtual machines on the ESX host from the temporary datastore on the ESX host.

  ir_identifier is the virtual machine's numeric identifier from the -ir_listvm output.

  The -force option suppresses the confirmation prompts.

-ir_reactivate_all
  Restarts an interrupted instant recovery job for all virtual machines on the ESX host and NetBackup media server combination.

-L progress_log
  Specifies the name of an existing file in which to write progress information. This option applies to vSphere restore and Hyper-V restore.

  Only default paths are allowed for this option and Veritas recommends to use the default paths. If you cannot use the NetBackup default path in your setup, you should add custom paths to the NetBackup configuration. The following are the default paths:

  UNIX systems: /usr/openv/netbackup/logs/user_ops/proglog
Windows systems: `install_path\NetBackup\logs\user_ops\proglog`

For more information on how to add a custom path, see the “BPCD_WHITELIST_PATH option for NetBackup servers and clients” topic in the NetBackup Administrator’s Guide, Volume I.

`-media_server media_server_activate_vm`

Specifies the media server on which the NFS datastores that contain the backup images were mounted when you reactivate virtual machines. This option is used only with the `-ir_reactivate_all` function.

`-O`

Overwrites the VMs and associated resources if they already exist with the same name. The resources are entities such as virtual machine disk format files (VMDKs) that explicitly belong to the existing VM. If `-O` is specified, the VMware server is requested to remove the VM before the VM is restored. If not specified, the restore may fail. This option is used with the VClient restore, the Hyper-V restore, and the BMR VM conversion.

`-R rename_file`

Specifies an absolute directory path to a rename file, which is used to restore a VMware virtual machine. The rename file indicates that the restore is to be redirected to an alternate location and specifies details about the alternate client location. For VMware, the rename file can include any of the following entries:

- change `/first_vmdk_path` to `/new_first_vmdk_path`
- change `/second_vmdk_path` to `/new_second_vmdk_path`
- ...     
- change `/n'th_vmdk_path` to `/new_nth_vmdk_path`
- change `vmname` to `NEW_VM_NAME`
- change `esxhost` to `NEW_ESX_HOST`
- change `datacenter` to `NEW_DATACENTER`
- change `folder` to `NEW_FOLDER`
- change `resourcepool` to `NEW_RESOURCEPOOL`
- change `datastore` to `NEW_DATASTORE`
- change `network` to `NEW_NETWORK`
- change `organization` to `NEW_ORGANIZATION`
- change `orgvdc` to `NEW_ORGVDC`
- change `vcdserver` to `NEW_VCDSERVER`
- change `vcdvapp` to `NEW_VCDVAPP`
- change `vcdvapptemplate` to `NEW_VCDVAPPTEMPLATE`
- change `vcdvmname` to `NEW_VCDVMNAME`
- change `vcddcatalog` to `NEW_VCDCATALOG`
Instant Recovery uses the following subset of this list:

change vmname to NEW_VM_NAME
change esxhost to NEW_ESX_HOST
change resourcepool to NEW_RESOURCEPOOL
change network to NEW_NETWORK

The following are notes regarding these entries:

- Enter the change line exactly as it appears in this list, except for the variable at the end (shown in all caps).
- Each change line must end with a carriage return. If the rename_file contains only one entry, make sure that the end of the line contains a carriage return.
- If the rename file has no contents, the restore uses default values from the backup image.
- Use change datastore to NEW_DATASTORE to identify the target datastore when you restore from backups that are not made with Replication Director.
- The rename file must be in UTF-8 character encoding.

With NetBackup 7.7.2 and later, only default paths are allowed for this option and Veritas recommends to use the default paths. If you cannot use the NetBackup default path in your setup, you should add custom paths to the NetBackup configuration.

For more information on how to add a custom path, see the “BPCD_WHITELIST_PATH option for NetBackup servers and clients” topic in the NetBackup Administrator’s Guide, Volume I.

-restorevspec filename

Creates a new virtual machine and restores the NetBackup client and disks that you specify in the filename to the new VM. A special case that is called In-place Disk Restore replaces all disks of an existing VM with the data in its backup. RDM and independent disks are not replaced or deleted. For In-place Disk Restore, the disks are restored to the same disk controller configuration that is acquired at the time of backup. The filename is a text file that uses the JavaScript Object Notation (JSON) format.

The text file must be in UTF-8 character encoding.

You can use the -restorevspecout option to create the JSON-formatted text file. You can edit the text file so that it contains only the virtual machine disks that you want to restore.

The following is an example of the restore parameters that the -restorevspec option requires:

{
"ClientType": "VMware",
"ClientName": "VM-client-name",
"RestoreType": "SelectiveDiskRestore",
"BackupImageSelection": {
  "MasterServer": "Master-server-name",
  "StartDate": "mm/dd/yy hh:mm:ss",
  "EndDate": "mm/dd/yy hh:mm:ss",
  "BackupId": "clientname_timestamp"
},
"VMwareRestoreParameters": {
  "vCenterServer": "vCenter-name-for-restore",
  "VMwareRecoveryHost": "Recovery-host-name",
  "DefaultDiskProvisioning": "thin",
  "TransportMode": "san:hotadd:nbd",
  "VMwareVirtualMachineDestination": {
    "VMName": "Restore-vm-name",
    "AttachDisksToExistingVM": "No",
    "PowerOn": "No",
    "Datacenter": "Path-of-Datacenter-for-destination-vm",
    "ESX": "Hostname-of-the-ESX-host",
    "Folder": "Path-to-destination-VM-folder",
    "ResourcePool/Vapp": "Path-of-vApp-or-resource-pool-destination",
    "VmxDatastore": ""
  },
  "VMwareVirtualDiskDestination": [
    {
      "VirtualDisk": "/DS1/BackedupVM/BackedupVM.vmdk",
      "OverwriteExistingDisk": "No",
      "Datastore": "[Datastore-name]",
      "Path": "",
      "Provisioning": "thin",
      "Controller": "scsi0-0"
    },
    {
      "VirtualDisk": "/DS2/BackedupVM/BackedupVM_1.vmdk",
      "OverwriteExistingDisk": "No",
      "Datastore": "",
      "Path": "[datastore_name] MyVm/MyVM_1.vmdk",
      "Provisioning": "eagerzeroed",
      "Controller": "scsi0-1"
    }
  ]
}
"VMwareAdvancedRestoreOptions": {
  "DeleteRestoredVMOnError": "No",
}
The following is an example of the restore parameters that the `-restorespec` option requires for In-place Disk Restore:

```json
{
  "BackupImageSelection": {
    "StartDate": "05/03/20 21:50:34",
    "BackupId": "bptesx60l-19vm1.rmnus.sen.symantec.com_1588560634",
    "EndDate": "05/03/20 21:50:34",
    "MasterServer": "bptms-lnr73-0029"
  },
  "ClientName": "bptesx60l-19vm1.rmnus.sen.symantec.com",
  "VMwareRestoreParameters": {
    "vmdk_compression": "none",
    "VMwareAdvancedRestoreOptions": {
      "VMShutdownWaitSeconds": 900,
      "DeleteRestoredVMOOnError": "No"
    },
    "VMwareRecoveryHost": "bptms-lnr73-0029",
    "VMwareVirtualMachineDestination": {
      "ResourcePool/Vapp": "/New Datacenter/host/Test01/Resources",
      "VmxDatastore": "datastore1",
      "Datacenter": "/New Datacenter",
      "AttachDisksToExistingVM": "DeleteAllDisksAndReplace",
      "ESX": "bptesx60l-19.rmnus.sen.symantec.com",
      "VMName": "bptesx60l-19vm1",
      "Folder": "/New Datacenter/vm/",
      "PowerOn": "Yes"
    },
    "DefaultDiskProvisioning": "unknown",
    "TransportMode": "nbdssl",
    "VMwareVirtualDiskDestination": [],
    "vCenterServer": "bptesx60l-19vc"
  },
  "ClientType": "VMware",
  "RestoreType": "SelectiveDiskRestore"
}
```

The following itemized lists describe the five sections of the *filename*. The optional sections or optional fields that you do not want to use must be omitted from the *filename*.

First section (required): The opening section of the *filename* provides the required information about the client that contains the disks that you want to restore.

- **ClientType.** The client type as configured in the backup policy. Required. For Vmware virtual machine disk restore, use *VMware*.
- **ClientName.** The client name as configured in the backup policy. Required.
- **RestoreType.** The type of restore. Required. For Vmware virtual machine disk restore, use *SelectiveDiskRestore*.

Second section (optional): The *BackupImageSelection* section of the *filename* specifies the information required to identify the backup image to restore. If this section is not specified, NetBackup restores from the most recent backup. The following are the fields that describe the *BackupImageSelection*:

- **MasterServer.** The fully-qualified domain name of the NetBackup master server to use to query the VM details. Optional. If not specified, the master server that is specified in the NetBackup configuration is used.
- **StartDate.** The start date to look for backup images, in *mm/dd/yy hh:mm:ss* format. If more than one backup image exits in the date range, NetBackup selects the most recent backup. Optional. If not specified, the start date is 6 months earlier than the current date.
- **EndDate.** The end date to look for backup images, in *mm/dd/yy hh:mm:ss* format. If more than one backup image exits in the date range, NetBackup selects the most recent backup. Optional. If not specified, NetBackup uses the current date.
- **BackupId.** The ID of the backup image to use for the restore, in *clientname_backuptime* format. The *backuptime* is the decimal number of seconds since January 1, 1970. Optional. If not specified, NetBackup uses the most recent backup image. If you specify a *StartDate*, *EndDate*, and a valid *BackupId*, NetBackup restores from the *BackupId* image.

Third section (required): The *VMwareRestoreParameters* section of the *filename* specifies the VMware attributes of the virtual disk to be restored. All of the fields in this section are optional; however, the section is required because
it also contains two required subsections. The following are the fields that
describe the VMwareRestoreParameters:

- **vCenterServer.** The host name of the destination vCenter for the restore,
in the same format as specified in the NetBackup Virtual Server
  credentials. Optional. To restore to a standalone ESXi hypervisor when the backup was through
  a vCenter, the value of this field must be None.

- **VMwareRecoveryHost.** The host that performs the restore. Optional. If not specified, NetBackup uses the backup host value from the backup image.

- **DefaultDiskProvisioning.** The default disk provisioning for all of the disks
to be created in the restore VM: thin, thick, eagerzeroed, or unknown. Optional. For each disk, you can override this default by specifying a different
  Provisioning value in the VMwareVirtualDiskDestination section of the filename.
  If neither DefaultDiskProvisioning or Provisioning are specified, NetBackup uses the provisioning as specified in the backup.

- **TransportMode.** The transport mode combination to use for the restore as
  specified in lowercase, colon separated values: hotadd:nbd:nbdssl:san. The order of the specification is significant; NetBackup attempts each
  method in turn until the restore succeeds. If all methods fail, the restore
  fails. Optional. If not specified, NetBackup uses the transport mode combination that was
  used for the backup.

Fourth section (required): The VMwareVirtualMachineDestination section
of the filename specifies the destination parameters for the restore. This
section is subordinate to the VMwareRestoreParameters section. It contains
the following fields:

- **VMName.** The unique display name of the new virtual machine for the restored
disk or disks. The nbrestorevm command adds a timestamp to the name
of the original VM client when it populates this field. The timestamp is the
decimal number of seconds since January 1, 1970. Required. NetBackup restores the virtual machine disks to a new VM. Therefore, if
this name conflicts with an existing display name, the restore fails.

- **AttachDisksToExistingVM.** Determines whether to restore the selected
VMDKs to: an existing VM, a new VM, or replace all the VMDKs on an
existing VM as follows:
- If the value is **Yes**, the VM specified in the `VMName` field must exist in the target vCenter or ESX server. If it does not exist, the restore fails with status code 2820.

- If the value is **No**, the VM specified in the `VMName` field must not exist in the target vCenter or ESX server. If it exists, the restore fails with status code 2820.

- If the value is **DeleteAllDisksAndReplace**, the VM specified in the `VMName` field must exist in the target vCenter or ESX server. If it does not exist, the restore fails with a NetBackup Status Code 2820. The default value is **No**.

- **PowerOn**. Whether to turn on the target VM after the restore, as follows:
  - If the value is **Yes**, the target VM is powered ON at the end of a successful restore.
  - If the value is **No**, the target VM is not turned on after the restore. If the restore is to an existing VM, the VM is turned off before the virtual disks are attached to it during the restore. The default value is **No**.

- **Datacenter**. The name of the VMware **Datacenter** for the virtual disk, in pathname format. Optional. To restore to a standalone ESXi hypervisor when the backup was through a vCenter, the value of this field must be **None**. If not specified, NetBackup uses the value from the backup.

- **ESX**. The name of the ESX host to which NetBackup should restore the virtual disk. Optional. If not specified, NetBackup uses the value from the backup.

- **Folder**. The pathname of the VM folder to which NetBackup should restore the virtual disk. Optional. To restore to a standalone ESXi hypervisor when the backup was through a vCenter, the value of this field must be **None**. If not specified, NetBackup uses the value from the backup.

- **ResourcePool/Vapp**. The pathname of the resource pool to which NetBackup should restore the virtual disk. If the restore is to a vApp, specify the path of the vApp. Optional. If not specified, NetBackup uses the value from the backup.

- **VmxDatastore**. The name of the **Datastore** to which NetBackup should restore the `.vmx` configuration file and other VM configuration files. This Datastore is also used to create the configuration files for the temporary
VM created during restore. You may enclose the name in square brackets but do not have to. Optional. If not specified, NetBackup uses the value from the backup.

- **DefaultDiskDatastore.** The datastore name to which NetBackup should restore all the virtual disks for In-Place Disk Restore. Optional. If not specified, NetBackup uses the value from the backup. This option is only valid for In-place Disk Restore. If this option is specified for other type of selective disk restore, it is ignored.

Fifth section (required, except when the VMwareVirtualDestination AttachDisksToExistingVM parameter is DeleteAllDisksAndReplace. If this option is specified for In-place Disk Restore, the restore validation fails.): The VMwareVirtualDiskDestination section of the filename is an array that specifies the disks to restore and the restore parameters for those disks. This section is subordinate to the VMwareRestoreParameters section. It can contain one or more sets of the following fields, one set per virtual machine disk. A comma must separate fields in a set, and a comma must separate sets.

- **VirtualDisk.** The full pathname of the virtual disk to restore. This path must match exactly the path of the .vmdk file when it was backed up. Required.

- **OverwriteExistingDisk.** Whether to overwrite the existing virtual disk or disks on the target VM, as follows:
  - If the value is **Yes**, overwrite the original virtual disk and retain the disk UUID.
  - If the value is **No**, restore the virtual disk to the target VM as a new disk. VMware assigns a new UUID to the disk. The default value is **No**.

- **Datastore.** The name of the Datastore that is the destination for the restore. You may enclose the name in square brackets but do not have to. (VMware generates the Datastore pathname using the naming conventions for the VM.) Optional. For a restore of virtual disks to a datastore cluster, specify the name of the datastore cluster in this field. If not specified, NetBackup uses the value that is specified in the Path field. If neither Datastore or Path are specified, NetBackup uses the Datastore from the backup image.

- **Path.** The full pathname to the restore destination for the virtual disk, in the following format:
  
  ![Datastore](datastore_name) MyVM/MyVM.vmdk
Optional.
If you specify a Path and it is not available or a disk already exists at that path, the restore fails. If neither Datastore or Path are specified, NetBackup uses the Datastore from the backup image.

- **Provisioning.** The disk provisioning for this specific disk: thin, thick, eagerzeroed, or unknown. Optional.
  If not specified, the NetBackup uses the DefaultDiskProvisioning value.

- **Controller**
  The virtual disk controller to which the disk is attached in the original VM.
  Optional
  This field is informational only to help you determine which virtual disk or disks to restore. The value is not used during a restore.

Sixth section (optional). The VMwareAdvancedRestoreOptions section of the file specifies parameters to restore to an existing VM. This section is subordinate to the VMwareRestoreParameters section.

- **DeleteRestoredVMOnError.** Whether to delete the temporary VM if the disk attach operation fails, as follows:
  - If the value is Yes, delete the temporary VM.
  - If the value is No, do not delete the temporary VM. If the disks are not successfully attached to the target VM, you can access the data on the temporary VM.
  The default value is No. Optional.

- **VMShutdownWaitSeconds.** For restores to an existing VM, the restore process shuts down the target virtual machine before it attaches the disk or disks. The duration of the shutdown operation depends on the VMware workload. Use this parameter to specify how long the restore process should wait for shutdown before giving up on restore.
  The default value is 900 seconds (15 minutes). Optional.

**-restorespecout filename**

Specifies the pathname of the file in which nbrestorevm writes the parameters of the individual virtual machine disk or disks that you want to restore. By default, nbrestorevm creates the file in the current working directory. To specify the backup image from which to obtain the parameters, use the -backupid option or the -s and -e options. If you specify the -s and -e options, NetBackup uses the most recent backup in that date range.

Edit the file so that it contains the appropriate information. Ensure that the VMName field contains the name for the new VM. Ensure that the VMwareVirtualDiskDestination section of the file contains only the virtual
machine disk or disks that you want to restore. Use the edited file as the input file for the `-restorespec` option, which restores the virtual machine disk or disks that are identified in the file.

By default, `nbrestorevm` creates the file in the current working directory. To create the file in a different directory, specify a pathname for the `filename`. That path must be in the NetBackup whitelist of paths. For more information on how to add a custom path, see the "BPCD_WHITELIST_PATH option for NetBackup servers and clients" topic in the NetBackup Administrator's Guide, Volume I.

- `-S master_server`
  Specifies a different master server to restore a virtual machine from a backup that was made by that master.

- `-s mm/dd/yyyy [hh:mm:ss] -e mm/dd/yyyy [hh:mm:ss]`
  Limits the selectable backup images to those with timestamps that fall within the specified period. NetBackup selects the latest suitable backup image within the range. Specifies the start date (-s) and end date (-e) for the listing. The start date and end date signify the time range to search for a valid backup image. The latest valid backup image within the specified time range is used to perform restores. These options are used with all functions except the BMR VM conversion.

- `-temp_location temp_location`
  Specifies a temporary datastore on the VM host server where all writes occur until the virtual machine is restored. All writes occur on this datastore until Storage vMotion is complete or until you are finished with the virtual machine (such as for troubleshooting). This datastore must exist before you run `nbrestorevm`. This option can be used only with `-ir_activate`. This option is used only with Instant Recovery.

- `-validate -restorespec filename`
  Validates the virtual machine disk restore parameters in the `filename`. The `-restorespec` option is required, and it must follow the `-validate` option.

  For a description of the `filename`, see the `-restorespec` option description.

- `-vcd`
  Restores a vCloud virtual machine. This option is required when you restore to the original location or to an alternate location in vCloud.

- `-vcdlfree`
  Restores a vCloud virtual machine by using the datastore with the largest available space. This option applies only to the restore operations that are not directed to the original location.
-vcdovw
   Overwrites the existing vCloud vApp.

-vcdred
   Redirects the vCloud restore.

-vcdremv
   Removes the vApp if you use the -vcdtemplate option to save the vApp as a template.

-vcdrte
   Restores a vCloud virtual machine to an existing vCloud vApp. This option is required when you restore to an existing vApp including an original location restore.

-vcdtemplate
   Restores a vCloud virtual machine as a template.

-veconfig ve_config_filepath
   Full (absolute) file path that contains the virtual environment details in param=value format. A veconfig file typically contains the following entries:

   esxhost="bmresx.xyz.com"
   name="Test_NBRestoreVM"
   network="VM Network"
   nbrestorediskformat="ThinVdisk"
   toolsIsoPath="C:\B2V\windows_esx5.iso"
   datacenter="/Test/XyzDatacenter"
   folder="/Test/XyzDatacenter/vm"
   resourcepool="/Test/XyzDatacenter/host/bmresx.xyz.com/Resources/resourcepoolname"
   harddisk=0:"B2V_4TB"
   harddisk=1:"storage1 (2)"
   harddisk=2:"storage2 (1)"

The following are notes regarding these entries:

- The folder, resourcepool, and diskformat fields are optional.
- The VM conversion on a standalone esx server uses the following values:

   datacenter="ha-datacenter"
   resourcepool="/ha-datacenter/host/esx_host_name/Resources"

- To create all VMDKs corresponding to disks on the same datastore, define the datastore name by using the entry datastore="datastoreName".
To create VMDKs on different datastores, populate the `veconfig` file as shown in the sample file above (`harddisk=0...`).

- `vmbz`
  Disk format of the restored disk will be 'eager zero'

- `vmfd`
  Restores the VMDK files as flat disks.

- `vmhost vm_host`
  Specifies the VM host on which the virtual machines were mounted when you reactivate virtual machines.

- `vmhv`
  Restores a Hyper-V virtual machine at the original location.

- `vmhvnew`
  Restores a Hyper-V virtual machine to a new location.

- `vmhstage`
  Restores Hyper-V virtual machine files to a staging location.

- `vmid`
  Restores the BIOS UUID of the virtual machine instead of creating a new one.

  **For VMware:** Restores the BIOS UUID of the virtual machine instead of creating a new one.

  **For Hyper-V:** Restores the GUID of the virtual machine instead of creating a new one.

  **Note:** For Hyper-V, when you restore to the original location or to a staging location, the virtual machine’s original GUID is restored. This behavior is true even if the `vmid` option is omitted.

- `vmInstanceId`
  Retains the Instance UUID of the original virtual machine (note that the Instance UUID is a vCenter specific unique identifier of a virtual machine). The virtual machine is restored with the same Instance UUID that it had when it was backed up.

  If the restore of the virtual machine is to a standalone ESXi host, this option is ignored.

  If a virtual machine with the same Instance UUID exists at the target restore location, NetBackup assigns a new UUID to the virtual machine.
-vmkeepv
Retains the hardware version upon recovery. This option applies only to VMware VM recovery.

-vmnewdiskuuid
Generate new virtual machine disk UUIDs during an instant recovery. Use this option with the \texttt{--ir\_activate} option.

The VMs that activate with this option do not retain the new vmdk UUID during a subsequent \texttt{--ir\_reactivate} operation. In such a scenario, the VMDKs revert to their UUIDs at the time of the backup.

-vmncf
Specifies that you do not want to restore the common files when you restore the Hyper-V virtual machine.

-vmpo
Automatically powers up the virtual machine after the restore operation.

-vmproxy VMware\_access\_host
Specifies the VMware access host. It overrides the default VMProxy used for backing up the virtual machines.

Storage lifecycle policies (SLPs) can use Auto Image Replication to replicate a virtual machine backup image to another NetBackup domain. To restore the virtual machine from the replicated image, you must include the \texttt{--vmproxy} option. Use the \texttt{--vmproxy} option to specify the backup host (access host) that is in the domain where the virtual machine was replicated.

-vmrb
Removes any mounted removable devices such as cd-rom or dvd-rom images.

-vmserver VMServer
Specifies a different target location for the restore operation (for example, ESX server or vCenter). It overrides the default VM server used for backing up the virtual machines. To restore to the same vCenter where the virtual machine originally resided, omit this option.

-vmsn
Strips the network interface of the virtual machine.

-vmst
Strips the VMware tags from the restore.

-vmtd
Disk format of the restored disk will be 'thin'.
Specifies the VMware transport mode. An example of the format of `vm_transport_mode` is `san:hotadd:nbd:nbdssl`.

Allows the VMware VMDK files to be restored to the same datastore where the VMX file is specified. A rename file that assigns a different vmdk file path overrides this option.

Restores a VMware virtual machine.

Causes NetBackup to wait for a completion status from the server before it returns you to the system prompt.

The required date and time values format in NetBackup commands varies according to your locale. The `/usr/openv/msg/.conf` file (UNIX) and the `install_path\VERITAS\msg\LC.CONF` file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

See the "About specifying the locale of the NetBackup installation" topic in the NetBackup Administrator’s Guide, Volume II.

You can optionally specify a wait time in hours, minutes, and seconds. The maximum wait time you can specify is 23:59:59. If the wait time expires before the restore is complete, the command exits with a timeout status. The restore, however, still completes on the server.

If you specify 0 or do not specify a time, the wait time is indefinite for the completion status.

**EXAMPLES**

**VSphere Examples**

Example 1 - Restore the specified virtual machine from its latest backup image. If a VM with the same name already exists, this command fails.

```
# nbrestorevm -vmw -C client1
```

To overwrite an existing VM with its latest backup image, execute the following command:

```
# nbrestorevm -vmw -C client1 -O -S master_server
```
Example 2 - Restore a VM to an alternate location that `rename_file` specifies. The latest available backup image is selected from the range between `start_time` and `end_time`. The VM is powered on after the restore operation and is overwritten at the alternate location if it already exists.

```
# nbrestorevm -vmw -S server1 -C client1 -R rename_file -s start_time -e end_time -vmpo -O
```

Example 3 - Restore a virtual machine to the original vApp in vCloud Director.

```
# nbrestorevm -vmw -S server1 -vcd -C vm_client -vmserver vm_server -vmproxy vm_proxy -vcdrte
```

To restore multiple virtual machines into the original vApp, run this `nbrestorevm` command for each virtual machine.

Example 4 - Restore multiple virtual machines into a vApp template

Run the command in Example 3 to restore each of the virtual machines into a non-template vApp, but do not restore the last virtual machine.

To restore the last virtual machine and copy all the restored virtual machines into a vApp template, run the following command:

```
# nbrestorevm -vmw -S server1 -vcd -C vm_client -vmserver vm_server -vmproxy vm_proxy -R rename_file -vcdtemplate -vcdremv -vcdlfree
```

`-R rename_file` is the full path to a text file that contains the following entry ending in a carriage return:

```
change vcdvapp to vApp_template_file
```

The `-vcdremv` option removes the non-template vApp into which you restored the virtual machines. The `-vcdlfree` option selects the datastore that has the largest available space. The `nbrestorevm` command in this example (with the rename file) creates a vApp template and copies the restored virtual machines into that template. No further virtual machines can be added to the template.

Example 5 - Restore a VM to an alternate location that `rename_file` specifies. The latest available backup image is selected from the range between `start_time` and `end_time`. The operation powers on the VM after the restore operation and overwrites the VM at the alternate location if it already exists.

```
nbrestorevm -vmhvnew -S srvrl -C client1 -R rename_file -s start_time -e end_time -O
```

Example 6 - Restore VM files from the latest backup to the staging location.

```
# nbrestorevm -vmhstage -C vm_client -R rename_file
```
BMR Example

Example 7 - Perform a BMR VM conversion of a client configuration to a VM server and power on the converted VM:

# nbrestorevm -bmr -vmw -C client1 -vmserver VmServer1 -vmproxy d86-12.xyz.com -veconfig C:\B2V\veconfig.txt -O -vmpo

Instant Recovery Examples

Example 8 - Perform a set of nbrestorevm commands in a typical sequence of Instant Recovery operations.

Initiate Instant Recovery by activating the virtual machine. Required parameters are shown. Other optional parameters are shown in Synopsis.

VMware example:

# nbrestorevm -vmw -ir_activate -C client1 -temp_location temploc1

List details about the activated virtual machine.

# nbrestorevm -ir_listvm

Deactivate or delete virtual machine whose ir_identifier is 26.

# nbrestorevm -ir_deactivate 26

Complete the VM instant recovery job for ir_identifier 14 after the data is migrated.

# nbrestorevm -ir_done 14

Reactivate VM with ir_identifier 11 or reactivate all virtual machines that are interrupted during recovery.

# nbrestorevm -ir_reactivate 11 -force

or

# nbrestorevm -ir_reactivate_all -vmhost host1 -media_server msvm2 -force

SEE ALSO

See bprestore on page 382.
nbseccmd

nbseccmd – run the NetBackup Security Configuration service utility

SYNOPSIS

nbseccmd -drpkgpassphrase
nbseccmd -getNBKeysize [-server master_server_name] [-json]
nbseccmd -getsecurityconfig -insecurecommunication | -autoaddhostmapping [-masterserver master_server_name]
nbseccmd -nbcalist [-state value] [-json]
nbseccmd -nbcaMigrate -initiateMigration | -i -keysizer key_value
-activateNewCA | -a -completeMigration | -c -decommissionCA | -d
-fingerprint certificate_fingerprint -summary | -s
-hostsPendingTrustPropagation | -pt -syncMigrationDB | -S
-hostsPendingRenewal | -pr [-reason description_for_auditing] [-json]
[-force] [-quiet]
nbseccmd -setsecurityconfig -insecurecommunication on|off |
-autoaddhostmapping on|off [-masterserver master_server_name]
nbseccmd -setuptrustedmaster -add | -update | -remove -masterserver master_server_name -remotemasterserver remote_master_server
[-domainname domain_name] [-username username] -fpfile filename
nbseccmd -setuptrustedmaster -add | -update | -remove -info answer_file

nbseccmd -help

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\

DESCRIPTION

Use the nbseccmd command to establish trust relationships among various master servers.
You must have root or administrator permissions to use this command if NetBackup Access Control (NBAC) is enabled.

**Note:** If the source or the target master server version is NetBackup 8.0 or earlier, please refer to the *NetBackup Commands Guide* for 8.0 or earlier. The command underwent a number of changes for NetBackup 8.1.

### OPTIONS

- **-activatenewca | -a**
  
  Use this option to activate the new NetBackup CA that can start issuing NetBackup certificates going forward.

- **-autoaddhostmapping [on|off]**
  
  Use this option to manage the addition of host ID to the host name or the IP addresses that the master server automatically detects.

  Hosts may have multiple host names or IP addresses associated with them. For successful communication among hosts, all relevant host names and IP addresses must be mapped to the respective host IDs. During communication, NetBackup may detect new host names or IP addresses with respect to a host ID.

  When you use the `-getsecurityconfig`, the option takes no parameters, and reports the current setting for the `-autoaddhostmapping` value.

  When you used the `-setsecurityconfig` option, this option enables or disables automatic host mapping. Use the `on` parameter to automatically map the host ID to the host name or the IP addresses detected. Disable this action with the `off` parameter.

- **-completeMigration | -c**
  
  Use this option to complete the NetBackup CA migration process that cleans up the migration status on the master server.

- **decommissionCA | -d**
  
  Use this option to decommission the NetBackup CA with the given fingerprint.

- **-domainname domain_name**
  
  Specifies the domain to which the user that is specified in `-username` belongs. You are prompted to enter a password to validate the credentials of the remote master server host.

  The `-domainname` option is mandatory for a target master server that uses NetBackup certificates.
-drpkgpassphrase

The -drpkgpassphrase option is used to specify the passphrase that is used to encrypt disaster recovery packages. If a passphrase already exists, it is overwritten.

Note: You must set the passphrase for successful catalog backups. Failure to set the passphrase results in failed catalog backups.

The disaster recovery package stores the identity of the NetBackup master server and is created during each catalog backup.

These packages are encrypted with the passphrase that you specify here. You must provide this passphrase when you reinstall NetBackup on the master server after a disaster.

Before using this command, you must run the bpnbat command to log on:

bpnbat -login -loginType WEB

When you set the passphrase, please note:

- Passphrase must contain a minimum of eight characters and a maximum of 1024 characters.
- The existing passphrase and the new passphrase must be different.
- You must be an authorized user with administrator or root privileges or you must be an Enhanced Auditing user to run the nbseccmd -drpkgpassphrase command.
- Only the characters that are listed are supported for the passphrase:
  - White spaces
  - Uppercase and lowercase characters (A to Z, a to z)
  - Numbers (0 to 9)
  - The special characters shown: ~ ! @ # $ % ^ & * ( ) _ + - = ` { } [ ] | : ; '",./)?<>}

Caution: If you enter an unsupported character, you may face issues during disaster recovery package restore. The passphrase may not be validated and you may not be able to restore the disaster recovery package.

-fingerprint certificate_fingerprint

Specifies the fingerprint of the NetBackup CA that needs to be decommissioned. Use this option with -decommissionCA.
-fpfile filename
This option accepts the root certificate fingerprint information that is required for validating the root certificate of the remote master server. You can store the fingerprint details in a text file.

-force
Suppresses the confirmation prompts. The -force option skips the check for the hosts awaiting trust propagation or certificate renewal. The -force option activates the new CA and completes the migration. Use this option with -completeMigration and -activatenewCA.

-getsecurityconfig -autoaddhostmapping | -insecurecommunication
Use this option to get the security configuration information for NetBackup. When you use the -autoaddhostmapping option, you get the value for the -autoaddhostmapping option. When you use the -insecurecommunication option, you get the value for the -insecurecommunication option.

-hostsPendingRenewal | -pr
Use this option to retrieve the list of hosts that require certificate renewal.

-hostspendingtrustpropagation | -pt
Use this option to retrieve the list of hosts that do not have the required CA certificates in their trust stores.

-info answerfile
The -info option accepts the information that is required for setting up a trusted master server. The information is stored in an answer file, which is a text file. It contains the following entries:

masterserver:
remotemasterserver:
trusttype:
domainname:
username:
password:
token:
fpfile:

The password is optional in the answer file. If you do not provide a password, you are prompted for the password when you run the command.
Note: The trusttype value is valid only for master servers at version 8.0 and earlier. Possible values for trusttype are mutualtrust, remoteonly, and localonly. The trusttype of localonly does not require a domain name or user credentials.

The entries in your answer file must match the format that is shown in the example.

Example sample file:

masterserver:testmaster1
remotemasterserver:testmaster2
trusttype:mutualtrust
domainname:testdomain
username:Administrator
password:abc123

-initiateMigration | -i
Use this option to initiate the NetBackup certificate authority (CA) migration. It sets up a new CA for NetBackup with the specified certificate key size. The new CA runs in a stand-by mode until the CA is activated or the migration status moves to ACTIVATED.

This operation does not change the root CA.

Before initiating the CA migration, confirm that you do not have media servers with NetBackup versions 8.1.2.1 or earlier that are configured as cloud storage servers. Backups on these media servers fail.

-insecurecommunication [on | off]
Use this option to manage insecure communication within your NetBackup environment. The on parameter enables insecure communication with all NetBackup hosts that are present in the NetBackup environment. Disable insecure communication with the off parameter.

Veritas implemented new security features in 8.1 which are not present in NetBackup 8.0 and earlier. NetBackup communicates with 8.0 and earlier hosts insecurely. For increased security, upgrade all your hosts to the current version of NetBackup, and then use this option with the on parameter. This action ensures that only secure communication is possible between NetBackup hosts.

-json
Prints the data in JSON format on a single line.
-keysize  \textit{key\_value}

Use this option with the -initiateMigration option to specify the certificate key size for a new NetBackup CA that you want to set up. The key size must be one of the sizes shown: 2048, 4096, 8192, or 16384 bits.

-masterserver  \textit{master\_server\_name}

Specifies the name of the master server that the user has logged into. Auto Image Replication uses this name for the current master server or the source master server.

-nbcamigrate

Migrates the existing NetBackup CA to a new one.

-nbcalist

Use this option to list the NetBackup CAs in your NetBackup domain.

-quiet

Suppresses the prompt message to proceed further. You can use this option with the -initiateMigration option.

-reason  \textit{description\_for\_auditing}

Specifies the reason that is stored in the audit record for this operation.

-remotemasterserver  \textit{remote\_master\_server}

Specifies the name of the remote master server with whom the trust is to be established. Auto Image Replication uses this name for the target master server.

-remoteonly | -localonly | -mutualtrust

Specifies the way that a trust must be established. Either the local master (source) trusts the remote master (target) or vice versa. If neither of these options is specified, a two-way trust (-mutualtrust) is established.

-setsecurityconfig -autoaddhostmapping | -insecurecommunication

Use this option to set the security configuration information for NetBackup. When you use the -autoaddhostmapping option, you set the behavior for the addition of host names and IP addresses. When you use the -insecurecommunication option, you set the behavior for secure communication.

-setuptrustedmaster -add | -update | -remove

Add, update, or remove inter-domain trust across master servers. To update a trust relationship, run the -update option on both the source and the target server. Both servers must be on version 8.1 or later. You must use the -update option if after you establish a trust, you upgrade the source or the target master server to version 8.1 or later. To remove a trusted master server, the domain, user name, and password are not required.
You can update the trust with external certificate to the trust with NetBackup certificate and vice versa.

You must run the `bpnbat` command to remove a trusted master before you can use the `-setuptrustedmaster` option. Log on locally on the master server you want to remove and use the `bpnbat` command as shown:

```
bpnbat -login
```

To remove the trust that is added using an external certificate, you do not need to run the `bpnbat -login` command.

```
-bpnbat -login
```

- `-state value`

Use this option with the `-nbcaList` option to retrieve NetBackup CAs of a particular state, for example: `ACTIVE`, `ABANDONED`, or `DECOMMISSIONED`. Use comma-separated states to filter the result with more than one state.

- `-summary`

Retrieves the NetBackup CA migration information. It shows the current NetBackup CA migration status and the fingerprint of the current certificate-issuing NetBackup CA.

- `syncMigrationDB | -S`

Updates the CA migration database with the current NetBackup CA certificate details.

- `-username username`

Specifies the logon user name of the remote master server host. This option is used with the `-domainname` option. You are prompted to enter a password to validate the credentials of the remote master server host. If you specify only the domain name, you are prompted to enter the Authorization Token of the remote master server.

The `-username` option is mandatory for the target master server that uses NetBackup certificate.

**EXAMPLES**

**Example 1 - Set up a trusted master server using user credentials.**

```
nbseccmd -setuptrustedmaster -add -masterserver testmaster1
-remotemasterserver testmaster2 -domainname testdomain -username Administrator
Password:******
```

The SHA1 fingerprint of root certificate is

```
```
Are you sure you want to continue using this certificate? (y/n): y

The validation of root certificate fingerprint is successful.
CA certificate stored successfully from server testmaster2.
testdomain.com.
Host certificate received successfully from server testmaster2.
testdomain.com.
Trusted master operation successful.

Example 2 – Set up a trusted master server using authentication token.
nbseccmd -setuptrustedmaster -add -masterserver testmaster1
-remotemasterserver testmaster2 -domainname testdomain
Authorization Token:*****
The SHA1 fingerprint of root certificate is
Are you sure you want to continue using this certificate? (y/n): y
The validation of root certificate fingerprint is successful.
CA certificate stored successfully from server testmaster2.
testdomain.com.
Host certificate received successfully from server testmaster2.
testdomain.com.
Trusted master operation successful.

Example 3 - Set up a trusted master server using -fpfile.
nbseccmd -setuptrustedmaster -add -masterserver testmaster1
-remotemasterserver testmaster2 -domainname testdomain -username Administrator
-fpfile C:\fp_file
Password:*****
The validation of root certificate fingerprint is successful.
CA certificate stored successfully from server testmaster2.
testdomain.com.
Host certificate received successfully from server testmaster2.
testdomain.com.
Trusted master operation successful.

Example 4 - Set up a trusted master server using an answer file.
nbseccmd -setuptrustedmaster -add -info C:\nbseccmd_answerfile.txt
The validation of root certificate fingerprint is successful. CA certificate stored successfully from server testmaster2. testdomain.com. Host certificate received successfully from server testmaster2. testdomain.com. Trusted master operation successful.

Example 5 - Update trust after you upgrade both the source and the master server to version 8.1 and later.

-setuptrustedmaster -update -masterserver testmaster1 -remotemasterserver testmaster2
Authorization Token:
Authenticity of root certificate cannot be established.
The SHA1 fingerprint of root certificate is finger_print_details
Are you sure you want to continue using this certificate? (y/n): y
The validation of root certificate fingerprint is successful. CA certificate stored successfully from server testmaster2. Host certificate received successfully from server testmaster2. Trusted master operation successful

Example 6 - Remove a trusted master server.

-setuptrustedmaster -remove -masterserver testmaster2 -remotemasterserver testmaster1
Certificate revoke request processed successfully. Trusted master operation successful
nbsetconfig

nbsetconfig — update a NetBackup configuration

SYNOPSIS

nbsetconfig [-h host] [-u user] [filename,...] [-r "reason"]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

The nbsetconfig command is used to update a configuration. This command is available for all NetBackup platforms.

You must have administrator privileges to run this command.

OPTIONS

filename,...
   Specifies the file or files where the updates are listed. If not specified, the standard input is read.

-h host
   Specifies the host name of the server or client whose configuration you update.

-r "reason"
   Indicates the reason why you choose this command action. The reason text string that you enter is captured and appears in the audit report. Enclose this string with double quotes ("..."). The string must not exceed 512 characters. It cannot begin with a dash character (-) nor contain a single quotation mark (').

-u user
   Specifies the user whose configuration you update.

EXAMPLE

Set the NetBackup configuration on the system to the designated servers. The master server is yellow.colors.org and the media server is orange.colors.org.
# nbsetconfig
SERVER = yellow.colors.org
SERVER = orange.colors.org

To escape on UNIX, press:

Ctrl+D

To escape on Windows, press:

Ctrl+Z

SEE ALSO

See nbgetconfig on page 714.
See bpgetconfig on page 158.
See bpsetconfig on page 416.
nbsnapimport

nbsnapimport – import a snapshot copy on a storage server

SYNOPSIS

nbsnapimport -backupid backup_id -cn copy_number -fim fim_name -stunit storage_unit [-mounthost mount_host]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\

DESCRIPTION

The nbsnapimport command imports a snapshot copy in NetBackup so that it can
be used to browse, restore, or create a NetBackup (tar) copy.

This command can be run only on the master server.

OPTIONS

-backupid backup_id
   Specifies the backup ID of a single backup image.

-cn copy_number
   Determines the copy number to import. Valid values are 1 through 10. The
default is 1.

-fim fim_name
   Specifies the snapshot method to use to create the image. Select the method
by using the type of data and hardware that the client uses.

For details on snapshot methods, refer to the NetBackup Snapshot Client
Administrator’s Guide.

The available options depend on the snapshot method. For a list of snapshot
methods and their options, refer to the opt_params area of each snapshot
method (FIM) listed in the vfm.conf file.

-mounthost mount_host
   Specifies the mount host where the snapshot copy will be imported.
-stunit storage_unit
    Specifies the storage unit.

FILES

UNIX systems:

/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/db/images/*

Windows systems:

install_path\NetBackup\db\images/*
install_path\NetBackup\logs\admin/*
nbsnapreplicate

nbsnapreplicate – initiate snapshot replication on a storage server

SYNOPSIS

nbsnapreplicate -backupid backup_id | -Bidfile filepath -cn copy_number -rcn replicate_copy_number -slpname policy_name -stunit storage_unit [-mediaServer media_server] [-priority number] [-v]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The nbsnapreplicate command allows a copy of a backup to be created.
This command can be run only on the master server.
Use nbsnapreplicate to create up to 10 copies of unexpired backups.

OPTIONS

-backupid backup_id
    Specifies the backup ID of a single backup to replicate.

-Bidfile file_name
    file_name specifies a file that contains a list of backup IDs to be replicated. List one backup ID per line in the file. If this parameter is specified, other selection criteria are ignored.

Also, file_name is removed during the execution of that command line interface (CLI), because the NetBackup GUIs commonly use this parameter. They expect the CLI to remove the temporary file that was used for the -Bidfile option upon completion. Direct CLI users can also use the option; however, it removes the file.

-cn copy_number
    Determines the copy number to replicate. Valid values are 1 through 10. The default is 1.
-mediaServer media_server
    Specifies the media server.

-priority number
    Sets a backup policy to run at a lesser or a higher priority than disk staging
duplication.

-rcn replicate_copy_number
    Specifies the copy number of the snapshot replication. The copy number is
the operation index value of the storage lifecycle policy replication operation
plus 100.

-slp_name policy_name
    Specifies the storage lifecycle policy name of the duplicated file.

-stunit storage_unit
    Specifies the storage unit.

-v
    Selects the verbose mode. When you specify the debug logs or progress logs,
the output includes more information.

EXAMPLES

Example 1 - List backups with a copy number of 1. They were backed up by the
policy that is named stdpol, and created between July 1, 2009, and August 1,
2009.

# nbsnapreplicate -cn 1

Example 2 - Create a duplicate copy of the backup IDs in file name plum. It
duplicates copy 1 to copy 5 on storage unit Tape_stu of pool Pool1.

# nbsnapreplicate -Bidfile plum dstunit Tape_stu -dp Pool1 -cn 1 -dcn 5

FILES

UNIX systems:

/usr/openv/netbackup/logs/admin/*
/usr/openv/netbackup/db/images/*

Windows systems:

install_path\NetBackup\db\images/*
install_path\NetBackup\logs\admin/*
nbsqladm

nbsqladm – configure SQL Server instances for a SQL Server Intelligent backup policy

SYNOPSIS

nbsqladm [-S master_server] -list_instances [instance_name] [-host name] [-active | -inactive] [-registered | -unregistered]
nbsqladm [-S master_server] -add_instance instance_name -host name
             [-instance_group name | -local_credentials | -user name -domain name] [-force]
nbsqladm [-S master_server] -register_instance instance_name [-host name]
             [-instance_group name | -local_credentials | -user name -domain name] [-force]
nbsqladm [-S master_server] -delete_instance instance_name [-host name]
nbsqladm [-S master_server] -modify_instance instance_name -host name
             [-instance_group name | -local_credentials | -user name -domain name]
             [-active | -inactive] [-force]
nbsqladm [-S master_server] -remove_from_instance_group instance_name
             [-instance_group name] [-host name]
nbsqladm [-S master_server] -initiate_availability_group_browse instance_name -host name
nbsqladm [-S master_server] -initiate_discovery
nbsqladm [-S master_server] -list_instance_groups [instance_group_name]
nbsqladm [-S master_server] -add_instance_group instance_group_name
             [-local_credentials | -user name -domain name]
nbsqladm [-S master_server] -delete_instance_group name
nbsqladm [-S master_server] -modify_instance_group name
             [-new_instance_group name] [-local_credentials | -user name -domain name]
             [-validate]
nbsqladm [-S master_server] -list_availability_groups [-ag_name name]
             [-cluster cluster_name] [-ag_id availability_group_ID]
DESCRIPTION

The nbsqladm command configures SQL Server instances, instance groups, and availability groups for use with a SQL Server Intelligent Policy. Supported availability groups include basic, advanced, and read-scale. You can also use this command on the master server to authorize DBAs to use the nbsqladm on a specific host.

You can disable or enable the nbsqladm command with the ENABLE_NBSQLADM option in the bp.conf file or in the registry. This command is enabled by default. To disable the command, use ENABLE_NBSQLADM=0.

nbsqladm [-S master_server] -add_availability_group -ag_name name {-cluster cluster_name | -ag_id availability_group_ID} [-instance instance_name -host name]

nbsqladm [-S master_server] -delete_availability_group -ag_name name {-cluster cluster_name | -ag_id availability_group_ID}

nbsqladm [-S master_server] -list_replicas -ag_name name {-cluster cluster_name | -ag_id availability_group_ID}

nbsqladm [-S master_server] -add_replica -ag_name name {-cluster cluster_name | -ag_id availability_group_ID} -instance instance_name -host name [-force]

nbsqladm [-S master_server] -delete_replica -ag_name name {-cluster cluster_name | -ag_id availability_group_ID} -instance instance_name -host name

nbsqladm [-S master_server] -list_dbas

nbsqladm [-S master_server] -add_dba host_name user_name

nbsqladm [-S master_server] -delete_dba host_name user_name

nbsqladm [-S master_server] -auto_registration instance_group_name

nbsqladm [-S master_server] -disable_auto_registration

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\
OPTIONS

-add_availability_group -ag_name name {-cluster cluster_name | -ag_id availability_group_ID} -instance instance_name -host name

Add an availability group to the NetBackup catalog. You can add only the availability group and at a later point add the instances. This way you can build the availability group topology more quickly. For advanced and basic availability groups provide the -cluster cluster_name, which is the name of the Windows Server Failover Clustering (WSFC) cluster. For read-scale availability groups provide the -ag_id availability_group_ID.

To add the full AG topology including the instances, use the -instance instance_name -host name option.

-add_dba host_name user_name

Authorizes the specified DBA (user_name) to use the nbsqladm command on a specific host (host_name). Can only be used on the master server.

If you have multiple NICs, provide the private interface name of the SQL Server host.

For a SQL Server cluster, authorize the DBA for each node in the cluster. (Do not authorize a DBA using the virtual name of the SQL Server cluster.) For the -host name provide one of the node names in the SQL Server cluster.

For a SQL Server cluster with multiple NICs, authorize the DBA using the private interface name for each of the nodes in the SQL Server cluster.

-add_instance instance_name -host name [-instance_group name | -local_credentials | -user name -domain name] [-force]

Add an instance to the NetBackup catalog. After you add an availability group instance, use the -add_replica option.

-add_instance_group instance_group_name [-local_credentials | -user name -domain name]

Add an instance group to the NetBackup catalog. You can add credentials to the instance group with the -local_credentials or the -user name -domain name option.

-auto_registration instance_group_name

Enables the automatic registration for the named instance group. Newly discovered instances are automatically registered with the group credentials and added to the instance group. If you want any instances that were previously discovered to be included in the instance group, you must add those instances manually. Only one instance group can be enabled for automatic registration.
-add_replica -ag_name name (-cluster cluster_name | -ag_id availability_group_ID) -instance instance_name -host name [-force]

Add a replica of an availability group to the NetBackup catalog. Use this option after you add the availability group instance. For advanced and basic availability groups provide the -cluster cluster_name, which is the name of the Windows Server Failover Clustering (WSFC) cluster. For read-scale availability groups provide the -ag_id availability_group_ID.

-delete_dba host_name user_name

Removes the authorization to use the nbsqladm command for the specified host (host_name) and DBA (user_name). Can only be used on the master server.

If you have multiple NICs, provide the private interface name of the SQL Server host.

For a SQL Server cluster, remove authorization for the DBA for each node in the cluster. (You cannot remove authorization for a DBA using the virtual name of the SQL Server cluster.) For the -host_name provide one of the node names in the SQL Server cluster.

For a SQL Server cluster with multiple NICs, remove authorization using the private interface name for each of the nodes in the SQL Server cluster.

-delete_availability_group -ag_name name (-cluster cluster_name | -ag_id availability_group_ID)

Delete an availability group from the NetBackup catalog. For advanced and basic availability groups provide the -cluster cluster_name, which is the name of the Windows Server Failover Clustering (WSFC) cluster. For read-scale availability groups provide the -ag_id availability_group_ID.

-delete_instance instance_name [-host name]

Delete an instance from the NetBackup catalog.

-delete_instance_group name

Delete an instance group.

-delete_replica -ag_name name (-cluster cluster_name | -ag_id availability_group_ID)

Delete a replica of an availability group from the NetBackup catalog. For advanced and basic availability groups provide the -cluster cluster_name, which is the name of the Windows Server Failover Clustering (WSFC) cluster. For read-scale availability groups provide the -ag_id availability_group_ID.

-disable_auto_registration

Disables the automatic registration so that newly discovered instances are not automatically registered and added to an instance group.
-force
Forces NetBackup to register the instance or the replica instance and skip the validation of the instance credentials. NetBackup for SQL Server cannot protect any instances that are not registered or that have invalid credentials.

-host name
Specifies the name of the host where the SQL Server database resides.
If you have multiple NICs, provide the private interface name of the SQL Server host. For a SQL Server cluster, for the host name provide the virtual name of the SQL Server cluster. For a SQL Server cluster with multiple NICs, provide the private virtual name of the SQL Server cluster.

-instance instance_name
Specifies the name of the SQL Server instance.

-instance_group name
Specifies the name of the instance group to which you want to add or remove an instance.
Or indicates that the instance group you want to use to register an instance. Alternatively, you can register an instance with instance group credentials or specific credentials. Also see the -local_credentials and -user name -domain name options.
The credentials must have certain security privileges. See the NetBackup for SQL Server Administrator's Guide.

-initiate_availability_group_browse instance_name -host name
Initiates discovery of a read-scale availability group. Any availability groups associated with the instance_name and host are discovered.

-initiate_discovery
Start the discovery process to discover any SQL Server instances that were added to your environment since the last discovery.

-list_availability_groups [-ag_name name] [-cluster cluster_name] [-ag_id availability_group_ID]
List the SQL Server availability groups in the NetBackup catalog. To list an availability group with a specific name, use -ag_name name. To list an advanced or a basic availability group that is part of a specific Windows Server Failover Clustering (WSFC) cluster, use -cluster cluster_name. To list read-scale availability groups, use the -ag_id availability_group_ID.

-list_dbas
Display a list of all database administrators (DBAs) able to use nbsqladm. Can only be used on the master server.
-list_instances [instance_name] [-host name] [-active | -inactive] [-registered | -unregistered]

List all SQL Server instances in the NetBackup catalog.

Use instance_name or -host name to list a specific instance. Use -registered or -unregistered to list the registered or unregistered SQL Server instances. The options -active and -inactive to display the instances that are active for NetBackup (available for backup) and the inactive instances.

-list_instance_groups [instance_group_name]

List the SQL Server instance groups that exist. Use instance_group_name to list a specific instance group.

-list_replicas -ag_name name {-cluster cluster_name | -ag_id availability_group_ID}

List all availability group replicas in the NetBackup catalog. The -ag_name name option indicates the availability group. To list replicas in an advanced or a basic availability group that is part of a specific Windows Server Failover Clustering (WSFC) cluster, use -cluster cluster_name. For read-scale availability groups, use -ag_id availability_group_ID.

-local_credentials

Indicates that you want to register an instance with the credentials that were used to install NetBackup. Alternatively, you can register an instance with instance group credentials or specific credentials. See the -instance_group name and -user name -domain name options.

The credentials must have certain security privileges. See the NetBackup for SQL Server Administrator’s Guide.

When it is used with the -validate option to modify an instance group you can also validate the credentials for each instance in the group.

-modify_instance instance_name -host name [-instance_group name | -local_credentials | -user name -domain name] [-active | -inactive] [-force]

Change the attributes of the specified instance.

Use -active to make an instance that you deactivated in NetBackup available for backup. Or you can make an instance inactive in NetBackup with -inactive. For example, if the instance is under maintenance.

The options -new_instance and -new_host are deprecated. To change an instance or a host name, delete the instance and use the -add_instance option to add the instance again.
-modify_instance_group [-new_instance_group name] [[-local_credentials [-user name -domain name]] [-validate]]

Change the attributes of the specified instance group.

-new_instance_group name changes the name of the instance group. Use -local_credentials or -user name -domain name to add or change the credentials for the instance group. The -validate option validates the group credentials for each instance in the instance group. This option is used with -local_credentials or -user name -domain name.

-register_instance instance_name [-instance_group name | -local_credentials | -user name -domain name] [-force]

Register credentials for an instance. See the description for -instance_group name, -local_credentials, and -user name -domain name.

For a SQL Server cluster or multiple NICs, before you register an instance ensure that the instance was added with the correct host name. If you have multiple NICs, the host name is the private interface name of the SQL Server host. A SQL Server cluster requires only one entry in instance management; the host name is the virtual name of the SQL Server cluster. For a SQL Server cluster with multiple NICs, the host name is the private virtual name of the SQL Server cluster.

-remove_from_instance_group instance_name [-instance_group name] [-host name]

Remove an instance from an instance group.

-S master_server

Specifies the master server for the instance or the instance group that you want to add, change, or delete. Or use to indicate the master server on which you want to perform a specific command.

-user name -domain name

Indicates that you want to register an instance with the specific credentials that you provide. Alternatively, you can register an instance with instance group credentials or local credentials. See the -instance_group name and -local_credentials options.

The credentials must have certain security privileges. See the NetBackup for SQL Server Administrator’s Guide.

When it is used with the -validate option to modify an instance group you can also validate the credentials for each instance in the group.
EXAMPLES

Example 1 - Add local credentials to the instance group marketing without validating the credentials.

nbsqladm -modify_instance_group marketing -local_credentials

Example 2 - Add credentials for the user adminuser in the domain corp to the instance group marketing. Also validate the credentials for each instance in the group.

nbsqladm -modify_instance_group marketing -user adminuser -domain corp -validate
nbstl

nbstl – add, delete, modify, or list NetBackup storage lifecycle policies

SYNOPSIS

[-uf used_for1 [,used_for2,...used_forn]]
[-source source1[,source2,...sourcen]]
[-residence storage_unit1 | __NA__[,storage_unit2 | __NA__,...storage_uni]n | __NA__]]
[-pool volume_pool1 | __NA__[,volume_pool2 | __NA__,...volume_pooln | __NA__]]
[-server_group host1 | *ANY* | *NONE* | __NA__[,host2 | *ANY* | *NONE* | __NA___,..hostn | *ANY* | *NONE* | __NA__]]
[-managed m1[,m2,...mn]] [-rl retention_level1 | __NA__[,retention_level2 | __NA__,...retention_leveln | __NA__]] [-as alt_read_server1 | __NA__[,alt_read_server2 | __NA__,...alt_read_servern | __NA__]]
[-mpx T | F [,T | F,..,T | F]] [-target_master target_master_server1 | __NA__[,target_master_server2 | __NA__,...target_master_servern | __NA__]][-target_importslp target_importslp1 | __NA__[,target_importslp2 | __NA__,...target_importslp]n | __NA__]] [-destpri priority1 [,priority2,...priorityn]] [-window window_1 [,window_2,...window_n]]
[-wcopt option_set1 [,option_set2,...option_setn]

nbstl storage_lifecycle_name -delete [-v] [-M master_server]


On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/
On Windows systems, the directory path to this command is 
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The nbstl command can do the following:

- **-add** adds a new storage lifecycle.
- **-delete** deletes an existing storage lifecycle.
- **-modify** modifies an existing storage lifecycle.
- **-L** or **-l** lists long or short information about one or all storage lifecycles. **-b** lists only the storage lifecycle policy names themselves.

The nbstl command creates, modifies, or deletes all of the destinations at the same time and does not support adding or modifying single destinations. To change properties of one destination, all of the existing destinations must be accounted for as well as the destination to be updated.

Many of the options that need to be entered for a destination may not be applicable (NA). In that case, enter the value as __NA__ (double underscores before and after NA). The following options accept __NA__ as a value:

- -residence
- -pool
- -server_group
- -as (alternate read server)
- -target_master
- -target_importslp

Note: Successful attempts to create, modify, or delete a storage lifecycle policy are audited and logged when they are initiated through the nbstl command, a NetBackup graphical user interface, or an API.

OPTIONS

- **-all_versions**
  
  Displays all versions of the specified storage lifecycle policy or all storage lifecycle policies if storage_lifecycle_name is not specified.
-b
Displays the name of the specified storage lifecycle policy or all storage lifecycle policies if storage_lifecycle_name is not specified. Use this option with the -all_versions option to display the name and version of all the storage lifecycle policies.

-conflicts
Shows how changes to this SLP as described by the other nbstl options can affect the policies that are associated with this SLP. nbstl submits the SLP changes for validation. It compares the proposed content of the SLP with all the policies that use the SLP and displays any errors on stdout. No changes are committed at this time. If no errors are found, the user can then resubmit the changes without the -conflicts option to commit the changes.

-dc class
Specifies the numeric data classification that is associated with this service.

-delete
Deletes the specified storage lifecycle policy.

-defop T | F [,T | F,...,T | F]
Sets the deferred operation flag for duplication copies.
  - F or f - Do not defer the creation of additional image copies.
  - T or t - Defer the creation of additional image copies until the source copy is about to expire. The duplication job begins about four hours before the source is to expire. This default time can be changed by changing the Deferred duplication offset parameter in the SLP Parameters host properties.

-dp duplication_priority
Specifies the duplication job priority that is associated with this Storage service.

storage_lifecycle_name
Identifies the name of the storage lifecycle policy to be created, modified, deleted, or displayed.

-json
Generates data in json format and spans multiple lines.

-json_compact
Generates data in json format on a single line.

-l
Displays the condensed output of the specified storage lifecycle policy, or all storage lifecycle policies if storage_lifecycle_name is not specified. The output contains only data for the storage lifecycle. It does not identify the name.
-L  Displays the long output of the specified storage lifecycle, or all storage lifecycles if storage_lifecycle_name is not specified. It identifies the output by name.

-M master_server  Specifies the NetBackup master server. The default is the local server.

-modify  Modifies the specified storage lifecycle policy. This option creates a new version of the storage lifecycle policy. You can modify information such as pool volume or retention level.

-modify_current  Modifies the current version of the storage lifecycle policy instead of creating a new policy. This option cannot be used with the –dc, -uf, -source, or –managed options.

-modify_version  Modifies the selected version (nn) of the storage lifecycle policy instead of creating a new policy. This option cannot be used with the –dc, -uf, -source, or –managed options.

-v  Selects the verbose mode for logging.

-version nn  Displays only the specified version number (nn) of the storage lifecycle policy or all storage lifecycle policies if storage_lifecycle_name is not specified.

The following destination options must all specify the same number of parameters, one for each destination of the Storage service. The resulting number of destinations equals the number of parameters. The parameters are separated by commas with no blank spaces between them.

-destpri priority1 [,priority2,...priorityn]  Specifies the job priority for each storage lifecycle policy destination index. This option can be used only for import destinations. All other destinations must be set to 0.

-managed m,...  Specifies the managed retention type for each destination. The possible values are the following:

-  0 - fixed
-  1 - capacity managed
- 2 - Expire after copy. After all operations complete that use this copy as a source, the copy expires. These include operations such as duplication, replication, backup from snapshot, and index from snapshot.

- 3 - remote (imported) expiration date.

- 4 - maximum snapshot rotation.

- 5 - mirror copy

For example, -managed 4 means that the retention type is maximum snapshot rotation.

```
-mpx T | F [,T | F,...,T | F]
```

Sets the preserve multiplexing flag for duplication copies. This option is not allowed for backup or snapshot copies. Settings in the policy host and storage unit properties determine the multiplexed state of the backup copies. The flag is only relevant for tape copies. The option is -mpx followed by a set of commas that are separated by the following values:

- F or f - Do not preserve multiplexing for the copy.
- T or t - Preserve multiplexing for the copy, if possible.
- __NA__ - Not applicable

```
-pool volume_pool1 | __NA__[,volume_pool2 | __NA__,..volume_pooln | __NA__]
```

Specifies the volume pool for each destination. Volume pools do not apply to disk copies.

```
-residence storage_unit1 | __NA__[,storage_unit2 | __NA__,..storage_unitn | __NA__]
```

The storage unit that is to be used for each destination. Storage units do not apply to snapshot destinations (-uf option set to 2) or duplication to remote master (-uf option set to 3).

```
-rl retention_level1 [,retention_level,...retention_level]
```

The retention level (0-100) applied to each destination. If you run this command on a pre-NetBackup 8.0 media server, the output only displays the retention levels between 0 and 24.

**Note:** Retention level 25 has a value of expire immediately. You cannot edit this value.
-server_group host1 | *ANY* | *NONE* | __NA__|,host2 | *ANY* | *NONE* | __NA__|...hostn | *ANY* | *NONE* | __NA__]

Specifies the server group. Use *ANY* when you can use any media sharing server group. Use *NONE* when no sharing group is allowed.

-as alt_read_server1 | __NA__|[,alt_read_server2 | __NA__|...alt_read_servern | __NA__]

The alternate read server for each destination. Alternate read servers apply only to duplication destinations.

-source source1[,source2,...sourcen]

Configures a hierarchy of duplications for the -add and -modify operations of storage lifecycle.

Accepted values for -source are the following:

■ Backup and snapshot destinations - value must be 0. Backup and snapshot copies do not require a source.

■ Duplication destinations - the serial number of the destination from the list of destinations to be used as the source copy. (A snapshot copy cannot be used as the source for a duplication.) Duplication destinations that do not use any specific source (that is, they use the primary copy as the source), must be set to 0.

-uf used_for1 [used_for2,...used_forn]

Specifies when each destination is used. Use one of the following values:

■ 0 - backup
■ 1 - duplication
■ 2 - snapshot
■ 3 - replication to remote master (requires a -residence value of __NA__)
■ 4 - import
■ 5 - backup from snapshot
■ 6 - index from snapshot
■ 7 - replication

For example, -uf 2 is for snapshot operation.
-wcprot option1 [,option2,...optionn]

Specifies how to treat images that cannot be suspended. If a window closes and the jobs for an SLP have not completed, NetBackup attempts to suspend the images that are in progress. When the window reopens, NetBackup resumes those jobs at the point they were when suspended.

If the images cannot be suspended, the option determines how the images are processed:

- **SFN** - Finish processing the active images. The window closes, but NetBackup continues to process the active images until they are finished. NetBackup does not begin to process any other images until the window reopens.

- **SHN** - Cancel the processing of the active images. The window closes and NetBackup immediately stops processing the active images. When the window reopens, NetBackup begins to process the images where it left off.

-window window_1 [,window_2,..window_n]

Specifies a time window for a specific destination. If the user runs the `bpschedule` command to create a new duplication window, then a subsequent `nbstl` command can create a lifecycle with a backup and duplication destination. And duplication from this policy would run only from 6 AM and last for 4 hours (which means all job should be done by 10AM).

**EXAMPLES**

Example 1 - List the long output of information on lifecycle1:

```
# nbstl lifecycle1 -L

Name: lifecycle1
Data Classification: Gold
Duplication job priority: 0
State: active
Destination 1 Use for: backup
Storage Unit: adv_dsu1
Volume Pool: (none specified)
Server Group: (none specified)
Retention Type: Fixed
Retention Level: 1 (2 hours)
Alternate Read Server: (none specified)
Preserve Multiplexing: false
State: inactive
Source: (client)
```
The storage unit named adv_dsu1 is inactive. Values for "State" in the -L display are either active or inactive.

Example 2 - Create a lifecycle named HDLifecycle1. This lifecycle has a data classification of Gold. It contains the following four destinations:

- A backup destination (-uf value is 0) with storage unit AdvDisk1 which does not require any source (-source value is 0).
- A backup destination using storage unit DataDomain1.
- A duplication destination (-uf value is 1) with storage unit DataDomain2 that uses destination at serial number 1 (i.e. the backup destination with storage unit DataDomain1) as a source (-source value is 1).
- A duplication destination with storage unit cooperstown-tape1 that uses the destination at serial number 2 (i.e. the duplication destination with storage unit DataDomain2) as the source (-source value is 2).

```
# nbstl HDLifecycle1 -add -dc Gold -uf 0,0,1,1,1 -residence AdvDisk1, DataDomain1,DataDomain2,cooperstown-tape1 -source 0,0,1,2
```

Example 3 - Create a lifecycle that does snapshot with backup to disk and then duplication to tape. The disk storage unit is DskSTU and the tape storage unit is TpSTU.

```
# nbstl LCPolicy -add -dc Gold -uf 0,1,2 -residence DskSTU,TpSTU,__NA__ -pool NetBackup,DLP_Pool1,__NA__ -managed 0,0,0 -rl 6,12,1
```

Data retention is defined as follows:

- Snapshot images are retained for one week.
- Backup images on disk are retained for six (6) months.
- Tape images are retained for five (5) years.
- The user has defined retention level 12 to be five (5) years.

Example 4 - Change the retention level for existing version 4 of the lifecycle:

```
# nbstl LCPolicy -modify_version -version 4 -rl 4,6,7,7
```

The storage lifecycle policy must have four destinations previously defined.

Example 5 - List the condensed contents of version 2 of LCPolicy:

```
# nbstl LCPolicy -l -version 2
```

Example 6 - Change the fields in the current version of the storage lifecycle policy SLP8:
Example 7 - Create a new duplication window. Then a subsequent `nbstl` command can create a lifecycle with a backup and duplication destination (0,1). A previous `bpplsched` command set the duplication window for this policy to run from 6:00 a.m. to 10:00 a.m. (4 hours).

```
# nbstl SLP8 -modify_current -pool Pool1,Pool2,Pool3 -as __NA__,
AltReadServer2,__NA__ -mpx F,F,T
```

```
# nbstl morning_dup_slp -add -dc Gold -dp 999 -uf 0,1 -source 0,1
-residence DISK1,TAPE1
```

SEE ALSO

See `nbdc` on page 631.

See `nbstlutil` on page 854.
nbstlutil

nbstlutil – run the NetBackup storage lifecycle policies utility

SYNOPSIS

nbstlutil active [-lifecycle name] [-destination name] [-before mm/dd/yyyy hh:mm:ss | -after mm/dd/yyyy hh:mm:ss]

nbstlutil inactive -lifecycle name | -destination name
 [-reactivation_time mm/dd/yyyy hh:mm:ss | -duration hours] [-before mm/dd/yyyy hh:mm:ss | -after mm/dd/yyyy hh:mm:ss]

nbstlutil inactive -lifecycle name -destination name
 [-reactivation_time mm/dd/yyyy hh:mm:ss | -duration hours] [-before mm/dd/yyyy hh:mm:ss | -after mm/dd/yyyy hh:mm:ss]

nbstlutil list_import_conf [-l|-U|-b|-json|-json_compact] [-lifecycle name] [-all_pending_images] [destination name] [-target_domain name]

nbstlutil cancel [-lifecycle name | -destination name] [-version number] [-before mm/dd/yyyy hh:mm:ss | -after mm/dd/yyyy hh:mm:ss]
[-nowarn]

nbstlutil active | inactive | cancel -backupid id_value

nbstlutil diskspaceinfo [-stype server_type]


nbstlutil pendimplist

nbstlutil redo -backupid value -slpindex value

nbstlutil repllist [-l] [-U] [-sincetime timeval]

nbstlutil report [-lifecycle name [-version number]] [-client name] [-mediaid value] [-mediaserver name] [-storageserver name]
nbstlutil stlilist [-l] [-U] [[[-lifecycle name] [-destination name]]
| -backupid value] [-client name] [-mediaid value] [-mediaserver
| name] [-image_state value] | -image_incomplete | -image_inactive]
| [-copy_type value]}

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The nbstlutil command provides a way for users to intervene in storage lifecycle
policy (SLP) operations. The following are the utility functions:

Note: It is not recommended that users modify or delete automanaged policies.

If the user modifies the SLP, they must make sure that the SLP continues to meet
the service level objective as defined by the protection plan.

If the user deletes the SLP, they must make sure that the asset is added to another
protection plan that meets the service level objective.

Note: Activating and suspending an SLP using the nbstlutil command are not
audited. These operations are audited only when they are initiated from a NetBackup
graphical user interface or API.

active

Activates processing of the secondary operations that have been suspended
within a storage lifecycle policy. Operations that qualify as secondary are
duplication, replication, and import from snapshot. Existing images and newly
created images are activated. The -lifecycle, -version, -destination,
-befores, -after, and -backupid options identify the secondary operations.

- If neither the -lifecycle option nor the -destination is specified,
nbstlutil resumes the processing of all secondary operations for all
storage lifecycle policies.

- If only a storage lifecycle policy (-lifecycle) is specified, nbstlutil
resumes the processing of all secondary operations for that storage lifecycle
policy only.
nbstlutil

If only a destination is specified, nbstlutil resumes the processing of all secondary operations that use the specified destination for all storage lifecycle policies.

You suspend secondary operations when you run the nbstlutil inactive command.

cancel

Permanently cancels storage lifecycle policy processing according to how the -lifecycle, -before, -after, and -destination options are used:

- If the -lifecycle option and the -destination option are both used, nbstlutil permanently cancels processing for the existing images that the options identify.
- If neither of the options is used, nbstlutil permanently cancels all pending copies for all existing images that the storage lifecycle policies manage.
- If only a storage lifecycle policy (-lifecycle) is specified, nbstlutil permanently cancels all pending copies of the existing images that it manages.
- If only a destination is specified, nbstlutil permanently cancels all pending copies that are bound for that destination, for all storage lifecycle policies.

Any new images that are created after this command are processed normally. If all pending copies of an image are canceled, that image is marked as complete. The destination name is the name of a storage unit or a storage unit group that is used in a storage lifecycle policy.

diskspaceinfo

Reports on the space that is used by all disk volumes or only the disk volumes that the specified type uses.

inactive

Suspends processing of secondary operations within a storage lifecycle policy, but retains the image information so that processing can resume later. Secondary operations are duplication, replication, and import from snapshot. Existing images and newly created images are suspended. The -lifecycle, -before, -after, and -destination options identify the secondary operations.

- If the -lifecycle option and the -destination option are both used, nbstlutil suspends processing for the existing images that the storage lifecycle policy and destination options identify.
- If only a storage lifecycle policy (-lifecycle) is specified, nbstlutil suspends all secondary operations for that storage lifecycle policy.
If only a destination is specified, `nbstlutil` suspends all secondary operations that use the specified destination for all storage lifecycle policies. The `inactive` option uses an accompanying `reactivation` option that lets you select when the inactive secondary operations can resume processing.

**list**

Shows the contents of an image list. It lists images that reference an SLP. You can specify the SLP name to filter the image list. This option is primarily a debugging tool, but support may use the information to troubleshoot problems.

**list_import_conf**

Lists the images that have been replicated to a target domain but the corresponding import confirmation message has not been received. By default, only those images waiting for confirmation longer than the configured threshold are listed. If the `-all_pending_images` option is selected, all waiting images are listed regardless of waiting time.

**pendimplist**

Lists all images in the pending import state. These are replication events that are received but not yet imported successfully. Because the image import function does not import images with a backup time in the future, these images remain pending until the backup time has passed.

**redo**

Repeats an SLP operation on an image. If a non-NetBackup action loses, damages, or destroys an image copy, `redo` lets you recreate the copy. If the original source copy is no longer available, the `redo` fails.

**report**

Shows a rollup of incomplete copies of lifecycle managed images.

**repllist**

Shows the status for completed replication copies.

**stlilist**

Shows the status for all copies of lifecycle managed images.

**OPTIONS**

- `-after mm/dd/yyyy hh:mm:ss`
  
  Restricts the SLP secondary operation to only those backups started after the specified date-time.

- `-all_pending_images`
  
  All waiting images are listed regardless of waiting time.
-b
Lists only the backup IDs.

-backupid value
Specifies the backup ID whose images are to be processed.

-before mm/dd/yyyy hh:mm:ss
Restricts the SLP secondary operation to only those backups started before the specified date-time.

-client name
Restricts the listing of images for storage lifecycle operations to only those on the client that is specified by name.

-copy_inactive value
Selects the images for which one or more copies are marked as inactive in the NetBackup database. This option is used primarily for debugging.

-copy_incomplete value
Selects the images for which one or more copies are not marked as duplication complete in the NetBackup database. This option is used for debugging.

-copy_state value
Selects the images with the specified copy state in the NetBackup database. This option is used primarily for debugging. Valid values for copy state are as follows:
- 1 - NOT_STARTED
- 2 - IN_PROCESS
- 3 - COMPLETE
- 9 - NOT_STARTED | INACTIVE
- 10 - IN_PROCESS | INACTIVE

-copy_type value
Selects a copy type filter for the list commands (list and stlilist). Valid values are the following:
- 0 - Backup
- 1 - Duplication
- 2 - Snapshot
- 3 - Duplication to remote master (replica)
- 4 - Import
-destination name
Selects the images that are scheduled to be duplicated to the storage unit or
storage unit group that is specified by name.

-duraction hours
Sets the amount of time in hours after the lifecycle images are inactivated
before reactivation begins. The number of hours must be in whole integers
(1,2,...). This option is used only with the inactive option.

-frag_state value
Selects the images with the specified fragment state in the NetBackup database.
This option is used for debugging. Valid values for frag state are as follows:

■ 1 - ACTIVE
■ 2 - TO_BE_DELETED
■ 3 - ELIGIBLE_FOR_EXPIRATION

-image_inactive value
Selects the images that are marked as inactive in the NetBackup database.
This option is used for debugging.

-image_incomplete value
Selects the images that are not marked as lifecycle complete in the NetBackup
database. This option is used for debugging.

-image_state value
Selects the images with the specified image state in the NetBackup database.
This option is used primarily for debugging. The valid values for image state
are as follows:

■ 1 - NOT_STARTED
■ 2 - IN_PROCESS
■ 3 - COMPLETE
■ 9 - NOT_STARTED | INACTIVE
■ 10 - IN_PROCESS | INACTIVE

-jobid value
Restricts the output listing of images for storage lifecycle operations to only
those that the specified job ID value has created. -jobid can be used only
with the list option.

-json
Produces output in expanded readable json format.
-json_compact
  Produces output in compressed json format.

-l
  Produces a condensed parsable output of the listing.

-lifecycle name
  Selects only lifecycle managed image list.

-mediaid value
  Restricts the listing of images for storage lifecycle operations to only those on
  the media ID that value specifies.

-mediawriter name
  Restricts the listing of images for storage lifecycle operations to only those on
  the media that name specifies.

-nowarn
  Skips the interactive warning message.

-policy name
  Restricts the processing of images to those that the specified backup policy
  (name) has created. -policy can be used only with the list option.

-reactivation_time mm/dd/yyyy hh:mm:ss
  Sets the time in mm/dd/yyyy hh:mm:ss format when you want the copies or
  SLPs that you are inactivating to be reactivated. The inactive option can use
  this option or the -duration option to reactivate inactivated copies or SLPs.

-rt I | IC | ICF | ICFS
  Selects the record types to be listed. The possible values are:
  ■ I - list only image records.
  ■ IC - list image and copy records.
  ■ ICF - list image, copy, and fragment records.
  ■ ICFS - list image, copy, fragment, and snapshot records.

-sincetime timeval
  Shows the status of completed replication copies from the specified timeval to
  the present. This option is used with the replist function.

-slpindex value
  Specifies the SLP operation to be repeated. -slpindex can be used only with
  the redo operation.
-storageserver name
Restricts the listing of images for storage lifecycle operations to only those on the storage server that name specifies.

-stype server_type
Specifies a string that identifies the storage server type. The server_type value can originate from one of the following sources:

- Veritas provided storage. Possible values are AdvancedDisk and PureDisk.
- Third-party disk appliances. The vendor supplies the server_type string.
- Cloud storage. Use the csconfig clconfig -l command to determine the possible stype values. The cloud stype values reflect the cloud storage provider. Cloud storage stype values can also incorporate a suffix (for example, amazon_crypt). Possible suffixes are:
  - _raw: The NetBackup backup image is sent to the cloud in raw format. Use this option if you do not want to compress or encrypt data before sending to cloud storage.
  - _rawc: Compresses the data before it is written to the cloud storage.
  - _crypt: Encrypt the data using AES-256 encryption before writing the data to cloud storage. You must have KMS configured in NetBackup to use this option.
  - _cryptc: Compress and encrypt the data before writing to cloud storage.

The storage server type is case sensitive.

-target_domain name
Selects for output only those records that pertain to the named target domain.

-U
Produces user-readable output of the listing.

-version number
Restricts the list output to only images that are controlled by the specified SLP version. It must be used with the -lifecycle option.

EXAMPLES

Example 1 - Displays the information about a lifecycle in-process image.

# nbstlutil -list -backupid dollhouse_1287744229 -U
Image:
Master Server : dollhouse
Backup ID : dollhouse_1287744229
Client : dollhouse
Backup Time : 1287744229 (Fri Aug 24 16:13:49 2012)
Policy : pol-slp-2bkup-70-level
Client Type : 13
Schedule Type : 0
Storage Lifecycle Policy : slp-pol-2backup-70-level
Storage Lifecycle State : 2 (IN-PROCESS)
Time In Process : 1287744327 (Fri Aug 24 16:15:27 2012)
Data Classification ID : 85AA96DF9781453289A41745DD240A48 (Platinum)
Version Number : 0
OriginMasterServer : (none specified)
OriginMasterServerID : 00000000-0000-0000-0000-000000000000
Import From Replica Time : 0 (Thu Jan 01 05:30:00 1970)
Required Expiration Date : 0 (Thu Jan 01 05:30:00 1970)
Created Date Time : 1287744297 (Fri Aug 24 16:14:57 2012)

Copy:
Master Server : dollhouse
Backup ID : dollhouse_1287744229
Copy Number : 1
Copy Type : 0
Expire Time : 1288953829 (Fri Nov 02 16:13:49 2012)
Expire LC Time : 1288953829 (Fri Nov 02 16:13:49 2012)
Try To Keep Time : 1288953829 (Fri Nov 02 16:13:49 2012)
Residence : PDDE-Stu
Copy State : 2 (IN-PROCESS)
Job ID : 0
Retention Type : 0 (FIXED)
MPX State : 0 (FALSE)
Source : 0
Destination ID : *NONE*
Last Retry Time : 0

Fragment:
Master Server : dollhouse
Backup ID : dollhouse_1287744229
Copy Number : 1
Fragment Number : 1
Resume Count : 0
Media ID : @aaaad
Media Server : dollhouse
Storage Server : (none specified)
Media Type : 0 (DISK)
The output displays "(none specified)" for blank fields.

**Example 2 - Display the contents of an image list in condensed parsable format.**

```
# nbstlutil list -l
V7.0 I abc.example.com abc_1225727 abc 1225727 Pol_SLPTest1 0 0 SLP_Test1 2 1225727 *NULL*
V7.0 C abc.example.com abc_1225727 1 2147483 1225735 AdvDisk1 3 0 0 0 0
V7.0 F abc.example.com abc_1225727 1 1 0 @ab abc.example.com *NULL* 0 6 1 32768 1 @ab
V7.0 C abc.example.com abc_1225727 2 2147483 1225735 AdvDisk2 3 0 0 0 0
```

**Example 3 - Display the information for an incomplete lifecycle image in user-readable output.**

```
# nbstlutil stlilist -U
Image abc_1225727928 for Lifecycle SLP_Test1 is IN_PROCESS
Copy to abc-tape1 is IN_PROCESS
Copy to AdvDisk3 is NOT_STARTED
```
nbstop

nbstop – stops the NetBackup services on the client where the command was run.

SYNOPSIS

nbstop [-k | -kill [-3 | -third_party] [-q | -quiet]]  
nbstop -l | -list [-3 | -third_party]  
nbstop -h | -help

On UNIX systems, the directory path to this command is  
/usr/openv/netbackup/bin

On Windows systems, the directory path to this command is  
install_path\NetBackup\bin

DESCRIPTION

The nbstop command shuts down the NetBackup services on the client where the command was run.

OPTIONS

-3 | -third_party
   Expands the scope of processes which are eligible for termination to include any process which might interfere with the NetBackup upgrade process. This scope includes any processes using or holding NetBackup libraries and files. On UNIX systems, the scope also includes any processes using or holding folders.

-h | -help
   Show usage statement.

-k | -kill
   Stops the NetBackup client processes. If you omit this option, you receive a confirmation request before the command continues.

-l | -list
   List the active processes that would be stopped as a result of this command.

-q | -quiet
   Suppress all output. The information is still logged.
EXAMPLES

Example 1 - Prompts the user to confirm the stop of all NetBackup processes. User opts to stop all processes.

nbstop

NetBackup software will be shut down. This may cause backups to fail.
Do you wish to proceed? (y/n) y
Gathering process information.
Initiating Orderly shutdown, 4 processes active
Requesting termination of /usr/openv/netbackup/bin/nbdisco.
Requesting termination of /usr/openv/netbackup/bin/bpcd.
Requesting termination of /usr/openv/netbackup/bin/vnetd.
Signaling process /usr/openv/netbackup/bin/bpclntcmd
All NetBackup specified processes terminated normally.

Example 2 - Prompts the user to confirm the stop of all NetBackup processes. User opts to exit stop process.

nbstop

NetBackup software will be shut down. This may cause backups to fail.
Do you wish to proceed? (y/n) n
Shutdown aborted.

Example 3 - Kills all NetBackup and third-party processes without user input.

nbstop -kill -third_party

Gathering process information.
Initiating Orderly shutdown, 5 processes active
Requesting termination of /usr/openv/netbackup/bin/nbdisco.
Requesting termination of /usr/openv/netbackup/bin/bpcd.
Requesting termination of /usr/openv/netbackup/bin/vnetd.
Signaling process /usr/openv/netbackup/bin/bpclntcmd
All NetBackup specified processes terminated normally.

There are 1 3rd party processes active.
nbstop_target_loadfile /usr/QE/nbstop_target_loadfile 18411 Third Party
Terminating third party process, nbstop_target_loadfile pid-18411
Signaling process /usr/QE/nbstop_target_loadfile

Example 4 - List all active NetBackup processes that would be stopped as a result of this command.
nbstop -list

<table>
<thead>
<tr>
<th>Name</th>
<th>Path</th>
<th>Pid</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>vnetd</td>
<td>/usr/openv/netbackup/bin/vnetd</td>
<td>18676</td>
<td>NetBackup</td>
</tr>
<tr>
<td>bpcd</td>
<td>/usr/openv/netbackup/bin/bpcd</td>
<td>18681</td>
<td>NetBackup</td>
</tr>
<tr>
<td>bpclntcmd</td>
<td>/usr/openv/netbackup/bin/bpclntcmd</td>
<td>18698</td>
<td>NetBackup</td>
</tr>
<tr>
<td>nbdisco</td>
<td>/usr/openv/netbackup/bin/nbdisco</td>
<td>18715</td>
<td>NetBackup</td>
</tr>
</tbody>
</table>
**nbsu**

*nbsu* – used to gather diagnostic information about the system on which the utility is run

**SYNOPSIS**

```
nbsu [-d collector] [-g collector_group] [-h] [-s collector] [-l] [-nozip] [-r NetBackup_role]
```

On UNIX systems, the directory path to this command is

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

On Windows systems, the directory path to this command is

```
install_path\NetBackup\bin\support\`
```

**DESCRIPTION**

The *nbsu* utility is a Veritas utility used to gather diagnostic information about the system on which the utility is run. By default, *nbsu* gathers appropriate diagnostic information based on the operating system and NetBackup environment.

The *nbsu* command always runs with a role. By default, when the user does not specify the role, the command determines the role and runs with that role. To skip the role determination process, specify the role with the `-r` option.

Starting with NetBackup 8.1.1 the command now generates the `stderr.txt` file. This file is a summary of all the commands that failed with a non-zero exit status.

If there are no command line options specified, *nbsu* selects and runs all appropriate diagnostics and gathers all available information. You can run `nbsu -help` to view the usage.

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_mmdyyyy_timestamp.extension
```

Example:

- **UNIX/Linux:** `NBSU_mylinuxvm_master_11072017_152100.tgz`
- **Windows:** `NBSU_mywindowsvm_master_11072017_152100.cab`
OPTIONS

-d collector
Run only the specified collector or group. Specify in a comma-separated list. Veritas does not recommend using the -d and -s options together.

Use the command that is shown to collect operating system, NET, and NetBackup installation log diagnostics:

nbsu -d DEV,OS,NET,NBU_install_log

This command is the same as running the previous version of nbsu with the -no_nbu option and gathering any installation logs that exist. This option is useful for new client installation issues.

-g collector_group
Only collect information from the specified group. You can use the -d option to achieve the same result. If you also use the -s option, the -g option is preferred.

Groups include:
- OS: Operating system
- NET: Network configuration
- NBU: NetBackup
- MM: Media manager
- DEV: Operating system device information

Use the command that is shown to collect only the media manager group diagnostics:

nbsu -g MM

To collect all operating system group diagnostics and except for the OS_set diagnostic, use the command shown:

nbsu -g OS -s OS_net

-h Display the help information.

-l List the various collectors. This option does not collect any data. It merely lists all the available collectors.

nbsu -l

NBU_adv_disk
NBU_all_log_entries
NBU_altnames
OS_config
OS_process_list

-nozip
Do not compress the NBSU output.

-r NetBackup_role
Specify the NetBackup role for which you want to collect data. Specify multiple roles in a comma-separated list. Avoid using the -r option with the -d option. Accepted values for NetBackup_role are:

- ma: NetBackup master server
- me: NetBackup media server
- cl: NetBackup client server

Use the command that is shown to specify the role NetBackup client:
nbsu -r cl

-s collector
Skip a particular collector. Specify multiple collectors to skip in a comma separated list.

EXAMPLES

Example: Sample output from the nbsu command:

NetBackup Install path: C:\Program Files\Veritas\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

SEE ALSO

See nbcplogs on page 606.
See nbdna on page 673.
nbsvrgrp – manage server groups

SYNOPSIS

nbsvrgrp -add -grpname name [-M master_name] -server
s1:t1:s2:t2:s3:t3...sN:tN -grptype MediaSharing | NOM |
AltServerRestore | BackupHostPool [-grpstate ACTIVE | INACTIVE]
-description text

nbsvrgrp -update -grpname name [-M master_name] [-addsver
s1:t1:s2:t2:s3:t3...sN:tN] [-remsvr s1:t1:s2:t2:s3:t3...sN:tN]
[-grptype MediaSharing | NOM | AltServerRestore] [-grpstate ACTIVE
| INACTIVE] [-description text]

nbsvrgrp -delete -grpname name [-M master_name]

nbsvrgrp -list [-M master_name] [-grptype MediaSharing | NOM |
AltServerRestore] [-grpname name] [-grpstate ACTIVE | INACTIVE]
[-summary | -verbose | -noverbose]

nbsvrgrp -list_machine_membership [-M master_name] -m machine_name
[-t machine_type] [-summary | -verbose | -noverbose]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The nbsvrgrp command adds, changes, deletes, or lists server groups.

Any authorized user can run nbsvrgrp.

For more information about NetBackup authorization, refer to the NetBackup Security
and Encryption Guide.

OPTIONS

-add

   Adds a new server group.
-addsvr s1:t1:s2:t2:s3:t3...sN:tN
   Specifies a list of server or server-type pairs to be added to a server group.
   Examples of server types are master, media, and ndmp.

-change
   Changes an existing server group.

-delete
   Deletes a server group. This operation fails if it is a Media Sharing Group and
   media is assigned to the group.

-description text
   Describes the server group. Use double quote marks if the description contains
   any spaces.

.grpname name
   Specifies the human readable name that is given to a server group. This name
   is case sensitive. It may only contain the characters a-z, A-Z, 0-9, plus(+),
   minus(-), underscore(_), and period(.)

-grptype type
   Specifies the group type that is used to designate the purpose of a server
   group. The current list of group types is MediaSharing, NOM, AltServerRead,
   and BackupHostPool.

-grpstate ACTIVE | INACTIVE
   Sets or changes the state of a server group. Allowable states are ACTIVE and
   INACTIVE.

-list [-summary | -verbose | -noverbose]
   Lists the information about all server groups. The -summary option specifies a
   brief format for the server group information. The -verbose option specifies a
   detailed format for the server group information. The -noverbose option
   specifies a parsable format for the server group information.

-list_machine_membership [-summary | -verbose | -noverbose]
   Lists the server groups in which a named machine has membership. The
   -summary option specifies a brief format for the server group information. The
   -verbose option specifies a detailed format for the server group information.
   The -noverbose option specifies a parsable format for the server group
   information.

-m machine_name
   Machine name to use with the -list_machine_membership option.
-remsvr s1:t1:s2:t2:s3:t3...sN:tN
   Specifies a list of server or server-type pairs to be removed from a server group. Examples of server types are *master*, *media*, and *ndmp*.

-server s1:t1:s2:t2:s3:t3...sN:tN
   Specifies a list of server (s1, s2,...) and server type (t1, t2,...) pairs to be configured in the server group. Examples of server types are *master*, *media*, and *ndmp*.

-t machine_type
   The machine type that corresponds to the machine that is named in the -m option. Examples include *master*, *media server*, and *ndmp*.

**NOTES**

*nbsvrgrp* provides only limited validation of the option parameters.

**EXAMPLES**

Example 1 - Add a new media sharing server group that is called *MyServerGroup*, with media servers *larry* and *moe*, and ndmp filer *myfiler*:

```
# nbsvrgrp -add -grpname MyServerGroup -server
```

Example 2 - List all server groups that are configured:

```
# nbsvrgrp -list -summary
```
resilient_clients

resilient_clients – run utility that enables resiliency in clients to WAN latency and the interruptions that cause communication failures

SYNOPSIS

resilient_clients on | off client1 [ client2 ... ]
resilient_clients status [ client1 ... ]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The resilient_clients utility enhances the communication between the client in a remote office and the NetBackup server in a central office. Clients are made resilient to wide area network (WAN) high latency and the interruptions that can cause operations to fail. resilient_clients enhances resiliency at three different connection levels: Legacy NetBackup, ClientDirect, and PureDisk.

You must have administrator privileges to run this command.

OPTIONS

on | off client1 [ client2 ... ]

Turns resiliency on and off for the specified client or clients.

status [ client1 ... ]

Displays the resiliency setting (on or off) of the specified client or clients. If no clients are listed, it displays the status of all clients of this master server.
restoretrace

restoretrace – consolidate debug logs for a restore job

SYNOPSIS


On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\admincmd\n
DESCRIPTION

The restoretrace utility consolidates the debug logs for the specified restore jobs. It copies to standard output the debug log lines relevant to the specified restore jobs. The messages sort by time. The utility tries to compensate for time zone changes and clock drift between remote servers and clients. The output is formatted to easily sort or group by timestamp, program name, server, or function for the following: bprd on the master server, bpbrm and bptm-bpdm on the media server, and tar on the client. For best results, set the verbose logging level to 5. Enable debug logging for bpdbm on the master server and for bpcd on all servers and clients in addition to already identified processes.

You must have administrator privileges to run this command.

OPTIONS

  -master_server name
    Name of the master server. Default is the local host name.

  -job_id number
    Job ID number of the restore job to analyze.

  -client_name name
    Client name of the jobs to analyze.

  -start_time hh:mm:ss
    Earliest timestamp to start analyzing the logs.
-end_time hh:mm:ss
   Latest timestamp to finish analyzing the logs.

mmddyy [mmddyy...]
   One or more day stamps that identify the log file names (log.mmddyy for UNIX, and mmddyy.log for Windows) that restoretrace analyzes.

NOTES

Media Manager logs are not analyzed.

EXAMPLES

Example 1 - Consolidate debug logs of all the restore jobs for the client peony on 071502. Use the start_time and end_time parameters to limit the window for the jobs that are evaluated.

UNIX systems:

/usr/openv/netbackup/bin/admincmd/restoretrace -job_id 234 081302 log.234

Windows systems:

C:\Program Files\Veritas\NetBackup\bin\admincmd\restoretrace
client peony install_path C:\Program Files\Veritas 071502 log.peony
stopltid

stopltid – stop the Media Manager device daemon

SYNOPSIS

stopltid

The directory path to this command is /usr/openv/volmgr/bin/

DESCRIPTION

This command operates only on UNIX systems.

The stopltid command stops ltid, avrd, and the robotic daemons.

The ltid command starts the Media Manager device daemon (ltid) and Automatic Volume Recognition daemon (avrd). These daemons manage Media Manager devices. With both daemons started, an operator can initiate the operator display, observe the drive status, and control the assignment of requests to standalone drives. ltid can be placed in a system initialization script.

The Media Manager volume daemon, vmd, also starts with the ltid command. ltid also starts the appropriate robotic daemons, if robotic devices were defined in Media Manager.

You must have administrator privileges to run this command.

ERRORS

Error messages are logged by using syslogd.

SEE ALSO

rc(8), syslogd (UNIX commands)

See ltid on page 549.

See tpconfig on page 892.

See tpunmount on page 917.
**tldd**

**tldd** – Tape library DLT (TLD) daemon (process) or control daemon (process).

**SYNOPSIS**

```
tldd [-v]
```

On UNIX systems, the directory path to this command is
```
/usr/openv/volmgr/bin/
```

On Windows systems, the directory path to this command is
```
install_path\Volmgr\bin\`
```

**DESCRIPTION**

**tldd** and **tldcd** interface with Media Manager to mount and unmount volumes in a tape library DLT (TLD) robot.

**ltid** is the Media Manager device daemon on UNIX systems and the NetBackup Device Manager service on Windows systems. **tldd** directly interfaces with **ltid**. **tldd** runs on each host with a drive connection and sends mount and unmount requests to the control daemon (**tldcd**). **tldcd** communicates directly with the robotics through a SCSI interface.

The following items apply only to NetBackup Enterprise Server:

- TLD robotic control software permits drives in the same robot to be configured on different hosts. **tldcd** may be running on a different host than **tldd**, depending on where the interface connection resides (see EXAMPLES). When the connection is established (the path for robotics can be opened), **tldd** puts the TLD robot in the UP state. It then can mount and unmount volumes. If the robotics are inaccessible, **tldd** changes the robot to the DOWN state. In this state, **tldd** is still running and returns the robot to the UP state if **tldcd** is able to make a connection.

- If drives are on different NetBackup hosts, enter the robotic information in the Media and Device Management of the Administration Console on all computers. The robot number must be the same on all computers.

On UNIX systems, **tldd** and **tldcd** automatically start and stop when **ltid** is started and stopped. To stop or start **tldd** independently of **ltid**, use `/usr/openv/volmgr/bin/vmps` or your server’s `ps` command to identify the **tldd** process ID. Then enter the following commands:
The control daemon, \texttt{tldcd}, is on the host that has the robotic control. \texttt{tldd} on that host automatically starts it (see EXAMPLES).

On Windows systems, \texttt{tldd} and \texttt{tldcd} are started when the NetBackup Device Manager service is started. They are stopped when this service is stopped. The control process, \texttt{tldcd}, is on the host that has the robotic control. \texttt{tldd} starts it automatically on that host (see EXAMPLES). \texttt{tldcd} stops when you stop the NetBackup Device Manager service.

Before you access any volumes through the NetBackup Device Manager service (Windows systems) or \texttt{ltid}, define the following information: the media ID and slot number for volumes in a robot in the EMM database.

If a cleaning volume is used, it must be defined in the volume configuration. See \texttt{tpclean} for information on setting the frequency to clean the drive automatically.

The drives are logically numbered 1 through \texttt{n}, where \texttt{n} is the number of drives in the robotic library. Use one or more of the following to determine the correct robot drive numbers:

- The Device Configuration Wizard (if the robotic library and drives support serialization).
- The robotic library vendor’s documentation on how to index drives.
- The robotic test utility, or experiment by mounting media and watch the operator display.

On UNIX systems, the Internet service port number for \texttt{tldcd} must be in \texttt{/etc/services}. If you use NIS (Network Information Service), place the entry in this host’s \texttt{/etc/services} file in the master NIS server database for services.

On Windows systems, the Internet service port number for \texttt{tldcd} must be in \texttt{%SystemRoot%\system32\drivers\etc\services}.

The default service port number is 13711.

You must have administrator privileges to run this command.

**OPTIONS**

The following option operates only on UNIX systems.

\texttt{-v}Logs debug information by using \texttt{syslogd}. If you start \texttt{ltid} with \texttt{-v}, \texttt{tldd} and \texttt{tldcd} are also started with \texttt{-v}. 
ERRORS

Media Manager logs any tape library DLT and robotic errors to the Windows application event log. Log entries are also made when the state changes between UP and DOWN.

tldd and tldcd log an error message if another copy of the daemon is in operation.

Media Manager logs any tape library DLT and robotic errors to syslogd. Log entries are also made when the state changes between UP and DOWN.

EXAMPLES

Example 1 - In the following diagram, the two drives and the robotics connect to Host A. ltid initiates tldd, which in turn initiates tldcd.

Figure A-1 Use of tldd with single host and TLD robot

Example 2 - This example applies only to NetBackup Enterprise Server. In the following diagram, each host connects to one drive and the robotics connect to host A. ltid on each computer initiates tldd. The tldd on host A also initiates tldcd, since that is where the robotic control is defined. Requests to mount tapes from host B go to tldd on host B, which sends the robotic command to tldcd on host A.
**Figure A-2**
Use of tldd with two hosts connected to TLD robot

---

**SEE ALSO**

See **tldcd** on page 882.
See **tpclean** on page 889.
See **tpconfig** on page 892.
See **ltid** on page 549.
syslogd
tldcd

tldcd – Tape library DLT (TLD) control daemon (process)

SYNOPSIS

tldcd [-v] [-t]

On UNIX systems, the directory path to this command is /usr/openv/volmgr/bin/

On Windows systems, the directory path to this command is install_path\Volmgr\bin\

DESCRIPTION

tldd and tldcd interface with Media Manager to mount and unmount volumes in a tape library DLT (TLD) robot.

ltid is the Media Manager device daemon on UNIX systems and the NetBackup Device Manager service on Windows systems. tldd directly interfaces with ltid. tldd runs on each host with a drive connection and sends mount and unmount requests to the control daemon (tldcd). tldcd communicates directly with the robotics through a SCSI interface.

The following items apply only to NetBackup Enterprise Server:

- TLD robotic control software permits drives in the same robot to be configured on different hosts. tldcd may be running on a different host than tldd, depending on where the interface connection resides (see EXAMPLES). When the connection is established (the path for robotics can be opened), tldd puts the TLD robot in the UP state. It then can mount and unmount volumes. If the robotics are inaccessible, tldd changes the robot to the DOWN state. In this state, tldd is still running and returns the robot to the UP state if tldcd is able to make a connection.

- If drives are on different NetBackup hosts, enter the robotic information in the Media and Device Management of the Administration Console on all computers. The robot number must be the same on all computers.

On UNIX systems, tldd and tldcd automatically start and stop when ltid is started and stopped. To stop or start tldd independently of ltid, use /usr/openv/volmgr/bin/vmps or your server's ps command to identify the tldd process ID. Then enter the following commands:
kill tldd_pid
/usr/openv/volmgr/bin/tldd [-v] &

The control daemon, tldcd, is on the host that has the robotic control. tldd on that host automatically starts it (see EXAMPLES).

On Windows systems, tldd and tldcd are started when the NetBackup Device Manager service is started. They are stopped when this service is stopped. The control process, tldcd, is on the host that has the robotic control. tldd starts it automatically on that host (see EXAMPLES). tldcd stops when you stop the NetBackup Device Manager service.

Before you access any volumes through the NetBackup Device Manager service (Windows systems) or ltid, define the following information: the media ID and slot number for volumes in a robot in the EMM database.

If a cleaning volume is used, it must be defined in the volume configuration. See tpclean for information on setting the frequency to clean the drive automatically.

The drives are logically numbered 1 through n, where n is the number of drives in the robotic library. Use one or more of the following to determine the correct robot drive numbers:

- The Device Configuration Wizard (if the robotic library and drives support serialization).
- The robotic library vendor's documentation on how to index drives.
- The robotic test utility, or experiment by mounting media and watch the operator display.

On UNIX systems, the Internet service port number for tldcd must be in /etc/services. If you use NIS (Network Information Service), place the entry in this host's /etc/services file in the master NIS server database for services.

On Windows systems, the Internet service port number for tldcd must be in %SystemRoot%\system32\drivers\etc\services.

The default service port number is 13711.

You must have administrator privileges to run this command.

OPTIONS

The following options operate only on UNIX systems.

- **-v** Logs debug information by using syslogd. If you start ltid with -v, tldd and tldcd are also started with -v.
- **-t** Terminates tldcd.
ERRORS

tldd and tldcd log an error message if another copy of the daemon is in operation.

Media Manager logs any tape library DLT and robotic errors to syslogd on UNIX systems, or to the Windows application event log on Windows systems. Log entries are also made when the state changes between UP and DOWN.

EXAMPLES

Example 1 - In the following diagram, the two drives and the robotics connect to Host A. ltid initiates tldd, which in turn initiates tldcd.

Figure A-3 Use of tldcd with single host and TLD robot

Example 2 - This example applies only to NetBackup Enterprise Server. In the following diagram, each host connects to one drive and the robotics connect to host A. ltid on each computer initiates tldd. The tldd on host A also initiates tldcd, since that is where the robotic control is defined. Requests to mount tapes from host B go to tldd on host B, which sends the robotic command to tldcd on host A.
**Figure A-4** Use of `tldcd` with two hosts connected to TLD robot

<table>
<thead>
<tr>
<th>Host A</th>
<th>TLD Robot</th>
<th>Host B</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ltid</code></td>
<td><code>ltid</code></td>
<td><code>ltid</code></td>
</tr>
<tr>
<td><code>tldd</code></td>
<td><code>tldd</code></td>
<td></td>
</tr>
<tr>
<td><code>tldcd</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCSI</td>
<td>Robotics</td>
<td>SCSI</td>
</tr>
<tr>
<td></td>
<td>drive 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>drive 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>drive 1</td>
<td></td>
</tr>
</tbody>
</table>

**SEE ALSO**

See `tldd` on page 878.
See `tpclean` on page 889.
See `tpconfig` on page 892.
See `ltid` on page 549.
syslogd (UNIX command)
tpautoconf

tpautoconf – discover and configure devices

SYNOPSIS

tpautoconf -get_gdbhost
tpautoconf -set_gdbhost host_name
tpautoconf -verify ndmp_host_name
tpautoconf -probe ndmp_host_name
tpautoconf -report_disc
tpautoconf -replace_drive drive_name -path drive_path
tpautoconf -replace_robot robot_number -path robot_path

On UNIX systems, the directory path to this command is /usr/openv/volmgr/bin/

On Windows systems, the directory path to this command is install_path\Volmgr\bin\n
DESCRIPTION

The Device Configuration Wizard normally uses tpautoconf to discover devices. This wizard calls tpautoconf with a different set of options.

The get and the set options are useful in special situations. For example, use them to specify a different host as the Enterprise Media Manager (EMM) server. The EMM server name is automatically defined when NetBackup is installed.

For more about how to manage the EMM server, see "About the Enterprise Media Manager" in the NetBackup Administrator’s Guide, Volume I.

Use -report_disc, -replace_drive, and -replace_robot to reconfigure the devices in the EMM database to reflect a serial number change that a configured device replacement caused. After hardware replacement, the correction process requires that at least one system is available through the operating system. You may need to re-map, rediscover, and restart the system.

After you configure the server or servers, use the -report_disc option to scan the current hardware and compare it with the configured hardware. A list of discrepancies appears and shows the replaced hardware and the new hardware.
Note: Not all servers have access to robotic hardware. Even though no access is expected, these robots are listed as missing.

The final step to add replacement hardware is to configure the hardware on all servers by their operating systems. Then run the Device Configuration Wizard to configure the new path information.

You must have administrator privileges to run this command.

OPTIONS

Note: Only limited validation of the option parameters is done.

-get_gdbhost
Returns the name of the EMM server host.

-set_gdbhost host_name
Sets the name of the EMMSERVER entry in bp.conf.

-probe ndmp_host_name
Lists all devices that are attached to the NDMP host.

-report_disc
Enables the device data to be queried from the EMM server to enable a "diff" to be run on these data records against those scanned. You can run this command on reconfigured servers to produce a list of new and missing hardware. This command scans for new hardware and produces a report that shows the new and the replaced hardware.

-replace_drive drive_name -path drive_path, -replace_robot robot_number -path robot_path
The EMM database is used to query or to update robot drives and robot records.

Note: On Windows systems, drive_path is a non-NDMP Windows device path for drives and robot_path is a non-NDMP Windows device path for robots. Use the path in the {p,b,t,l} format (where p -port, b -bus, t -target, and l -lun). This information is located in the registry.

-verify ndmp_host_name
Verifies the server name of the NDMP host.
EXAMPLES

Example 1 - Return the name of the host where the Enterprise Media Manager database is stored:

```
# tpautoconf -get_gdbhost
```

Example 2 - Set the Enterprise Media Manager Server to be the host server2:

```
# tpautoconf -set_gdbhost server2
```

Example 3 - Show the -report_disc command reports discrepancies between detected devices and the EMM database. Included is an example of how to use the -replace_drive drive_name -path drive_path command.

```
# tpautoconf -report_disc
=============== New Device (Tape) ====================
Inquiry = "QUANTUM DLT8000 0250"
Serial Number = PXB08P3242
Drive Path = /dev/rmt/119cbn
Found as TLD(6), Drive = 1
=============== Missing Device (Drive) ===============
Drive Name = QUANTUMDLT800014
Drive Path = /dev/rmt/9cbn
Inquiry = "QUANTUM DLT8000 0250"
Serial Number = PXB08P1345
TLD(6) definition Drive = 1
Hosts configured for this device:
  Host = plum
  Host = avocado
# tpautoconf -replace_drive QUANTUMDLT800014 -path /dev/rmt/119cbn
Found a matching device in EMM DB, QUANTUMDLT800014 on host plum
  update on host plum completed
Found a matching device in EMM DB, QUANTUMDLT800014 on host avocado
  update on host avocado completed
```

SEE ALSO

See tpconfig on page 892.
tpclean

tpclean – manage the cleaning of the tape drive

SYNOPSIS

tpclean -L | -C drive_name [-priority number] | -M drive_name | -F drive_name cleaning_frequency

On UNIX systems, the directory path to this command is /usr/openv/volmgr/bin/

On Windows systems, the directory path to this command is \install_path\Volmgr\bin\n
DESCRIPTION

tpclean enables you to monitor Media Manager tape drive usage and optionally configure tape drives to be cleaned automatically. (This function does not apply to drives in ACS robots or QIC drives.)

Media Manager tracks the total amount of time that volumes have been mounted in the drives. You can use tpclean to specify a cleaning frequency (in hours) for a drive.

The drive is cleaned if the following conditions are true:

- The mount time exceeds the cleaning frequency.
- A TapeAlert "CLEAN NOW" or "CLEAN PERIODIC" flag has been raised.
- The drive is in a robot.
- The Media Manager volume configuration shows a cleaning tape in the robot.

The Comment field in the tpclean -L output contains the message, NEEDS CLEANING, if the following are true:

- The mount time exceeds the cleaning frequency.
- The drive is a standalone drive or does not have a defined cleaning tape.

Manually clean the drive and reset the mount time by using the -M option.

For the -C, -M, and -F options to operate, the following must occur: ltid must be running on UNIX systems, or the NetBackup Device Manager service must be running on Windows systems.
For more about TapeAlert and other drive-cleaning topics, see the *NetBackup Administrator's Guide, Volume II*.

In a NetBackup Enterprise Server, a frequency-based cleaning is not supported for shared drives.

You must have administrator privileges to run this command.

**OPTIONS**

-C *drive_name*

Initiates the cleaning of a drive in a robot. The drive must be defined in a robot and a defined cleaning tape in the Media Manager volume configuration. The mount time is reset to zero. The drive name is the name that was assigned to the drive when it was added to the configuration.

-L

Prints the cleaning statistics. (On UNIX systems, it prints to `stdout`.)

-priority *number*

Specifies a new priority for the job at which *tpclean* gets a media-drive pair of resources. The new priority overrides the default job priority.

-M *drive_name*

Indicates that the drive was manually cleaned. The mount time is reset to zero. The drive name is the name that was assigned to the drive when it was added to the device configuration.

-F *drive_name* *cleaning_frequency*

Sets the cleaning frequency for the specified drive to *cleaning_frequency* hours. The drive name is the name that was assigned to the drive when it was added. The value of *cleaning_frequency* must be between zero (0) hours and 10,000 hours.

**NOTES**

*tpconfig* -d, *tpconfig* -l, and *vmoprcmd* may truncate long drive names. Use *tpconfig* -dl to obtain the full drive name.

*tpclean* truncates drive names to 22 characters.

**EXAMPLES**

Example 1 - Display cleaning statistics. An asterisk next to the drive type indicates that the device is defined as robotic.
Example 2 - Set the cleaning frequency for the drive named dlt_dr6v6 to 25 hours. The drive is flagged as having a need to be cleaned after 25 hours of mount time has occurred.

# tpclean -F dlt_dr6v6 25

Example 3 - Reset the mount time for the drive named rob_A_dr6v1 to zero. You normally use this command after you manually clean the drive.

# tpclean -M rob_A_dr6v1

Example 4 - Initiate the cleaning of drive rob_A_dr6v1. This example assumes that the drive is a robotic drive with a cleaning tape defined. The mount time is reset to zero.

You can use the -C option to force the cleaning of a drive before you reach cleaning_frequency. Normally, robotic drives are cleaned automatically when their mount time exceeds the cleaning frequency.

# tpclean -C rob_A_dr6v1

**Note:** To use a cleaning tape, the Cleanings Remaining for that tape must be greater than zero. (This value appears in the volume list of the Media node in the NetBackup Administration Console or from the vmquery command.) This cleaning count refers to how many more times the cleaning tape can be used. You can change this count by using the Media node or the vmchange command.

**SEE ALSO**

See ltid on page 549.

See tpconfig on page 892.
tpconfig

tpconfig – run tape configuration utility

SYNOPSIS

UNIX systems:  tpconfig [-noverify]

  tpconfig -d | -dl | -l


  tpconfig -delete -drive drvindex

  tpconfig -multiple_delete -drive drvindex1:....:drvindexN
tpconfig -add -disk_array array_hostname -disk_user_id user_ID -arraytype_name "name:displayname" -requiredport IP_port_number [-password password [-key encryption_key]]

tpconfig -update -disk_array array_hostname -disk_user_id user_ID -requiredport IP_port_number [-arraytype_name "name:displayname"] [-password password [-key encryption_key]]

tpconfig -delete -disk_array array_hostname -disk_user_id user_ID [-arraytype_name "name:displayname"]

tpconfig -add -robot robnum -robtype robtype -robpath devfile [-nh ndmp_hostname]

Windows systems: tpconfig -add -robot robnum -robtype robtype -port port -bus bus -target target -lun lun

Windows systems: tpconfig -add -robot robnum -robtype robtype [-nh ndmp_hostname] -robpath changername [-bus bus -target target -lun lun]

tpconfig -add -robot robnum -robtype robtype -cntlhost cntlhost

UNIX systems: tpconfig -update -robot robnum [-robtype robtype] [-robpath devfile] [-cntlhost cntlhost]

Windows systems: tpconfig -update -robot robnum [-robtype robtype] [-port port -bus bus -target target -lun lun | -cntlhost cntlhost]


tpconfig -update -robot robnum [-robtype robtype]

tpconfig -delete -robot robnum

tpconfig -multiple_delete -robot robnum1:...:robnumN

tpconfig -add -drpath -path drivepath [-nh ndmp_hostname] -asciiname asciiidrivename [-drstatus [UP|DOWN|DISABLED]] [-noverify]

Windows systems:

```
   tpconfig -update -drpath -old_port port -old_bus bus -old_target target -old_lun lun -port port -bus bus -target target -lun lun -asciiname asciidrvname [-drstatus [UP|DOWN|DISABLED]] [-noverify]
```

UNIX systems:

```
   tpconfig -delete -drpath -path drivepath -asciiname asciidrvname [-nh ndmp_hostname]
```

Windows systems:

```
   tpconfig -delete -drpath -port port -bus bus -target target -lun lun | -path drivepath [-nh ndmp_hostname] -asciiname asciidrvname
```

```
   tpconfig -dnh
```

```
   tpconfig -dnh -all_hosts
```

```
   tpconfig -ddnh
```

```
   tpconfig -add -nh ndmp_hostname
```

```
   tpconfig -add -nh ndmp_hostname -user_id | -filer_user_id user ID [-password password [-key encryption_key]] -snap_vault_filer
```

```
   tpconfig -update -nh ndmp_hostname -user_id | -filer_user_id user ID [-password password [-key encryption_key]]
```

```
   tpconfig -delete -nh ndmp_hostname -user_id | -filer_user_id user ID
```

```
   tpconfig -multiple_delete -nh ndmp_hostname_1: ... :ndmp_hostname_N
```

```
   tpconfig -add -default_user_id user ID [-password password [-key encryption_key]]
```

```
   tpconfig -update -default_user_id user ID [-password password [-key encryption_key]]
```

```
   tpconfig -delete -default_user_id
```

```
   tpconfig -add | -update -disk_array disk_array_host_name -disk_user_id user_ID -arraytype disk_array_type -requiredport IP_port_number [-password password [-key encryption_key]]
```

```
   tpconfig -delete -disk_array disk_array_host_name -disk_user_id user_ID [-arraytype disk_array_type]
```

```
   tpconfig -ddiskarrays
```

```
   tpconfig -add | -update -virtual_machine virtual_machine_name -vm_user_id user_id -vm_type virtual_machine_type -requiredport IP_port_number [-password password [-key encryption_key]]
```
tpconfig -delete -virtual_machine virtual_machine_name -vm_user_id user_id [-vm_type virtual_machine_type]

tpconfig -dvirtualmachines

tpconfig -add -storage_server server_name -stype server_type -sts_user_id user_ID [-password password] [-st storage_type]

tpconfig -update -storage_server server_name -stype server_type -sts_user_id user_ID [-password password]

tpconfig -delete -storage_server server_name -stype server_type -sts_user_id user_ID

tpconfig -dsh [-stype server_type]

tpconfig -dsh -all_hosts

tpconfig -dev_ping [-drive -path drivepath | -robpath robotpath] [-nh ndmp_hostname]

Windows systems: tpconfig -dev_ping [-drive] -port port -bus bus -target target -lun lun

tpconfig -emm_dev_list [-noverbose]

tpconfig -add -application_server application_server_name [-application_server_user_id user_ID] -application_type application_type -requiredport IP_port_number [-password password [-key encryption_key]] [-host_user_id host user ID] [-host_password hostpassword] [-host_RSA_key host RSA key]

tpconfig -update -application_server application_server_name [-application_server_user_id user_ID] -application_type application_type -requiredport IP_port_number [-password password [-key encryption_key]] [-host_user_id host user ID] [-host_password hostpassword] [-host_RSA_key host RSA key]

tpconfig -delete -application_server application_server_name [-application_server_user_id user_ID] -application_type application_type -requiredport IP_port_number [-password password [-key encryption_key]]

tpconfig -dappservers

tpconfig -add_plugin -cloudpoint_server server_name -plugin_id netbackup_plugin_ID -plugin_type cloudpoint_plugin_type
tpconfig -modify_plugin -cloudpoint_server server_name -plugin_id netbackup_plugin_ID -plugin_type cloudpoint_plugin_type

tpconfig -list_plugins --cloudpoint_server server_name

tpconfig -list_supported_plugins

tpconfig -add -cloudpoint_server cloudpoint_server_name -cloudpoint_server_user_id user_ID -manage_workload manage_workload [-requiredport IP_port_number]

tpconfig -update -cloudpoint_server cloudpoint_server_name -cloudpoint_server_user_id cloudpoint_user_id -manage_workload manage_workload [-requiredport IP_port_number]

tpconfig -cloudpoint_server cloudpoint_server_name [-delete_media_server media_server]

tpconfig -list_supported_cloud_providers

tpconfig [-dcloudpointservers | -dmediaservers] [-cloudpoint_server cloudpoint_server_name]

tpconfig -dcloudpointservers [-manage_workload manage_workload]

tpconfig -reset_password -cloudpoint_server cloudpoint_server_name -cloudpoint_server_user_id user_ID

tpconfig -refresh [-cloudpoint_server cloudpoint_server_name]

On UNIX systems, the directory path to this command is `/usr/openv/volmgr/bin/`

On Windows systems, the directory path to this command is `install_path\Volmgr\bin\`

**DESCRIPTION**

*tpconfig* configures robots, drives, drive arrays, drive paths, and hosts for use with NetBackup.

On UNIX systems, *tpconfig* [-noverify] starts the media management and device management utility. This menu-based utility creates and modifies devices in the EMM database. The EMM database identifies the robotics and drives that are under control of *ltid* (the Media Manager device daemon). *ltid* uses this database to correlate drives in the operator’s drive status display to the device files in the /dev directory.
For example, assume that you want to configure a drive that the system recognizes as an 8-mm type drive. Look in the /dev directory and locate the no rewind on close device path for an 8-mm type drive. Then specify this device path for the drive. `tpconfig` then records the device path in the appropriate device database.

After you use `tpconfig` to change your device configuration, use `stopltid` to stop the `ltid` and `avrd` daemons (if they are running). Then use the `ltid` command to start the daemons again. See `ltid` for more information.

On Windows systems, when your device configuration changes are complete, stop and restart the NetBackup Device Manager service.

You must have administrator privileges to run this utility.

**OPTIONS**

The following four options apply only to NetBackup Enterprise Server. They specify the configuration for ACS (Automated Cartridge System) robots.

- `-ACS acsnum, -LSM lsmnum, -PANEL panelnum, -DRIVE drivenum`
  - `acsnum` specifies the number for the robotic library as configured on the ACS library software host.
  - `lsmnum` specifies the Library Storage Module that has this drive.
  - `panelnum` specifies the robot panel where this drive is located.
  - `drivenum` specifies the number of this drive.

- `-add`
  Adds a drive, a robot, a virtual machine, an application server, or CloudPoint server, depending on the accompanying options.

- `-add_media_server media_server`
  Add the media servers you want to associate with the CloudPoint server for protecting cloud workloads. To associate multiple media servers, you must run the command multiple times. The media server must be on version 8.1.2 or later. If you do not associate a media server, the NetBackup master server is used.

- `-all_hosts`
  Displays all hosts that have credentials on a media server.

- `-add_plugin`
  Adds a CloudPoint plug-in to the CloudPoint server that is configured with NetBackup.

- `-application_server application_server_name`
  Specifies the host name of the application server.
-application_server_user_id user_ID
   Specifies the user name that is required to log into the application server.

-application_type application_type
   Specifies the type of the application server. You can also use values as
   specified by the third-party plug-in vendor. The example values for the
   application_type are:
   - hadoop
   - hbase
   - mongodb

-arraytype_name "name:displayname"
   Specifies the type of the disk array for which to add, update, or delete
   credentials.
   The double quote marks (") are required only if name or displayname includes
   one or more spaces.
   The disk array vendor provides the values for name:displayname. The name
   portion is a unique string used internally by NetBackup. The displayname
   portion is a more human-readable string that is used in NetBackup
   Administration Console displays and menus.
   The values depend on the disk array vendor and the provider type that are
   used for the array, as follows:
   - For an array-specific provider, the format is as follows:
     vendorID_productID:displayname
     By default, NetBackup includes several array-specific providers, including
     (but not limited to) the following:
     - HP_HSV:HP EVA
     - EMC_CLARIION:EMC CLARiiON
     - EMC_SYMMETRIX:EMC Symmetrix
     - IBM_TOTALSTORAGE:IBM System Storage
     - NETAPP_LUN:NetApp
   - For the generic array provider, the format is as follows:
     OPENARRAY::vendorID_productID:displayname
     For example, OPENARRAY::HITACHI_HDS:Hitachi HDS DF Series.
   To determine valid disk array type names, use the -list_array_types option.
   Requires a Flexible Disk or Snapshot Client license.
-asciiname asciidrivename
   Specifies a name for the drive. This name identifies the drive to Media Manager.
   If you do not specify a drive name, Media Manager generates a name. If you
   add or update shared drives (Shared Storage Option), make this name as
   descriptive as possible.

-bus bus
   Specifies the SCSI bus number to which the robot or drive connects.
   See the NetBackup Device Configuration Guide.

-cleanfreq hours
   Specifies the number of hours between drive cleanings. When you add a drive,
   NetBackup starts to record the amount of time that volumes are mounted in
   that drive.

   If the drive is in a robot and a cleaning volume is defined in the robot, the
   cleaning occurs in the following situation: The accumulated mount time exceeds
   the time that you specify for the cleaning frequency. NetBackup resets the
   mount time when the drive is cleaned.

   If the drive is standalone or a cleaning tape is not defined, the following
   message appears in the tpclean -L output comment field: NEEDS CLEANING.
   To clean the drive, use the tpclean command.

   A frequency-based cleaning is not needed if TapeAlert is used.

-cloudpoint_server server_name
   Specifies the host name of the CloudPoint server.

-cloudpoint_server_user_id user_id
   Configures the user name and password for the CloudPoint server. Use this
   option with the -add, -update, or -delete command to specify the user name
   and password of the CloudPoint server.

-cntlhost cntlhost
   This option is only applicable for NetBackup Enterprise Server.
   For a robot whose robotic control is on another host, this option specifies the
   host that controls the robotic library.

   This option applies only for the TLD robots that can have the robotic control
   on another host. It also applies to ACS robots.

   For an ACS robot, specify the host name where the ACS library software is
   installed.
-comment comment
   Adds a comment about the drive. This field is useful for storing SCSI inquiry
data so you can easily check the drive type and firmware level.

-d
   Lists the current configuration information. On UNIX systems, the listing is sent
to stdout. This option may truncate drive names to 22 characters.

-dappservers
   Displays all configured application servers. For example, hadoop server or
hbase server.

-dcloudpointservers
   Lists all the CloudPoint servers you have configured NetBackup.

-ddiskarrays
   Displays all configured disk arrays.

-ddnh
   Displays the default credentials on the media server.

-default_user_id user_ID
   Configures a user name and password for all media servers and NDMP host
combinations under a given master server. You add a user name and password
only once per filer. Use this option with the -add, -update, or -delete command
to specify the user name and password.

-delete
   Deletes a drive, robot, or host credentials, depending on the accompanying
options.

-delete_media_server media_server
   Delete a media server that is associated with a CloudPoint server.

-dev_ping
   Retrieves the device information from a device.

-disk_array array_hostname
   Specifies the host name of the disk array. You can only use this option if the
NetBackup Snapshot Client license is installed.

-disk_user_id user_ID
   Specifies the user name that NetBackup must use to communicate with a disk
array. You can only use this option if the NetBackup Snapshot Client license
is installed.
-dl
  Lists the current configuration information in long format. On UNIX systems, the listing is sent to stdout. Lists the full drive name.

-dmediaservers [-cloudpoint_server cloudpoint_server_name]
  Displays all the media servers that are configured with a CloudPoint server. If you do not provide the CloudPoint server name, all the media servers that are configured with all the CloudPoint servers are displayed.

-dnh
  Displays the credentials on the NDMP host that is on the media server.

-drive
  Use this option with the -add option to specify that the action is for a drive.

-drive drvindex
  Specifies the drive index. Use this option with the -update, -delete, or the -multiple_delete command that specifies the action for a drive.

-drpath
  The drive path that is added, updated, or deleted.

-drstatus UP|DOWN|DISABLED
  Sets the initial status of the tape drive to the UP, DOWN, or DISABLED state. Discovered drive paths are enabled (UP) by default. An administrator or operator can disable or configure the drive path up/down. The user can also perform this action with options in the Device Management window.

  A drive status of DISABLED means NetBackup stores the path but never to use it. In addition, if subsequent discoveries of this drive path occur, NetBackup does not configure it for use.

-dsh
  Displays the OpenStorage credentials for the specified server type (-stype server_type) or for all media servers (-all_hosts).

-dvirtualmachines
  Displays all configured virtual computers.

-emm_dev_list [-noverbose]
  Lists the complete tape device configuration as seen by the EMM database. This information includes all media servers, master server, NDMP hosts, and their credentials.

-filer_user_id user ID
  Configures a user name and password for all media servers that are connected to a filer. You add a user name and password only once per filer. Use this
option with the -add, -update, or -delete command to specify the user name and password.

-host_user_id host user ID
Enter the host's user ID for SSH implementation. Use this option only with relevant BigData workloads. For example, MongoDB needs this option, but these are not required for Hadoop.

-host_password hostpassword
Enter the host's user password for SSH implementation. Use this option only with relevant BigData workloads. For example, MongoDB needs this option, but these are not required for Hadoop.

-host_RSA_key host RSA key
Enter the RSA key fingerprint for SSH implementation. Use this option only with relevant BigData workloads. For example, MongoDB needs this option, but these are not required for Hadoop.

-index drvindex
Specifies a drive index, a unique number that is used to identify the drive. When you add a drive, you are not required to supply a drive index, since Media Manager uses the next available drive index. Each drive on a particular host must have a unique index number.

-key encryption_key
Creates an encrypted key so that encrypted credentials can be safely sent over the network. If the -key option is specified, tpconfig assumes the password to be provided in MD5 encrypted format.

-l
Lists the current device configuration (to stdout). On Windows systems, -l displays the Windows device paths in the \{p,b,t,l\} encoded form: p is the port, b is the bus, t is the target, and l is the LUN.

-list_array_types [media_server]
Lists the disk array types for which you can add and manage credentials.

To restrict the output to the disk array types that are valid for a specific media server, specify that media server.

The command output is in a name:displayname format for each array type.

The disk array vendor provides the values for name:displayname. The name portion is a unique string used internally by NetBackup. The displayname portion is a more human-readable string that is used in NetBackup Administration Console displays and menus.
The values depend on the disk array vendor and the provider type that are used for the array, as follows:

- For an array-specific provider, the format is as follows:
  
  \[ \text{vendorID\_productID:displayname} \]

  By default, NetBackup includes several array-specific providers, including (but not limited to) the following:
  
  - \text{HP\_HSV:HP EVA}
  - \text{EMC\_CLARIION:EMC CLARiiON}
  - \text{EMC\_SYMMETRIX:EMC Symmetrix}
  - \text{IBM\_TOTALSTORAGE:IBM System Storage}
  - \text{NETAPP\_LUN:NetApp}

- For the generic array provider, the format is as follows:
  
  \[ \text{OPENARRAY::vendorID\_productID:displayname} \]

  For example, \text{OPENARRAY::HITACHI\_HDS:Hitachi HDS DF Series}.

- \text{-list\_supported\_cloud\_providers}
  
  Lists the integer that is associated with each cloud provider.

- \text{-list\_supported\_plugins}
  
  Lists all the supported CloudPoint plug-ins for the CloudPoint server that is configured with NetBackup.

- \text{-list\_plugins}
  
  List all the configured plug-ins with CloudPoint server.

- \text{-lun lun}
  
  Specifies the logical unit number (or SCSI ID) to which the robot or drive connects.

  For more about device paths, see the \text{NetBackup Device Configuration Guide}.

- \text{-manage\_workload}
  
  Specifies if the CloudPoint server is used for on-premises storage array management or in-cloud workloads. This option is required when you register a CloudPoint server.

  - \text{ONPREM} specifies that the CloudPoint server is used for on-premises storage array management.

  - \text{CLOUD} specifies that the CloudPoint server is used for cloud management.
-modify_plugin
  Modifies the credentials of a CloudPoint plug-in that is added to the CloudPoint server that is configured with NetBackup.

-multiple_delete
  Deletes multiple drives or robots, depending on the accompanying options.

-newasciiname asciidrivename
  Specifies a new name for the drive.

-nh ndmp_hostname | puredisk_hostname
  Specifies the host name of the NDMP server or the PureDisk server. Veritas supports the PureDisk option on NetBackup 5000 series appliances only.

-noverify
  Drive paths are not verified. Normally, tpconfig verifies that the no rewind on close drive path has the correct minor number bits that relate to the following: No rewind, variable, Berkeley-style, and so on. This option may be helpful if you use non-standard platform device files, so make sure that your device files are correct.

-old_bus bus
  This option is used on Windows systems. It specifies the SCSI bus number that a user may want to add, upgrade, or delete.

-old_lun lun
  This option is used on Windows systems. It specifies the logical unit number (or SCSI ID) to which the robot or drive connects. You can find this information in the registry. Use this command to add, upgrade, or delete an existing logical unit number.

-old_path drivepath
  When this option is used with the -update command, you can change the path to one that already exists in the database. If the path does not exist, an error occurs.

-old_port port
  This option is used on Windows systems. It specifies an existing SCSI port number that a user may want to add, upgrade, or delete.

-old_target target
  This option is used on Windows systems. It specifies an existing target number (or SCSI ID) to which the robot or drive connects. Use this command to add, upgrade, or delete an existing target.
-password password

Sets the password to log on to the NDMP, Media Server Deduplication Pool, OpenStorage, virtual machine host, or an application server. The password length should not exceed 100 characters.

-path drivepath

Specifies the drive’s device path on the media server or on the NDMP filer.

On Windows systems, the drive_path variable is a non-NDMP Windows device path for drives. Use it in the {p,b,t,l} format: p is the port, b is the bus, t is the target, and l is the LUN. This information is located in the registry.

-plugin_id netbackup_plugin_ID

Specify a plug-in ID for NetBackup to associate with the cloud plug-in. The plug-in ID must be unique. The ID can contain only the letters and symbols shown:

- A-Z, a-z
- 0-9
- +, ., _, -

-plugin_type cloudpoint_plugin_type

Specify the CloudPoint plug-in type. You can use the tpconfig -list_supported_plugins command to get a list of all the CloudPoint server supported plug-ins.

-port port

Specifies the SCSI port number to which the robot or drive connects. You can find this information in the registry.

-refresh

Refreshes the CloudPoint server.

-requiredport IP_port_number

Specifies the IP port number on which the disk array, a virtual machine, or an application server accepts a connection from NetBackup. The default port number for a Nutanix Acropolis Cluster is 9440. The default port number for Hadoop is HDFS NameNode HTTP UI. The provision to change this port number is available only through the command line interface. If you have configured the host-related parameters for a BigData workload, you must specify all the parameters if you want to update the required port.

-reset_password

Resets the CloudPoint server password.
-robdrnum robdrvnum

Specifies the physical location (within the robot) of the drive. If you assign the wrong number, NetBackup does not detect it. An error eventually occurs because the robotic control tries to mount media on the wrong drive.

You can usually determine the physical location by checking the connectors to the drives or the vendor documentation.

-robot robnum

A unique number that identifies the robot to NetBackup. You assign the robot number with the add option.

Robot numbers must be unique for all robots, regardless of the robot type or the host that controls them.

On NetBackup Enterprise Server, robot numbers must be unique for all robots that share the same EMM server (and use the same EMM database). This requirement applies regardless of the robot type or the host that controls them. For example, the same EMM server but different hosts control two TLD robots. If so, the robot numbers must be different.

-robpath devfile

Specifies the robot's device path on the media server or on the NDMP filer.

On Windows systems, the drive_path variable is a non-NDMP Windows device path for drives. Use it in the \{p,b,t,l\} format: p is the port, b is the bus, t is the target, and l is the LUN. This information is located in the registry.

-robtype robtype

Specifies the type of robot that you plan to configure and can be any of the types that NetBackup supports. Check the Support website to determine the robot type to specify for a particular model of robotic library.

Robot type can be any of the following for NetBackup Enterprise Server:

acs for Automated Cartridge System or tld for tape library DLT.

Robot type can be any of the following for NetBackup server:

tld for tape library DLT

-scsi_protection SPR | SR | NONE

Specifies the access protection that NetBackup uses for SCSI tape drives.

SPR - SCSI Persistent Reserve In / Persistent Reserve Out
SR - SCSI Reserve/Release
NONE - No SCSI access protection

The default condition is SCSI Reserve/Release (SR).
-shared yes|no
Indicates that you want to add or update shared drives.

-snap_vault_filer
The -snap_vault_filer flag is used with the NetApp P3 feature. Set this flag when the user name and password for that filer are stored. If not set, the user interfaces do not allow the user to add volumes on this filer. If you stash the user name and password without this flag, do the following: Decide if you want its functionality, do a tpconfig -delete operation, and then re-add it with the flag. This flag is used with the NetApp P3 feature when used in the following context:

```
tpconfig -add -user_id root -nh mmnetapp2-target target
-snap_vault_filer
```

-st storage_type
Specifies a numeric value that identifies the storage server properties. The storage vendor provides this value. Whether the disk is formatted and how it is attached are mutually exclusive and complementary.

The following are the possible values of storage_type:

- Formatted disk = 1
- Raw disk = 2
- Direct attached = 4
- Network attached = 8

The storage_type value is the sum of whether the disk is formatted or raw (1 or 2) and how the disk is attached (4 or 8). The default value is 9 (a network attached, formatted disk).

-storage_server server_name
Specifies the host name of the storage server.

-sts_user_id user_id
Specifies the user name that is needed to log into the storage server. If the storage server does not require logon credentials, enter dummy credentials.

You must remember these credentials. You need these credentials during disaster recovery of the CloudCatalyst storage server.

-stype server_type
Specifies a string that identifies the storage server type. The server_type value can originate from one of the following sources:

- Veritas provided storage. Possible values are AdvancedDisk and PureDisk.
- Third-party disk appliances. The vendor supplies the `server_type` string.

- Cloud storage. Use the `csconfig cldprovider -l` command to determine the possible `stype` values. The cloud `stype` values reflect the cloud storage provider. Cloud storage `stype` values can also incorporate a suffix (for example, `amazon_crypt`). Possible suffixes are:
  - `_raw`: The NetBackup backup image is sent to the cloud in raw format. Use this option if you do not want to compress or encrypt data before sending to cloud storage.
  - `_rawc`: Compresses the data before it is written to the cloud storage.
  - `_crypt`: Encrypts the data using AES-256 encryption before writing the data to cloud storage. You must have KMS configured in NetBackup to use this option.
  - `_cryptc`: Compress and encrypt the data before writing to cloud storage.

The storage server type is case-sensitive.

- **-target target**
  Specifies the target number (or SCSI ID) to which the robot or drive connects.

  You can find this information in the registry (Windows systems) or the `NetBackup Device Configuration Guide`.

- **-type drvtype**
  Specifies the type of drive that you configure.

  Drive type can be any of the following for NetBackup Enterprise Server:

  - `4mm` for 4mm tape drive, `8mm` for 8mm tape drive, `8mm2` for 8mm tape drive 2, `8mm3` for 8mm tape drive 3, `dlt` for DLT tape drive, `dlt2` for DLT tape drive 2, `dlt3` for DLT tape drive 3, `dtf` for DTF tape drive, `qscsi` for QIC tape drive, `hcart` for Half-inch cartridge drive, `hcart2` for Half-inch cartridge drive 2, `hcart3` for half-inch cartridge drive 3. Drive type can be any of the following for NetBackup server: `4mm` for 4mm tape drive, `8mm` for 8mm tape drive, `dlt` for DLT tape drive, `hcart` for Half-inch cartridge drive, `qscsi` for QIC tape drive.

- **-update**
  Changes the configuration information for a drive, robot, or CloudPoint server.

- **-user_id user_ID**
  Specifies the user ID of a particular NDMP host on a media server for which you add credentials.
**Note:** A media server is allowed only one user ID per NDMP host name. If you try to add a second user ID for a single NDMP host name fails.

-virtual_machine virtual_machine_name
Specifies the host name of the virtual machine whose credentials are to be added, updated, or deleted. You can only use this option if the NetBackup Snapshot Client license is installed.

-vm_type virtual_machine_type
Specifies the type of virtual machine. The following are possible values:
1 - VMware VirtualCenter Servers
2 - VMware ESX Servers
3 - VMware Converter Servers
You can only use this option if the NetBackup Snapshot Client license is installed.

-vm_user_id user_id
Specifies the user name that NetBackup must use to communicate with a virtual machine’s disk array. You can only use this option if the NetBackup Snapshot Client license is installed.

You must have administrator privileges to run this command.

**NOTES**

`tpconfig -d` may truncate drive names to 22 characters, and `tpconfig -l` may truncate drive names to 32 characters. To list the full drive name, use `tpconfig -dl`.

The delete multiple NDMP host credentials applies only to credentials that are specific to this host and the specified filer. In other words, it has no default or no filer credentials.

**EXAMPLES**

In the following examples, the command that is entered is shown on multiple lines because of page limitations. The actual command is entered on one line.

**Example 1 - Robotic control on the local Windows server**
The following example adds a robot that connects directly to a Windows host, and also adds drives to that robot.

The following procedure applies only to NetBackup server:
- Add the robot by using the following command:
  
  ```
  # tpconfig -add -robot 7 -robtype tld -port 0 -bus 0 -target 2 lun 0
  ```

- If there are drives in the robot that have not been configured, add them. The following command configures the drive with the system name of Tape0 under control of the robot that is configured in step 1. (The server has attached and recognized Tape0.)
  
  ```
  # tpconfig -add -drive -type dlt -port 1 -bus 2 -target 3 / -lun 4 -comment "DEC DLT2000 8414" -index 0 -drstatus up / -robot 7 -robtype tld -robdrnum 1 -asciiname DLT2000_D1
  ```

  The command in this example uses the comment field. This field is useful for storing the drive’s SCSI inquiry data so that drive type and firmware level can be easily checked.

- If the robot contains any drives that are currently configured as standalone drives, update the drive configuration to place them under robotic control. The following commands update the configuration for drives 1 and 2:
  
  ```
  # tpconfig -update -drive 1 -type dlt -robot 7 -robtype tld
  # tpconfig -update -drive 2 -type dlt -robot 7 -robtype tld
  ```

  **Note:** Assign the correct robot drive number to the drives. If robot drive numbers are incorrect, tape mounts or backups may fail.

**Example 2 - Robotic control on the remote host**

This example applies only to NetBackup Enterprise Server:

It assumes that one or more tape drives that are in the robot, connect to the Windows host where you currently manage devices.

The following is a sequence of `tpconfig` operations that adds a robot that connects to another host:

- Add the robot by executing the following command:
  
  ```
  # tpconfig -add -robot 9 -robtype tld -cntlhost perch
  ```

  Ensure that the robot number matches the one on the control host.

- If the robot contains any drives that are currently configured as standalone, update the drive configuration to place them under robotic control.
The following commands update the configuration for drives 1 and 2:

```bash
# tpconfig -update -drive 1 -type dlt -robot 9 -robtype tld -robdrnum 1
# tpconfig -update -drive 2 -type dlt -robot 9 -robtype tld -robdrnum 2
```

**Note:** Assigned the correct robot drive number. If robot drive numbers are incorrect, tape mounts or backups may fail.

- If there are drives in the robot that have not been configured, add them now. The following command configures the drive with the system name of Tape0 under control of the robot that is configured in step 1. (The Windows server has attached and recognized Tape0.)

```bash
# tpconfig -add -drive -type dlt -port 1 -bus 2 -target 3 -lun 4 -comment 'DEC DLT2000 8414' -index 3 -drstatus up -robot 9 -robtype tld -robdrnum 3 -asciiname DLT2000_D3
```

**Example 3 - Configuring new standalone drives**

The following is an example of how to add a standalone drive after the drive is installed:

```bash
# tpconfig -add -drive -type dlt -port 1 -bus 2 -target 3 -lun 4 -comment 'DEC DLT2000 8414' -index 6 -asciiname DLT2000_standalone
```

**Example 4 - Demonstrate how Windows displays device paths**

This example demonstrates how the `-l` option displays the Windows device paths in the `p, b, t, l` format.

```
C:\Program Files\VERITAS\Volmgr\bin>tpconfig -l
```

<table>
<thead>
<tr>
<th>Device</th>
<th>Robot</th>
<th>Drive</th>
<th>Robot</th>
<th>Drive</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Num</td>
<td>Index</td>
<td>Type</td>
<td>DrNum</td>
<td>Status</td>
</tr>
<tr>
<td>robot</td>
<td>0</td>
<td>-</td>
<td>TLD</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>robot</td>
<td>1</td>
<td>-</td>
<td>TLD</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>robot</td>
<td>2</td>
<td>-</td>
<td>TLD</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>drive</td>
<td>-</td>
<td>0</td>
<td>pcd</td>
<td>-</td>
<td>DISABL</td>
</tr>
<tr>
<td>drive</td>
<td>-</td>
<td>1</td>
<td>hcart2</td>
<td>2</td>
<td>UP</td>
</tr>
<tr>
<td>drive</td>
<td>-</td>
<td>1</td>
<td>hcart2</td>
<td>2</td>
<td>UP</td>
</tr>
<tr>
<td>drive</td>
<td>-</td>
<td>2</td>
<td>hcart2</td>
<td>1</td>
<td>UP</td>
</tr>
<tr>
<td>drive</td>
<td>-</td>
<td>2</td>
<td>hcart2</td>
<td>1</td>
<td>UP</td>
</tr>
<tr>
<td>drive</td>
<td>-</td>
<td>3</td>
<td>hcart</td>
<td>1</td>
<td>DOWN</td>
</tr>
</tbody>
</table>
Example 5 - Add a CloudPoint server in NetBackup

```
tpconfig -add -cloudpoint_server testserver.test.com
-cloudpoint_server_user_id User1 -manage_workload ONPREM -requiredport 1024
```

Enter the CloudPoint Server host's password for User Id User 1:

Please re-enter the CloudPoint Server host's password to confirm it:

Example 6 - Add a CloudPoint plugin in NetBackup

```
tpconfig -add_plugin -cloudpoint_server testserver.test.com
-plugin_id ITAzure -plugin_type azure
```

Enter Tenant ID: test

Enter Client ID: test

Enter Secret Key:

Enter confirm Secret Key:

SEE ALSO

See `ltid` on page 549.
tpext

tpext – update EMM database device mappings and external attribute files

SYNOPSIS

tpext -loadEMM

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\

DESCRIPTION

The tpext command updates the EMM database with new versions of the device mappings and external attribute files.

EXAMPLE

Before you repopulate this data, make sure that you have the most current support for new devices. New devices are added approximately every two months.

■ Obtain the external_types.txt mapping file from contact Technical support.

■ On the EMM server or the master server, place external_types.txt in the following directory to replace the current external_types.txt file:

UNIX systems: /usr/openv/var/global

Windows systems: install_path\var\global

■ Repopulate the EMM data by running the tpext utility:

UNIX systems: /usr/openv/volmgr/bin/tpext -loadEMM

Windows systems: install_path\Volmgr\bin\tpext -loadEMM

During regular installation, tpext is run automatically.

Caution: If you use the create_nbdb command to create a database manually, you must also run the tpext utility. tpext loads EMM data into the database.
tpreq

tpreq – request a tape volume for mounting and assign a file name to the drive

SYNOPSIS

```
tpreq -m media_id [-a accessmode] [-d density] [-p poolname]
[-priority number] [-f] filename
```

On UNIX systems, the directory path to this command is
/usr/openv/volmgr/bin/

On Windows systems, the directory path to this command is
install_path\Volmgr\bin\n
DESCRIPTION

This command initiates a mount request for a tape volume on a removable media
device. The information that you specify with this command identifies and registers
the specified file as a logical identifier for the mount request with Media Manager.
It also manages access to the volume.

Media Manager automatically mounts the media if it is in a robotic drive. Otherwise,
an operator mount request appears in the Device Monitor window. tpreq does not
complete normally in the case of a mount request for a robotic drive, if operator
intervention is required. These requests also appear in the Device Monitor window.

When the operation is complete, use tpunmount to unmount the volume and remove
the file name from the directory in which the file was created.

On UNIX systems, tpreq calls the script drive_mount_notify immediately after
the media is successfully placed in a pre-selected drive. This script allows user
special handling to occur now. Control is then returned to tpreq to resume
processing. The script is only called from the tpreq command for the drives that
are in robots and is not valid for standalone drives. This script resides in the
/usr/openv/volmgr/bin/goodies directory. To use this script, activate it and copy it
into the /usr/openv/volmgr/bin directory; usage information is documented within
the script.

You must have administrator privileges to run this command.
OPTIONS

-\texttt{m} \texttt{media\_id}
  
  Specifies the media ID of the volume to be mounted. You can enter the ID in upper or lowercase; Media Manager converts it to uppercase.

-\texttt{a} \texttt{accessmode}
  
  Specifies the access mode of the volume. Valid access modes are \texttt{w} and \texttt{r}. If the access mode is \texttt{w} (write), the media must be mounted with write enabled. The default is \texttt{r} (read), which means the media may be write protected.

-\texttt{d} \texttt{density}
  
  Specifies the density of the drive. This option determines the type of drive on which the tape volume is mounted. The default density is \texttt{dlt}.

Valid densities for NetBackup Enterprise Server follow:

4mm for 4-mm cartridge, 8mm for 8-mm cartridge, 8mm2 for 8-mm cartridge 2, 8mm3 for 8-mm cartridge 3, dlt for DLT cartridge, dlt2 for DLT cartridge 2, dlt3 for DLT cartridge 3, dtf for DTF cartridge, \texttt{hcart} for 1/2-inch cartridge, \texttt{hcart2} for 1/2 Inch cartridge 2, \texttt{hcart3} for 1/2 Inch cartridge 3, qscsi for 1/4-inch cartridge.

The following applies only to NetBackup Enterprise Server:

The half-inch cartridge densities (\texttt{hcart}, \texttt{hcart2}, and \texttt{hcart3}) can be used to distinguish between any supported half-inch drive types. However, tape requests can only be assigned to drives of the associated media type. For example, it assigns a tape request with density \texttt{hcart2} that specifies a media ID with media type \texttt{HCART2} to an \texttt{hcart2} drive. Likewise, it assigns a tape request with density \texttt{hcart} that specifies a media ID with media type \texttt{HCART} to an \texttt{hcart} drive. The same rules apply to the DLT densities (\texttt{dlt}, \texttt{dlt2}, and \texttt{dlt3}) and the 8MM densities (8mm, 8mm2, and 8mm3).

Valid densities for NetBackup server follow:

4mm for 4-mm cartridge, 8mm for 8-mm cartridge, dlt for DLT cartridge, \texttt{hcart} for 1/2 Inch cartridge, qscsi for 1/4-inch cartridge.

The mount request must be performed on a drive type that satisfies the density.

-\texttt{p} \texttt{poolname}
  
  Specifies the volume pool where the volume resides. \texttt{poolname} is case-sensitive. The default is None.

-\texttt{priority} \texttt{number}
  
  Specifies a new priority for the job that overrides the default job priority.
-f filename

Specifies the file to be associated with the volume. The file name represents a symbolic link to the drive where the volume is mounted.

The file name can be a single name or a complete path. If you specify only a file name, the file is created in the current working directory. If you specify a path, the file is created in the directory that is named in the path. filename cannot be an existing file.

If the tpreq command is successful, Media Manager creates a file with the name that you specified. This file contains the name of the tape device where the media is mounted. Do not delete this file. Use the tpunmount command to remove it.

The specification of -f before filename is optional.

EXAMPLE

Create file tape1 in the current working directory that links the file to the drive that contains the volume whose media ID is JLR01. The access mode for the tape file is set to write, and a 1/4-inch cartridge drive is assigned.

# tpreq -f tape1 -m jlr01 -a w -d qscsi

SEE ALSO

See tpunmount on page 917.
**tpunmount**

*tpunmount* – remove a tape volume from a drive and a tape file from the directory

**SYNOPSIS**

```
.tpunmount [-f] filename [-force]
```

On UNIX systems, the directory path to this command is /usr/openv/volmgr/bin/

On Windows systems, the directory path to this command is install_path\Volmgr\bin\n
**DESCRIPTION**

*tpunmount* removes a tape file from the directory and physically removes the tape volume from the drive (if the media was mounted).

On UNIX systems, when *tpunmount* is executed for drives, a call is made to execute the `drive_unmount_notify` script. This script allows user special-handling to occur. Control is then returned to *tpunmount* to resume processing. The script resides in the `/usr/openv/volmgr/bin/goodies` directory. To use this script, activate it and copy it into the `/usr/openv/volmgr/bin` directory. The script is called from the *tpreq* command for only the drives that are in robots. The script is not valid for standalone drives or NDMP drives.

Standalone drives are not unloaded when the `DO_NOT_EJECT_STANDALONE` option is specified (and the `-force` option is not specified). This option is now stored in EMM.

The tape file and the device must be closed before you can use *tpunmount*.

You must have administrator privileges to run this command.

**OPTIONS**

- **-f filename**
  
  Specifies the file that is associated with the media. You must specify a file name. The specification of `-f` before `filename` is optional.

- **-force**
  
  Ejects the volume from a standalone drive, even if `DO_NOT_EJECT_STANDALONE` is specified in the EMM database.
EXAMPLE

The following command unmounts the tape volume that is associated with file `tapel` and removes the file from the current directory:

```
# tpunmount tapel
```

SEE ALSO

See `tpreq` on page 914.
verifytrace

verifytrace – trace debug logs for verify jobs

SYNOPSIS

verifytrace [-master_server name] -job_id number [-start_time hh:mm:ss] [-end_time hh:mm:ss] mmddyy [mmddyy _]

verifytrace [-master_server name] -backup_id id [-start_time hh:mm:ss] [-end_time hh:mm:ss] mmddyy [mmddyy _]

verifytrace [-master_server name] [-policy_name name] [-client_name name] [-start_time hh:mm:ss] [-end_time hh:mm:ss] mmddyy [mmddyy _]

On UNIX systems, the directory path to this command is 
/usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is 
install_path\NetBackup\bin\admincmd

DESCRIPTION

The verifytrace command consolidates the debug log messages for the specified verify jobs and writes them to standard output. The messages sort by time. verifytrace tries to compensate for time zone changes and clock drift between remote servers and clients.

At a minimum, you must enable debug logging for the following:

- UNIX systems: The /usr/openv/netbackup/admin directory on the master server
- Windows systems: The install_path\NetBackup\bin\admincmd directory on the master server
- The bpbrm, bptm/bpdm, and tar commands on the media server

For best results, set the verbose logging level to 5. Enable debug logging for bpdbm on the master server and bpcd on all servers and clients in addition to already identified processes.

If you specify either -job_id or -backup_id, verifytrace uses this option as the sole criteria to select the verify jobs it traces. You cannot use the options -policy_name or -client_name with -job_id or -backup_id. If you do not specify -job_id or -backup_id, verifytrace selects all the verify jobs that match the
specified selection criteria. If none of the following options is specified, verifytrace traces all the jobs that ran on the days that the day stamps (mmddyy) specify:
- \(-\text{job\_id}\), \(-\text{backup\_id}\), \(-\text{policy\_name}\), or \(-\text{client\_name}\). If \(-\text{start\_time}/-\text{end\_time}\) options are used, the debug logs on the specified time interval are examined.

If \texttt{verifytrace} is started with \(-\text{backup\_id id}\), it looks for a verify job that \texttt{bpverify} started with \(-\text{backup\_id id}\) where the backup IDs (\textit{id}) match.

If \texttt{verifytrace} is started with \(-\text{policy\_name name}\), it looks for a verify job that \texttt{bpverify} started with \(-\text{policy\_name name}\) where the policy names (\textit{name}) match.

If \texttt{verifytrace} is started with \(-\text{client\_name name}\), it looks for a verify job that \texttt{bpverify} started with \(-\text{client\_name name}\) where the client names (\textit{name}) match.

\texttt{verifytrace} writes error messages to standard error.

You must have administrator privileges to run this command.

\section*{OPTIONS}

\begin{description}
\item \texttt{-master\_server}
  Name of the master server. Default is the local host name.
\item \texttt{-job\_id}
  Job ID number of the verify job to analyze. Default is any job ID.
\item \texttt{-backup\_id}
  Backup ID number of the backup image that the verify job verified to analyze. Default is any backup ID.
\item \texttt{-policy\_name}
  Policy name of the verify jobs to analyze. Default is any policy.
\item \texttt{-client\_name}
  Client name of the verify jobs to analyze. Default is any client.
\item \texttt{-start\_time}
  Earliest timestamp to start analyzing the logs. Default is 00:00:00
\item \texttt{-end\_time}
  Latest timestamp to finish analyzing the logs. Default is 23:59:59.
\item \texttt{mmddyy}
  One or more "day stamps". This option identifies the log file names (log.mmddyy for UNIX, mmddyy.log for Windows) that are analyzed.
\end{description}
OUTPUT FORMAT

The format of an output line is: `daystamp.millisecs.program.sequence machine log_line`

daystamp
The day of the log is created in `yyyymmdd` format.

millisecs
The number of milliseconds since midnight on the local computer.

program
The name of program (ADMIN, BPBRM, BPCD, 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.

EXAMPLES

Example 1 - Analyze the log of verify job with job ID 2 that ran on August 6, 2011.

# verifytrace -job_id 2 080611

Example 2 - Analyzes the verify jobs log that verify backup images with backup ID `pride_1028666945`, which ran on 20th August 2011. This command only analyzes those verify jobs that ran with option `-backupid pride_1028666945`.

# verifytrace -backup_id pride_1028666945 082011

Example 3 - Analyzes the verify jobs log that ran on policy `Pride-Std` and client `pride` on August 16, 2011 and August 23, 2011. This command only analyzes those verify jobs that ran with options `-policy Pride-Std` and `-client pride`.

# verifytrace -policy_name Pride-Std -client_name pride 081611 082311

Example 4 - Analyzes the verify jobs log that ran on August 5, 2011 and August 17, 2011.

# verifytrace 080511 081711
**vltadm**

vltadm – start the NetBackup Vault menu interface for administrators

**SYNOPSIS**

vltadm [-version]

The directory path to this command is /usr/openv/netbackup/bin/

**DESCRIPTION**

This command operates only on UNIX systems.

vltadm is a menu interface utility that an administrator can use to configure NetBackup Vault. You must have administrator privileges. This command can be used from any character-based terminal (or terminal emulation window) for which the administrator has a `termcap` or `terminfo` definition.

See the *NetBackup Vault Administrator’s Guide* and the vltadm online Help for detailed operating instructions.

**OPTIONS**

- `-version`

  Display the vltadm version and exit.

**RETURN VALUES**

Vault may exit with a status code greater than 255. Such status codes are called extended exit status codes. For such a case, the exit status that is returned to the system is 252. The actual exit status is written to `stderr` in the format, `EXIT status = exit status`

The extended exit status values are documented in the *NetBackup Troubleshooting Guide* and in the NetBackup Troubleshooter Wizard.

**FILES**

/usr/openv/netbackup/help/vltadm/*
/usr/openv/netbackup/db/vault/vault.xml
/tmp/bp_robots
/tmp/bp_vaults
/tmp/bp_profiles
/tmp/bp_duplicates
/tmp/_tmp
vltcontainers

vltcontainers – move volumes logically into containers

SYNOPSIS

vltcontainers -run [-rn robot_number]
vltcontainers -run -usingbarcodes [-rn robot_number]
vltcontainers -run -vltcid container_id -vault vault_name -sessionid session_id
vltcontainers -run -vltcid container_id -f file_name [-rn robot_number] [-usingbarcodes]
vltcontainers -view [-vltcid container_id]
vltcontainers -change -vltcid container_id -rd return_date
vltcontainers -delete -vltcid container_id
vltcontainers -version

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/
On Windows systems, the directory path to this command is
install_path\NetBackup\bin\n
DESCRIPTION

vltcontainers logically adds to containers the media that was ejected from one or more vault sessions. It can view, set, or change the return date of containers that go off-site or are already at the off-site vault. vltcontainers can also delete a container from the NetBackup and Media Manager catalogs.

You can add media IDs to containers as follows:

- Use the keyboard to enter the container and the media IDs.
- Use a keyboard interface barcode reader to scan the container IDs and media IDs. Keyboard interface readers are also known as keyboard wedge readers because they connect (or wedge) between the keyboard and the keyboard port on your computer.
- Use an input file that contains the media IDs or numeric equivalents of barcodes of all the media that are added to one container. To add media to more than one container, enter the IDs by using the keyboard or a keyboard interface barcode reader. Or, run the `vltcontainers` command again and specify different container and file name options.

- Add all the media that a specific session ejects to one container. To add media from a single eject session into more than one container, enter IDs using the keyboard or a keyboard interface barcode reader.

The required date and time values format in NetBackup commands varies according to your locale. The `/usr/openv/msg/.conf` file (UNIX) and the `install_path\VERITAS\msg\LC.CONF` file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

See the "About specifying the locale of the NetBackup installation" topic in the NetBackup Administrator's Guide, Volume II for more information.

Run the `vltcontainers` command from a NetBackup master server that is licensed for Vault.

If the following directory with public-write access exists, `vltcontainers` writes to its daily debug log file (`log.DDMMYY` where `DDMMYY` is current date):

UNIX systems: `usr/openv/netbackup/logs/vault`

Windows systems: `install_path\netbackup\logs\vault`

Public-write access is required because not all executable files that write to this file can run as administrator or root user.

**OPTIONS**

- **-change**
  Changes the default return date for the container. The default return date of a container is the date of the volume in the container that is returned the latest. It requires the `-vltcid container_id` option.

- **-delete**
  Deletes the container record from the NetBackup and Media Manager catalogs. You can delete a container only if it contains no media.

- **-f file_name**
  Specifies the file from which to read media IDs. All the listed media in the file are added to the container that the `-vltcid` option specifies. The file can be a list of media IDs (one per line). Or it can be the numeric equivalents of barcodes (one per line) scanned into a file by a barcode reader.
-rd return_date
   Specifies the return date for the container.
   The return date format depends on the locale setting.

-rn robot_number
   Specifies the robot, which is used to determine the EMM Server from which
   the vltcontainers command should obtain media information. If -rn
   robot_number is not used, the master server is considered as the EMM server.
   The only media that can be added to containers is the media in the database
   on the EMM server.

-run
   Logically adds media to the container. If you specify no other options, you must
   enter the container IDs and the media IDs by using the keyboard. To use a
   barcode reader to scan the container and the media IDs, specify the
   -usingbarcodes option. To add the media that a specific session ejects, use
   the -vault vault_name and -sessionid session_id options. To add the
   media that is specified in a file, use the -f file_name option. To specify an
   EMM server other than the master server, use the -rn robot_number option.

-sessionid session_id
   The ID of a vault session. All media that the specified session ejects are added
   to the container that the -vltcid option specifies.

-usingbarcodes
   Specifies a keyboard interface barcode reader that scans container IDs and
   media IDs, or the barcode numbers that are used in the file that -f file_name
   specifies. Keyboard interface barcode readers (also called keyboard wedge
   barcode readers) connect between the keyboard and the keyboard port on
   your computer.

-vault vault_name
   The name of the vault to which the profile that ejected the media belongs. You
   also must specify the ID of the session (-sessionid) that ejected the media
   to be added to the container.

-version
   Displays the vltcontainers version and exit.

-view [-vltcid container_id]
   Shows the return date that is assigned to all containers. Use the -vltcid
   container_id option and argument to show the return date of a specific
   container.
Specifies the container ID. Container ID can be a string of up to 29 alphanumeric characters (no spaces). The \(-rd\) \(\text{return\_date}\) option and argument are required to change a container return date.

**EXAMPLES**

Example 1 - Use the following command to:
- Add the volumes that are ejected from robot number 0 to containers.
- Use a barcode reader to scan the container ID and media ID.

```bash
# vltcontainers -run -usingbarcodes -rn 0
```

Example 2 - View the return date of container ABC123:

```bash
# vltcontainers -view -vltcid ABC123
```

Example 3 - Change the return date of container ABC123 to December 07, 2012:

```bash
# vltcontainers -change -vltcid ABC123 -rd 12/07/2012
```

Example 4 - Delete container ABC123 from the NetBackup and Media Manager catalogs, use the following command:

```bash
# vltcontainers -delete -vltcid ABC123
```

Example 5 - Add all media that was ejected to container ABC123 by session 4 of vault MyVault_Cntr, use the following command:

```bash
# vltcontainers -run -vltcid ABC123 -vault MyVault_Cntr -sessionid 4
```

Example 6 - Add the media that is listed in the `medialist` file that is ejected from robot number 0 to container ABC123:

**UNIX systems:**

```bash
# vltcontainers -run -vltcid ABC123 -f /home/jack/medialist -rn 0
```

**Windows systems:**

```bash
# vltcontainers -run -vltcid ABC123 -f C:\home\jack\medialist -rn 0
```

Example 7 - Use the following command to:
- Add media to container ABC123 that was ejected from a robot that is attached to the master server
Read the barcodes for that media from the medialist file

UNIX systems: # vltcontainers -run -vltcid ABC123 -f /home/jack/medialist -usingbarcodes

Windows systems: # vltcontainers -run -vltcid ABC123 -f C:\home\jack\medialist -usingbarcodes

RETURN VALUES

Vault may exit with a status code greater than 255. Such status codes are called extended exit status codes. For such a case, the exit status that returned to the system is 252. The actual exit status is written to stderr in the format EXIT status = exit status

The extended exit status values are documented in the NetBackup Troubleshooting Guide and in the NetBackup Troubleshooting Wizard.

FILES

UNIX systems:

/usr/openv/netbackup/vault/sessions/cntrDB
/usr/openv/netbackup/db/vault/vault.xml
/usr/openv/netbackup/logs/vault

Windows systems:

install_path\NetBackup\vault\sessions\cntrDB
install_path\NetBackup\db\vault\vault.xml
install_path\NetBackup\logs\vault

SEE ALSO

See vltoffsitemedia on page 935.
See vltopmenu on page 939.
vlteject

vlteject – eject media and generate reports for previously run sessions

SYNOPSIS

vlteject
vlteject -eject [-profile profile_name] [-robot robot_name] [-vault vault_name [-sessionid id]] [-auto y|n] [-eject_delay seconds]
vlteject -report [-profile profile_name] [-robot robot_name] [-vault vault_name [-sessionid id]] [-legacy]
vlteject -preview [-vault vault_name [-profile profile_name]] [-profile robot_no / vault_name / profile_name] [-robot robot_name] [-sessionid id]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/
On Windows systems, the directory path to this command is install_path\NetBackup\bin

DESCRIPTION

vlteject ejects media and generates the corresponding reports (as configured in the profiles) for vault sessions for which media have not yet been ejected. vlteject can process the pending ejects and reports for all sessions, for a specific robot, for a specific vault, or for a specific profile. To process all pending ejects and reports, do not use the -profile, -robot, or -vault option.

vlteject operates only on sessions for which the session directory still exists. After that directory is cleaned up (removed by NetBackup), vlteject can no longer eject or report for that session.

Whether vlteject can run interactively or not depends on how it is called. Run interactively when you plan to eject more media than that amount that fits in the media access port.

Do not modify your vault configuration while vlteject is running.
vlteject can be run in any of the following ways:

- Directly from the command line
- By using the NetBackup policy schedule. The policy must be of type Vault, and the policy’s file list must consist of a vlteject command.
- By using vltopmenu to run an eject operation or a consolidated eject or consolidated report operation

If the following directory exists and has public write access, vlteject writes to its daily debug log file:

- UNIX systems: /usr/openv/netbackup/logs/vault
- Windows systems: install_path\netbackup\logs\vault

The daily debug log file is log.DDMMYY; the DDMMYY is the current date.

Public-write access is required because not all executable files that write to this file can run as administrator or root user. The host property "Keep vault logs for n days" determines how long the vault session directories are retained.

Any authorized user can run this command.

For more information about NetBackup authorization, refer to the NetBackup Security and Encryption Guide.

OPTIONS

- -auto y|n
  Specifies automatic (y) or interactive mode (n). In automatic mode (y), vlteject runs without input from the user and does not display output. In interactive mode (default), vlteject runs interactively. It accepts input and displays output.

- -eject
  Ejects the media for the indicated sessions. -eject is optional if eject was completed and you only want to generate reports.

- -eject_delay seconds
  The number of seconds to delay before the media is ejected. This option is useful if an operation such as backing up or duplication recently occurred on the affected media. The default is 0. The maximum is 3600 (1 hour).

- -legacy
  Generates the reports by using the old-style consolidation. Valid only with the -report option.
-preview
Lists the sessions and the media that are ejected for the sessions. Does not eject the media.

-profile robot _no / vault_name / profile_name
Identifies a robot number, vault name, and profile name from which to eject media and generate reports. All three options must be used with -profile. To process all pending ejects and reports, use -profile with profile_name only.

-report
Generates the reports for the indicated sessions. If the corresponding eject process has completed, it generates and distributes any pending reports from the selected sessions. The reports are not generated again if vlteject is run again. If the eject has not completed, the subset of reports that does not depend on completion of eject are generated. These reports are generated again if vlteject -report is run again after eject has completed.

-robot robot_no
Specifies the robot number that identifies the robot which you want to eject media and generate reports. All vaults in the robot should use the same off-site volume group. To process all pending ejects and reports, do not use the -profile, -robot, or -vault option.

-sessionid id
The numeric session ID. If -profile, -robot, or -vault is specified, but -session id is not specified, vlteject operates on all sessions for the specified profile, robot, or vault.

-vault vault_name
The vault for which to eject media and generate reports. To process all pending ejects and reports; do not use the -profile, -robot, or -vault option.

-version
Displays the vlteject version and exit.

EXAMPLES

Example 1 - Eject media and generate reports for all robots that have sessions for which media have not yet been ejected:

# vlteject -eject -report

Example 2 - Eject all media that have not yet been ejected for all sessions for the CustomerDB vault and generate corresponding reports:
RETURN VALUES

Vault may exit with a status code greater than 255. Such status codes are called extended exit status codes. For such a case, the exit status that is returned to the system is 252. The actual exit status is written to stderr in the format, EXIT status = exit status

The extended exit status values are documented in the *NetBackup Troubleshooting Guide* and in the *NetBackup Troubleshooting Wizard*.

FILES

UNIX systems:

/usr/openv/netbackup/db/vault/vault.xml
/usr/openv/netbackup/logs/vault/log.mmddyy
/usr/openv/netbackup/vault/sessions/vlt_name/sidxxx/detail.log
/usr/openv/netbackup/vault/sessions/vlt_name/sidxxx/summary.log
/usr/openv/netbackup/vault/sessions/vlt_name/sidxxx/vlteject_status
/usr/openv/netbackup/vault/sessions/vlteject.mstr
/usr/openv/netbackup/bp.conf

Windows systems:

install_path\NetBackup\db\vault\vault.xml
install_path\NetBackup\logs\bpbrmvlt\mmddyy.log
install_path\NetBackup\logs\vault\mmddyy.log
install_path\NetBackup\vault\sessions\vlt_name\sidxxx\detail.log
install_path\NetBackup\vault\sessions\vlt_name\sidxxx\summary.log
install_path\NetBackup\vault\sessions\vlt_name\sidxxx\vlteject.status
install_path\NetBackup\vault\sessions\vlteject.mstr
install_path\NetBackup\bp.conf

SEE ALSO

See *vltopmenu* on page 939.
vltinject

vltinject – inject volumes into a robot for a specified vault configuration

SYNOPSIS

vltinject profile|robot/vault/profile [-version]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

vltinject injects volumes into a robot and updates the Enterprise Media Manager Database. It runs vmupdate and assigns it the robot number, robot type, and robotic volume group from the vault configuration that matches the specified profile.

If the following directory exists and has public write access, vltinject writes to the daily debug log file:

UNIX systems: /usr/openv/netbackup/logs/vault

Windows systems: install_path\NetBackup\logs\vault

The daily debug log file is log.DDMMYY; the DDMMYY is the current date.

You then can use this file for troubleshooting. Public-write access is needed because not all executables that write to this file can run as administrator or root.

Any authorized user can run this command.

For more information about NetBackup authorization, refer to the NetBackup Security and Encryption Guide.

OPTIONS

profile|robot/vault/profile

The name of a profile or a robot number, vault, and profile that are nested within the vault configuration file. If profile is used without robot and vault, the profile must be unique. vltinject executes vmupdate with the robot number, robot type, and robotic volume group from this profile’s configuration.
Display the vltinject version and exit.

EXAMPLES

Example 1 - Inject the volumes that the Payroll profile has vaulted and that were returned from the off-site vault, enter the following:

# vltinject Payroll

Example 2 - Inject the volumes that the Weekly profile (in the Finance vault) vaulted and that the off-site vault has returned. The user enters the following:

# vltinject 8/Finance/Weekly

RETURN VALUES

0 - The EMM database was successfully updated.

Non-zero - A problem was encountered updating the EMM database.

Vault may exit with a status code greater than 255. Such status codes are called extended exit status codes. For such a case, the exit status that is returned to the system is 252. The actual exit status is written to stderr in the format, EXIT status = exit status.

FILES

UNIX systems:

/usr/openv/netbackup/logs/vault/log.mmddyy

Windows systems:

install_path\NetBackup\logs\vault\mmddyy.log
vltoffsitemedia

vltoffsitemedia – list off-site parameter values for a group of media, or change the off-site parameter value for a single media

SYNOPSIS

vltoffsitemedia -list [-W] [-vault vault_name] [-voldbhost host_name]
vltoffsitemedia -version

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/
On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

vltoffsitemedia allows the user to change the vault-specific parameters of a given media. This command lets the user change one or more parameters by using a single command. It lets the user view the various vault parameters of all media for a particular EMM server or vault.

If you create the following directory with public-write access, vltoffsitemedia creates a daily debug log in this directory:
UNIX: /usr/openv/netbackup/logs/vault
Windows: install_path\NetBackup\logs\vault

The log is called log.DDMMYY (where DDMMYY is the current date). You then can use this file that for troubleshooting.

Public-write access is needed because not all executables that write to this file can run as root.
OPTIONS

-change
Changes the attributes of the specified volume.

-d media_description
Specifies the description for the volume.

To configure NetBackup so that the media description field is cleared automatically when volumes are returned to the robot, set the VAULT_CLEAR_MEDIA_DESC parameter in EMM.

-list
Lists the off-site parameters for the media in the local EMM database. To restrict the list to a specific vault for the local EMM database, include the -vault option with the command. To list the off-site parameters for media for a specific EMM database, include the -voldbhost option with the command.

-m media_id
Media ID of the volume whose vault parameters are to be changed.

-vault vault_name
Specifies the name of the vault for which all media IDs and their vault-specific parameters are listed.

-version
Displays the vltoffsitemedia version and exit.

-vltcid container_id
Specifies the container in which a volume is stored. container_id (a string of up to 29 alphanumeric characters (no spaces) specifies the new container for the volume. You must specify an existing container ID. You cannot assign media from one EMM server to a container that has media from a different EMM server. Use the -m option to specify the media ID of the volume.

-vltname vault_name
Specifies the name of the logical vault that is configured for the robot that ejected the volume.

-vltreturn date
Specifies the date and time the media was requested for return from the vault vendor. For Catalog Backup volumes, this date is the date that the media is requested for return from the vault vendor.

The required date and time values format in NetBackup commands varies according to your locale. The /usr/openv/msg/.conf file (UNIX) and the install_path\VERITAS\msg\LC.CONF file (Windows) contain information such
as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

See the "About specifying the locale of the NetBackup installation" topic in the NetBackup Administrator's Guide, Volume II for more information.

-vltsent date

Specifies the date and time the media was sent to the off-site vault.

The required date and time values format in NetBackup commands varies according to your locale. The /usr/openv/msg/.conf file (UNIX) and the install_path\VERITAS\msg\LC.CONF file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

See the "About specifying the locale of the NetBackup installation" topic in the NetBackup Administrator's Guide, Volume II for more information.

mm/dd/yyyy [hh[:mm[:ss]]]

-vltsession session_id

Specifies the identifier of the Vault session that ejected this media.

-vltslot slot_no

Specifies the vault vendor's slot number for the slot that this volume occupies.

-voldbhost host_name

Specifies the name of the EMM server.

-W

Specifies the parsable output format for the media off-site parameters. For containers, the output includes the length of the container description, the container description, and the container ID. The output header line is a space that is separated line of column labels; the output data lines are space-separated fields.

EXAMPLES

Example 1 - Change the vault name and the vault sent dates of the media with the ID BYQ.

vltoffsitemedia -change -m BYQ -vltnname THISTLE -vltsent 08/01/2012 12:22:00

Example 2 - Change the vault slot number to 100 for a media with ID 000012.

vltoffsitemedia -change -m 000012 -vltslot 100
Example 3 - Clear out the vault-specific fields for a media.

vltoffsitemedia -change -m 000012 -vltname "" -vltsession 0 -vltslot 0 -vltsent 0 -vltreturn 0

or:

vltoffsitemedia -change -m 000012 -vltname - -vltsession 0 -vltslot 0 -vltsent 00/00/00 -vltreturn 00/00/00

Example 4 - Clear the container ID and media description of volume ABC123.

vltoffsitemedia -change -m ABC123 -vltcid - -d ""

or:

vltoffsitemedia -change -m ABC123 -vltcid "" -d ""

The vltoffsitemedia command uses the Media Manager commands to query or update the EMM database.

If the vltoffsitemedia command fails, look at the debug log on the following directory for detailed information about the actual Media Manager command that failed:

UNIX systems: /usr/openv/netbackup/logs/vault

Windows systems: install_path\netbackup\logs\vault

For more information on the status codes that Media Manager commands return, see the NetBackup Status Codes Reference Guide.

**RETURN VALUES**

Vault may exit with a status code greater than 255. Such status codes are called "extended exit status codes." For such a case, the exit status that is returned to the system is 252. The actual exit status is written to stderr in the format, EXIT status = exit status

The extended exit status values are documented in the NetBackup Status Codes Reference Guide and in the NetBackup Troubleshooter Wizard.
vltopmenu

vltopmenu – start NetBackup Vault menu interface for operators

SYNOPSIS

vltopmenu [-version]

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin\n
DESCRIPTION

Allows the user to activate a menu screen that contains the various options that an
Operator of the NetBackup Vault feature can use. It lets the user eject or inject
media, print various reports individually or collectively. It also consolidates all reports
and ejects for all sessions that have not ejected media yet. This interface can be
used from any character-based terminal (or terminal emulation window) for which
the user has a termcap or a terminfo definition.

See the NetBackup Operator’s Guide for detailed operating instructions.

Any authorized user can run this command.

For more information about NetBackup authorization, refer to the NetBackup Security
and Encryption Guide.

OPTIONS

-version

Displays the vltopmenu version and exit.

RETURN VALUES

Vault may exit with an extended exit status code (greater than 255). For such a
case, the exit status is returned to the system is 252. The actual exit status is written
to stderr in the format, EXIT status = exit status

The extended exit status values are documented in the NetBackup Troubleshooting
Guide and in the NetBackup Troubleshooting Wizard.
FILES

UNIX systems:

/usr/openv/netbackup/vault/sessions/vlteject.mstr
/usr/openv/netbackup/vault/sessions/vlteject_status.log.timestamp
/usr/openv/netbackup/vault/sessions/*/sid*/detail.log

Windows systems:

install_path\NetBackup\vault\sessions\vlteject.mstr
install_path\NetBackup\vault\sessions\vlteject_status.log.timestamp
install_path\NetBackup\vault\sessions\*\sid*\detail.log
vltrun

vltrun – Run a NetBackup Vault session

SYNOPSIS


On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\

DESCRIPTION

vltrun drives a NetBackup Vault session by issuing a sequence of calls to the vault engine. Optionally, the session can include callouts to user-provided notify scripts.

OPTIONS

profile | robot/vault/profile

Specifies the name of a profile or a nested robot number, vault, and profile in the vault parameter file. If profile is used without robot and vault, the profile must be unique within the vault parameter file. This option is required.

-vjob vault_jobid

Specifies the job ID of an active vault job that is currently duplicated.

-haltdups

Terminates all associated, active vault duplication jobs.

-preview

Generates the preview list of images to be vaulted in a vault session. The results go to the file preview.list in the session directory.

-verbose | -v

Reports verbosely on the session in the vault debug log.

-version

Displays the vltrun version and exit.
The `vltrun` session follows this sequence:

- Run the `vlt_start_notify` script.
- Inventory media.
- Initialize Media Manager database for the vault media that is returned to the robot.
- Generate the list of preview images to be vaulted.
- Duplicate images.
- Inventory Media Manager database (first time).
- Assign media for the NetBackup catalog backup.
- Inventory Media Manager database (second time).
- Inventory images.
- Suspend media.
- Run the `vlt_end_notify` script.
- Re-inventory images.
- Assign slot IDs.
- Back up the NetBackup catalog.
- Inventory the Media Manager database (third and final time).
- Run the `vlt_ejectlist_notify` script.
- Generate the eject list.
- Run the `vlt_starteject_notify` script.
- Eject and report.
- Run the `vlt_end_notify` script.

`vltrun` can be run in any of the following ways:

- Directly from the command line.
- By NetBackup policy scheduling. In this case, the policy must consist of type Vault, and the policy's file list must consist of a `vltrun` command.
- By running the command `Start Session` for a profile in the Vault interface or `vltadm`.

`vltrun` uses the option `profile|robot/vault/profile` to run a vault session. You can use the `profile` form of the option if there is no other profile with the same
name in your vault configuration. In this case, the profile name is sufficient to uniquely identify the configuration information.

If there is more than one profile with the same name, then use the robot/vault/profile form to uniquely identify the configuration.

Do not modify your vault configuration while a vault session is running.

When the session starts, it creates a directory to hold the files that vltrun and the vault engine create during the session.

The vault session uses the following directory:

UNIX systems:

/usr/openv/netbackup/vault/sessions/vault_name/sidxxx

Windows systems:

install_path\NetBackup\vault\sessions\vault_name\sidxxx

The xxx variable is an integer uniquely assigned to this session. For each vault name, session identifiers are sequentially assigned, starting with 1.

If you have configured an email address in your vault properties, then email is sent to this address at the end of the session. The email reports the results. By default, email is sent to root.

vltrun produces an overview of the session, called summary.log, in the session directory.

Control the vault process at several points in the session by installing notify scripts in the directory for NetBackup binaries, /usr/openv/netbackup/bin. Refer to the NetBackup Vault Administrator’s Guide for more information on notify scripts.

You can monitor the progress of your vltrun session in the NetBackup Activity Monitor.

The Operation field on the main Activity Monitor window shows the progress of your vault session by using the following statuses:

- Choosing Images.
- Duplicating Images.
- Choosing Media.
- Catalog Backup.
- Eject and Report.
- Done.
If you create the following directory with public-write access, `vltrun` creates a daily debug log on this directory:

UNIX systems:

usr/openv/netbackup/logs/vault

Windows systems:

`install_path\netbackup\logs\vault`

The log is called `log.DDMMYY` (where `DDMMYY` is the current date). You can then use this file for troubleshooting.

Public-write access is needed because not all executables that write to this file run as administrator or root.

You can adjust the level of logging information that is provided in this log file by adjusting the following: the vault logging level parameter on the Logging page of the master server’s properties through Host Properties on the NetBackup Administration Console.

You can terminate active vault duplication jobs by using the `vltrun -haltdups` command. Initiate a `-haltdups` script that sends a SIGUSR2 signal to the main vault job (currently at the duplication step). It then automatically propagates the signal to all of the vault duplication instances without waiting for any current duplication job instance to finish. After this step completes, the main vault job proceeds with the remaining steps.

After the SIGUSR2 signal is received, the job details of the following message of the terminated vault duplication job appears: termination requested by administrator (150).

You must have administrator privileges to run this command.

**EXAMPLES**

Example 1 - Vault the profile `my_profile`.

```
# vltrun my_profile
```

Example 2 - Vault the images for robot 0, vault Financials, and profile Weekly.

```
# vltrun 0/Financials/Weekly
```

Example 3 - Terminate an active vault duplication job with the ID of 1.

```
# vltrun -haltdups -vjob 1
```
RETURN VALUES

On UNIX systems, vault may exit with a status code greater than 255. For these extended exit status codes, the status that is returned to the system is 252. The actual exit status is written to stderr in the format: EXIT status = exit status.

FILES

UNIX systems:

/usr/openv/netbackup/vault
/usr/openv/netbackup/bp.conf
/usr/openv/netbackup/logs/bpcd/log.mmddyy
/usr/openv/netbackup/logs/vault/log.mmddyy
/usr/openv/netbackup/db/vault/vault.xml
/usr/openv/netbackup/vault/sessions/vault_name/sidxxx
/usr/openv/netbackup/vault/sessions/vault_name/sidxxx/summary.log
/usr/openv/netbackup/vault/sessions/vault_name/sidxxx/detail.log

Windows systems:

install_path\NetBackup\vault
install_path\NetBackup\bp.conf
install_path\NetBackup\logs\bpbrmvlt\mmddyy.log
install_path\NetBackup\logs\bpcd\mmddyy.log
install_path\NetBackup\logs\vault\mmddyy.log
install_path\NetBackup\db\vault\vault.xml
install_path\NetBackup\vault\sessions\vault_name\sidxxx
install_path\NetBackup\vault\sessions\vault_name\sidxxx\summary.log
install_path\NetBackup\vault\sessions\vault_name\sidxxx\detail.log

SEE ALSO

See vltadm on page 922.
See vlteject on page 929.
See vlthinject on page 933.
See vltoffsitemedia on page 935.
See vltopmenu on page 939.
vmadd

vmadd – add volumes to EMM database

SYNOPSIS


On UNIX systems, the directory path to this command is /usr/openv/volmgr/bin/

On Windows systems, the directory path to this command is install_path\Volmgr\bin\n
DESCRIPTION

Add volumes to the Enterprise Media Manager (EMM) database.

Any authorized user can run this command.

For more information about NetBackup authorization, refer to the NetBackup Security and Encryption Guide.

OPTIONS

-m media_id
	Specifies the media ID of the volume to add. The media ID can be a maximum of 6 ASCII characters. The actual character input is restricted to alpha numerics and ',', '+', '_', and '-' if they are not the first character.

The following applies only to NetBackup Enterprise Server:

-mt media_type
	Specifies the media type of the volume to add.

Valid media types for NetBackup Enterprise Server are as follows:

4mm, 8mm, 8mm2, 8mm3, dlt, dlt2, dlt3, dltf, hcart, hcart2, hcart3, qcart, 4mm_clean, 8mm_clean, 8mm2_clean, 8mm3_clean, dlt_clean, dlt2_clean, dlt3_clean, dltf_clean, hcart_clean, hcart2_clean, hcart3_clean

Valid media types for NetBackup server are as follows:
4mm, 8mm, dlt, hcart, qcart, 4mm_clean, 8mm_clean, dlt_clean, hcart_clean

-h EMM_server | volume_database_host
  This option is only applicable for NetBackup Enterprise Server.
  The name of the Enterprise Media Manager database host that contains
  information about volumes. If no host is specified, the configured EMM server
  is used by default.

-verbose
  Selects the verbose mode.

-b barcode
  Specifies the barcode that is attached to the volume.

-rt robot_type
  Specifies the robot type of the robot where the volume is located.
  Valid robot types for NetBackup Enterprise Server are as follows:
  none, acs, tld.
  Valid robot types for NetBackup server are as follows:
  none, tld.

-rn robot_number
  Unique, logical identification number for the robot where the volume is located.

-rh robot_host
  Name of the host that controls the robot, where the volume is located.

-rcl rob_slot
  Robot coordinate 1 is the slot number in the robot where the volume is located.
  The following applies only to NetBackup Enterprise Server:
  Do not enter slot information for Media Manager API robot types. The robot
  software tracks the slot locations for these robots.

-p pool_number
  Index of the volume pool that contains this volume. You can use vmpool
  -listall to determine the index for a given pool name.

-mm max_mounts
  Maximum number of mounts that are allowed for this volume. Only used for
  non-cleaning media. When this limit is exceeded, the volume can be mounted
  for read operations only.
-n cleanings
    The number of cleanings that remain for this volume. Only used for cleaning media.

-d "media_description"
    Media description of the volume. The double quote marks are required if the description contains any spaces.

EXAMPLES

Example 1 - Add volume AJU244 in the NetBackup volume pool to the EMM database on the host that is named llama. The volume has the barcode AJU244 and is in slot 2 of TLD robot 1. For write operations, the volume may be mounted a maximum of 1000 times.

The following point applies only to NetBackup server:

Only one host (the master) exists, so the -h option is not needed.

**Note:** This command is usually entered on only one line.

```
# vmadd -m AJU244 -mt dlt -h llama -b AJU244 -rt tld -rn 1 -rh llama -rc1 2 -p 1 -mm 1000 -d "vmadd example"
```

NOTES

Only limited validation of the option parameters is done.

SEE ALSO

See `vmchange` on page 949.
See `vmdelete` on page 960.
See `vmpool` on page 971.
See `vmquery` on page 974.
vmchange

vmchange – change media information in EMM database

SYNOPSIS

vmchange [-h EMM_server | volume_database_host] -vg_res -rt robot_type
    -rn robot_number -rh robot_control_host -v volume_group

vmchange [-h EMM_server | volume_database_host] -res -m media_id -mt
    media_type -rt robot_type -rn robot_number -rh robot_control_host -v
    volume_group -rc1 rob_slot

vmchange [-h EMM_server | volume_database_host] -exp date -m media_id

vmchange [-h EMM_server | volume_database_host] -barcode barcode -m
    media_id [-rt robot_type]

vmchange [-h EMM_server | volume_database_host] -m media_id -vltcid
    vault_container_id

vmchange [-h EMM_server | volume_database_host] -barcode barcode
    -vltcid vault_container_id

vmchange [-h EMM_server | volume_database_host] -d "media_description"
    -m media_id

vmchange [-h EMM_server | volume_database_host] -p pool_number -m
    media_id

vmchange [-h EMM_server | volume_database_host] -maxmounts max_mounts
    -m media_id

vmchange [-h EMM_server | volume_database_host] -clean cleanings left
    -m media_id

vmchange [-h EMM_server | volume_database_host] -n num_mounts -m
    media_id

vmchange [-h EMM_server | volume_database_host] -new_mt media_type
    -m media_id

vmchange [-h EMM_server | volume_database_host] -new_rt robot_type
    -m media_id -rn robot_number

vmchange [-h EMM_server | volume_database_host] -new_v volume_group
    [-m media_id |{-b barcode -mt media_type -rt robot_type}]]
vmchange  [-h EMM_server | volume_database_host] -vltname vault_name -m media_id
vmchange  [-h EMM_server | volume_database_host] -vltsent date -m media_id
vmchange  [-h EMM_server | volume_database_host] -vltreturn date -m media_id
vmchange  [-h EMM_server | volume_database_host] -vltslot vault_slot -m media_id
vmchange  [-h EMM_server | volume_database_host] -vltsession vault_session_id -m media_id
vmchange  -api_eject -map map_id:mapid:...:mapid | any -w [-h EMM_server | volume_database_host] -res -ml media_id:media_id:...:media_id -rt robot_type -rn robot_number -rh robot_control_host [-v volume_group]
vmchange  -multi_eject -w [-h EMM_server | volume_database_host] -res -ml media_id:media_id:...:media_id -rt robot_type -verbose -rn robot_number -rh robot_control_host
vmchange  -multi_inject -w [-h EMM_server | volume_database_host] -res -rt robot_type -verbose -rn robot_number -rh robot_control_host
vmchange  [-h EMM_server | volume_database_host] -res -robot_info -verbose -rn robot_number -rt robot_type -rh robot_control_host

On UNIX systems, the directory path to this command is /usr/openv/volmgr/bin/

On Windows systems, the directory path to this command is install_path\Volmgr\bin\n
DESCRIPTION

Change volume information in the Enterprise Media Manager database.

Any authorized user can run this command.

For more information about NetBackup authorization, refer to the NetBackup Security and Encryption Guide.
OPTIONS

-h EMM_server | volume_database_host
   This option is only applicable for NetBackup Enterprise Server.
   The name of the Enterprise Media Manager database host that contains
   information about volumes. If no host is specified, the configured EMM server
   is used by default.

-evg_res
   Change volume group residence.

-rt robot_type
   Specifies the robot type of the robot where the volume is located.
   Valid robot types for NetBackup Enterprise Server follow:
   none, acs, tld
   Valid robot types for NetBackup Server follow:
   none, tld

-rn robot_number
   Unique, logical identification number for the robot where the volume is located.

-rh robot_control_host
   Name of the host that controls the robot, where the volume is located.

-v volume_group
   A volume group is a logical grouping that identifies a set of volumes that reside
   at the same physical location.

-res
   Changes the volume's residence.

-m media_id
   Specifies the media ID of the volume to change.

-mt media_type
   Specifies the media type of the volume to change.
   Valid media types for NetBackup Enterprise Server follow:
   4mm, 8mm, 8mm2, 8mm3, dlt, dlt2, dlt3, dlf, hcart, hcart2, hcart3, qcart,
   4mm_clean, 8mm_clean, 8mm2_clean, 8mm3_clean, dlt_clean, dlt2_clean,
   dlt3_clean, dlf_clean, hcart_clean, hcart2_clean, hcart3_clean
   Valid media types for NetBackup Server follow:
   4mm, 8mm, dlt, hcart, qcart, 4mm_clean, 8mm_clean, dlt_clean, hcart_clean
-rcl rob_slot

   Robot coordinate 1 is the robot slot number where the volume is located.

   The following applies only to NetBackup Enterprise Server:

   Do not enter slot information for API robot types. The robot software tracks the
   slot locations for these robots.

-exp date

   Expiration date for this volume.

   The required date and time values format in NetBackup commands varies
   according to your locale. The /usr/openv/msg/.conf file (UNIX) and the
   install_path\VERITAS\msg\LC.CONF file (Windows) contain information such
   as the date-time formats for each supported locale. The files contain specific
   instructions on how to add or modify the list of supported locales and formats.

   See the "About specifying the locale of the NetBackup installation" topic in the

-barcode barcode

   Specifies the barcode that is attached to the volume.

-d "media_description"

   Media description for the volume. The double quote marks are required if the
   description contains any spaces.

-p pool_number

   Index of the volume pool that contains this volume. You can get the pool index
   using vmpool -listall.

-maxmounts max_mounts

   Maximum number of mounts that are allowed for this volume. Only used for
   non-cleaning media.

-n num_mounts

   For non-cleaning media, num_mounts is the number of times this volume has
   been mounted.

-clean cleanings_left

   For cleaning media, cleanings_left is the number of cleanings that remain for
   this cleaning tape.

-new_mt media_type

   Specifies the media type of the volume to change. See the -mt option for a list
   of media types.

-new_rt robot_type

   Specifies the robot type. See the -rt option for a list of robot types.
-new_v volume_group
   A volume group is a logical grouping that identifies a set of volumes that reside at the same physical location.

-b barcode
   Specifies the barcode that is attached to the volume.

-vltcid vault_container_id
   Changes the container in which a volume is stored. vault_container_id (a string of up to 29 alphanumeric characters) specifies the new container for the volume. Use the -m or -barcode option to specify the volume.

-vltname vault_name
   Specifies the name of the logical vault that is configured for the robot that ejected the volume.

-vltsent date
   Specifies the date the volume was sent off site.
   The format of date depends on the user's locale setting. For the C locale, the date syntax is as follows:
   mm/dd/yyyy [hh:mm:ss]]

-vltreturn date
   Specifies the date the volume was requested for return from the vault vendor. For catalog backup volumes, this date is the date that the volume is requested for return from the vault vendor.
   The required date and time values format in NetBackup commands varies according to your locale. The /usr/openv/msg/.conf file (UNIX) and the install_path\VERITAS\msg\LC.CONF file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.
   See the "About specifying the locale of the NetBackup installation" topic in the NetBackup Administrator's Guide, Volume II for more information.

-vltslot vault_slot
   Specifies the vault vendor's slot number for the slot that this volume occupies.

-vltsession vault_session_id
   Specifies the ID of the vault session that ejected this media.

-api_eject
   Eject ACS volumes from the specified robot. The ejection timeout period is one week.
-map map_id:mapid: ...:mapid | any
   For ACS robots, this option can specify multiple media access ports (MAPs) to use for eject operations. The map_id (also known as the CAP ID) can be all or ALL, which specifies all MAPs in the robot. Or it can be a colon-separated list of MAP IDs in the format of ACS,LSM,CAP. When the -map option is used, media are ejected to the MAPs that are specified by using a nearest MAP algorithm. The algorithm assumes that the LSMs are connected in a line.

-w
   Wait flag. This flag must be used with the eject, multiple eject, and multiple inject commands.

-verbose
   Selects the verbose mode.

-ml media_id:media_id: ...:media_id
   Specifies a list of media to be ejected from the robot.

-multi_eject
   Uses the robotic library’s media access port to eject multiple volumes. This option is only valid for TLD robot types. The ejection timeout period is 30 minutes.

-multi_inject
   Uses the robotic library’s media access port to inject multiple volumes. This option is only valid for TLD robot types. The user must run the vmupdate command after this operation to update the EMM database.

-robot_info
   Retrieves the information about a robotic library. This option is only valid for TL8 robot types
   ■ Field 1 = Number of slots
   ■ Field 2 = Number of mail slots
   ■ Field 3 = Number of drives
   ■ Field 4 = Robot type and subtype (e.g., tld -> 0)
   ■ Field 5 = Barcode reader. If a barcode reader exists on this robotic device, this field contains the following string: This robot has a barcode reader.
   ■ Field 6 = Starting slot
   ■ Field 7 = Ending slot
   ■ Field 8 = Primary inquiry string (e.g., HP~~~~~~C6240-8000~~~~~~2912)
CAUTIONS

Some robotic libraries implement different functionality for their media access ports. For example, some libraries have the front-panel inject and the eject features that conflict with NetBackup's use of the media access port. (For example, Spectra Logic Bullfrog.) Other libraries require front-panel interaction when you use the media access port (for example, Spectra Logic Gator).

The media is returned to (injected into) the robot in the following situation: you use an eject option and the media is not removed and a timeout condition occurs. If this action occurs, inventory the robot and then eject the media that was returned to the robot.

Make sure that you read the operator manual for your robotic library to gain an understanding of its media access port functionality. Libraries such as those that are noted may not be fully compatible with NetBackup inject and eject features if not properly handled. Other libraries may not be compatible at all. In addition, NetBackup performs limited validation of these option parameters.

EXAMPLES

Example 1 - Change the expiration date of volume AJS100:

```
# vmchange -exp 12/31/12 23:59:59 -m AJS100
```

Example 2 - Change the pool (which contains volume AJS999) to pool 1 (the NetBackup pool):

```
# vmchange -p 1 -m AJS999
```

Example 3 - Eject volumes abc123 and abc124 from ACS robot number 700. The residences for these two volumes are changed to standalone.

```
# vmchange -res -api_eject -w -ml abc123:abc124 -rt acs -rn 700 -rh verbena -map 0,0,0
```

Example 4 - Change the container ID of volume ABC123:

```
# vmchange -vltcid Container001 -m ABC123
```

SEE ALSO

See `vmadd` on page 946.

See `vmdelete` on page 960.

See `vmpool` on page 971.

See `vmquery` on page 974.
vmcheckxxx

vmcheckxxx – report the media contents of a robotic library

SYNOPSIS


On UNIX systems, the directory path to this command is
/usr/openv/volmgr/bin/

On Windows systems, the directory path to this command is
install_path\Volmgr\bin\n
DESCRIPTION

Report the media contents of a robotic library and optionally compare its contents with the volume configuration.

If no options are specified, the media contents of the robot and the volume configuration are listed along with a list of any mismatches detected.

Any authorized user can run this command.

For more information about NetBackup authorization, refer to the NetBackup Security and Encryption Guide.

OPTIONS

-rt robot_type
   Specifies the robot type of the robot to inventory.
   Valid robot types for NetBackup Enterprise Server follow:
   none, acs, tld.
   Valid robot types for NetBackup server follow:
   none, tld.

-rn robot_number
   Unique, logical identification number of the robot to inventory.
-rh robot_host
   Name of the host that controls the robot. If no host is specified, the host where
   you execute this command is assumed.

-h EMM_server | volume_database_host
   This option is only applicable for NetBackup Enterprise Server.
   The name of the Enterprise Media Manager database host that contains
   information about the volumes in a robot. If no host is specified, the configured
   EMM server is used by default.

-if inventory_filter_value
   This option is only applicable for NetBackup Enterprise Server.
   Specifies the inventory filter values. Multiple -if options may be specified. The
   inventory filter value is an ACS scratch pool ID.
   The -if and -full options cannot be specified together.

-full
   Specifies the full inventory. The -full and -if options cannot be specified
   together.

-list
   Lists the robot contents.

NOTES

Only limited validation of the option parameters is done.

EXAMPLES

Example: List the media contents of TLD robot 1 and the volume configuration for
that robot on the host named server2. It also lists any mismatches that are detected:

# vmcheckxxx -rt tld -rn 1 -rh server2

SEE ALSO

See vmupdate on page 982.
vmd

vmd – run EMM daemon

SYNOPSIS

vmd [-v]

The directory path to this command is /usr/openv/volmgr/bin/

DESCRIPTION

This command operates only on UNIX systems.

ltid does not require volumes to be defined in the EMM database before it is used.

The following paragraph applies only to NetBackup Enterprise Server:

The automatic mount of volumes in robotic devices does not take place until the following actions occur: the volumes are defined and their slot information (for non-API robots) is entered in the EMM database.

A direct interface to the EMM database is provided to facilitate EMM database administrative activities easily. Graphical, menu-driven, and command-line Media Manager utilities are provided.

vmd is also used for remote Media Manager device management and for managing the volume pool, barcode rules, and device databases.

The Internet service port number for vmd must be in /etc/services. If you use NIS (Network Information Service), place the entry that is in this host’s /etc/services file in the master NIS server database for services. The default service port number is 13701.

The following paragraphs apply only to NetBackup Enterprise Server.

OPTIONS

- v  Logs detailed the debug information if you create the debug/daemon directory (see ERRORS). Specify this option only if problems occur or if requested by Veritas support.

ERRORS

vmd logs an error message using syslogd if there is a copy of vmd in operation.
vmd logs an error message using syslogd if the port that it binds to is in use. If this message appears, you may need to override the services file by using the mechanism that is described under DESCRIPTION.

To run vmd in debug mode do the following:

- Before you start vmd, create the following directory:
  
  /usr/openv/volmgr/debug/daemon

  If vmd is running, stop, and restart it after creating the directory.

- Start vmd in verbose mode as follows or put a VERBOSE entry in vm.conf.

  /usr/openv/volmgr/bin/vmd -v

- Check the log message in /usr/openv/volmgr/debug/daemon.

If problems persist, you can obtain more debug information on the requestor by creating the following directory: /usr/openv/volmgr/debug/reqlib.

One log per day is created in each debug directory. These logs continue to build until the debug directory is moved or removed, unless you specify a DAYS_TO_KEEP_LOGS entry in vm.conf. Do not remove the debug directory while vmd is running. Only run vmd in debug mode when necessary.

FILES

/usr/openv/volmgr/debug/daemon/*
/usr/openv/volmgr/debug/reqlib/*

EMM database

SEE ALSO

See ltid on page 549.
See vmadd on page 946.
See vmchange on page 949.
See vmdelete on page 960.
See vmquery on page 974.
vmdelete

vmdelete – delete volumes from EMM database

SYNOPSIS

vmdelete [-h EMM_server | volume_database_host] [-m media_id | -v volume_group]

On UNIX systems, the directory path to this command is
/usr/openv/volmgr/bin/

On Windows systems, the directory path to this command is
install_path\Volmgr\bin\

DESCRIPTION

Delete volumes from the Enterprise Media Manager database.

Any authorized user can run this command.

For more information about NetBackup authorization, refer to the NetBackup Security
and Encryption Guide.

OPTIONS

-h EMM_server | volume_database_host

This option is only applicable for NetBackup Enterprise Server.

The name of the Enterprise Media Manager database host that contains
information about volumes. If no host is specified, the configured EMM server
is used by default.

-m media_id

Specifies the media ID of the volume to delete from the volume database.

-v volume_group

Specifies the volume group to delete. All volumes in this group are deleted
from the volume database.

NOTES

Only limited validation of the option parameters is done.
EXAMPLES

Example 1 - Delete a single volume:

# vmdelete -m AJS144

Example 2 - Delete all volumes with the volume group name of DELETE_ME:

# vmdelete -v DELETE_ME

SEE ALSO

See vmadd on page 946.

See vmchange on page 949.

See vmquery on page 974.
vmoprcmd

vmoprcmd – perform operator functions on drives

SYNOPSIS

vmoprcmd -devmon [pr | ds | hs] [-h device_host] default_operation
vmoprcmd -dp [pr | ds | ad] [-h device_host]
vmoprcmd -down | -up | -upopr | -reset drive_index [-h device_host]
vmoprcmd -downbyname | -upbyname | -upoprbname | -path drive_path
                [-nh ndmp_hostname] [-h device_host]
vmoprcmd -resetbyname drive_name [-h device_host]
vmoprcmd -assign drive_index mount_request_id [-h device_host]
vmoprcmd -assignbyname drive_name mount_request_id [-h device_host]
vmoprcmd -deny | -resubmit mount_request_index [-h device_host]
vmoprcmd -comment drive_index ["comment"] [-h device_host]
vmoprcmd -commentbyname drive_name ["comment"] [-h device_host]
vmoprcmd -crawlreleasebyname drive_name [-h EMM_Server]
vmoprcmd [-activate_host | -deactivate_host] [-h device_host]
vmoprcmd -hoststatus [-h device_host]

On UNIX systems, the directory path to this command is /usr/openv/volmgr/bin/

On Windows systems, the directory path to this command is install_path\Volmgr\bin\n
DESCRIPTION

This command lets you perform operator functions on drives. The -h option is not required, but you must choose only one of the following other options.

Non NDMP Windows device paths appear as {p,b,t,l}: where p is the port, b is the bus, t is the target, and l is the LUN. When vmoprcmd is run by using the -path argument, specify the path in the {p,b,t,l} format.

Any authorized user can run this command.
For more information about NetBackup authorization, refer to the NetBackup Security and Encryption Guide.

OPTIONS

-**assign** *drive_index* *mount_request_id*
  Assign a drive to a mount request.

-**assignbyname** *drive_name* *mount_request_id*
  This option is similar to the -**assign** option, except the drive name specifies the drive instead of the drive index.

  The following point applies only to NetBackup server:

  The device host is the host where Media Manager is installed.

-**comment** *drive_index* ["*comment*"]
  Add a comment for the drive. The quotes are required if your comment contains any spaces. If you do not specify *comment*, any existing comments for the drive are deleted.

-**commentbyname** *drive_name* ["*comment*"]
  This option is similar to the -**comment** option, except the drive name specified the drive instead of drive index.

-**crawlreleasebyname** *drive_name*
  This option is only applicable for NetBackup Enterprise Server.

  This option forces all hosts (that are registered to use the drive) to issue a SCSI release command to the drive. Issue this option on the host that is the SSO device allocator (DA host) or use the -h option to specify the DA host.

  **Caution:** Use this option after a PEND status has been seen in Device Monitor. Do not use this option during backups.

-**down** | -**up** | -**upopr** | -**reset** *drive_index*
  -**down** Sets the drive to the DOWN state, if it is not assigned.
  -**up** Sets the drive to the UP position in Automatic Volume Recognition (AVR) mode. This mode is the normal mode for all drives.
  -**upopr** Sets the drive to the UP position in Operator (OPR) mode. This mode is normally used only for security reasons. For a drive in a robot, OPR and AVR are treated identically while the robot daemon or process is running.
-reset Resets the specified drive. Also, it unloads the drive (if not assigned in the EMM database). You can use the unload capability to unload the media that is stuck in the drive.

-downbyname | -upbyname | -upopbyname | -resetbyname drive_name

These options are similar to -down, -up, -upopr, and -reset respectively, except the drive name specifies the drive instead of the drive index.

-deny | -resubmit mount_request_id

-deny Denying a mount request returns an error message to the user.

-resubmit Resubmit a mount request. If a pending action message involves a robot, you must correct the problem and resubmit the request that caused the message.

-dp [pr | ds | ad]

If none of the following optional display parameters are specified, all information is displayed.

pr - Displays any pending requests.

ds - Displays the status of drives under control of Media Manager.

ad - Displays additional status of drives under control of Media Manager.

-devmon [pr | ds | hs] default_operation

The -devmon command lists all of the drive paths that are configured for a given drive name. If none of the following optional display parameters are specified, all information is displayed. Full device pathnames are displayed.

pr Displays any pending requests.

ds Displays the status of drives under control of Media Manager.

hs Displays additional status of drives under control of Media Manager.

-h EMM_Server | device host

Name of the Enterprise Media Manager database host where the drives are attached and configured. If no host option is specified, the device host where you run the command is default.

The device host is the host where the device is attached and configured.

-hoststatus

Displays the current status of the host. The following states can appear:

DEACTIVATED - This state prevents any new jobs from starting on this host.

ACTIVE - The media server is available to run any jobs.

ACTIVE-DISK - The media server is available to run jobs for disk storage units only.
ACTIVE-TAPE - The media server is available to run jobs for tape storage units only.

OFFLINE - The media server is not available to run jobs for either tape storage units or disk storage units. This state occurs because the media server is not active for tape or disk, or because the master server cannot communicate with the media server.

\[-nh \texttt{ndmp\_hostname}\]

Specifies the host name of the NDMP server.

\[-activate\_host\]

Makes the host available to run jobs.

\[-deactivate\_host\]

Makes the host unavailable to run jobs.

\[-path \texttt{drivepath}\]

Specifies the system name for the drive. For example, /dev/rmt/0cbn.

\[-setpath \texttt{drivepath drive\_name ndmp\_hostname}\]

Specifies the system name and the drive name of the NDMP host.

**NOTES**

Only limited validation of the option parameters is done.

tpconfig -d, tpconfig -l, and vmoprcmd may truncate long drive names. Use tpconfig -dl to obtain the full drive name.

vmoprcmd may truncate drive names to 20 characters.

**EXAMPLES**

Example 1 - Set the drive, with a drive index of 0, to UP mode:

```
# vmoprcmd -up 0
```

Example 2 - Display the drive status of all drives:

```
# vmoprcmd -d ds
```

Example 3 - Display pending requests and the drive status of all drives on the device host named crab:

```
# vmoprcmd -h crab
```

Example 4 - Demonstrate how non-NDMP Windows device paths appear.
# vmoprcmd

## HOST STATUS

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Version</th>
<th>Host Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>hamex</td>
<td>600000</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

## PENDING REQUESTS

<NONE>

## DRIVE STATUS

<table>
<thead>
<tr>
<th>Drive Name</th>
<th>Label</th>
<th>Ready</th>
<th>RecMID</th>
<th>ExtMID</th>
<th>Wr.Enbl.</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM.ULTRIUM-TD2.001</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>hcart2</td>
<td>TLD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hamex</td>
<td></td>
<td></td>
<td>{3,1,0,2}</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>hamex</td>
<td></td>
<td></td>
<td>{3,1,1,2}</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM.ULTRIUM-TD1.004</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>hcart</td>
<td>TLD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hamex</td>
<td></td>
<td></td>
<td>{3,1,0,7}</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>hamex</td>
<td></td>
<td></td>
<td>{3,1,1,7}</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM.ULTRIUM-TD2.005</td>
<td>Yes</td>
<td>Yes</td>
<td>J945L2</td>
<td>Yes</td>
<td>hcart2</td>
<td>TLD</td>
<td></td>
</tr>
<tr>
<td>hamex</td>
<td></td>
<td></td>
<td>{3,1,2,1}</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM.ULTRIUM-TD2.006</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>hcart2</td>
<td>TLD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hamex</td>
<td></td>
<td></td>
<td>{3,1,2,2}</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

# vmoprcmd -downbyname IBM.ULTRIUM-TD1.004 -path {3,1,0,7}
vmphyinv

vmphyinv – inventory media contents of a robotic library or standalone drive and update the volume database

SYNOPSIS

\texttt{vmphyinv -rn robot\_number} \texttt{| [-rh robot\_control\_host]} \texttt{| [-h device\_host]} \texttt{| [-pn pool\_name]} \texttt{| [-v volume\_group]} \texttt{| [-rc1 robot\_coord1\_number number]} \texttt{| [-drv\_cnt count]} \texttt{| [-non\_interactive]} \texttt{| [-mount\_timeout timeout]} \texttt{| [-priority number]} \texttt{| [-verbose]}

\texttt{vmphyinv -rn robot\_number} \texttt{| [-rh robot\_control\_host]} \texttt{| [-h device\_host]} \texttt{| -ml media\_id:media\_id:...:media\_id} \texttt{| [-drv\_cnt count]} \texttt{| [-non\_interactive]} \texttt{| [-mount\_timeout timeout]} \texttt{| [-priority number]} \texttt{| [-verbose]}

\texttt{vmphyinv -rn robot\_number} \texttt{| [-rh robot\_control\_host]} \texttt{| [-h device\_host]} \texttt{| { { [-slot\_range from to]} [-slot\_list s1:s2:...:sN]} \texttt{| [-d density]} \texttt{| { { [-slot\_range from to]} [-slot\_list s1:s2:...:sN]} \texttt{| [-d density]} \texttt{| [-drv\_cnt count]} \texttt{| [-non\_interactive]} \texttt{| [-mount\_timeout timeout]} \texttt{| [-priority number]} \texttt{| [-verbose]}

\texttt{vmphyinv \{-u drive\_number | -n drive\_name\}} \texttt{| [-h device\_host]} \texttt{| [-non\_interactive]} \texttt{| [-mount\_timeout timeout]} \texttt{| [-verbose]}

On UNIX systems, the directory path to this command is \\
\texttt{/usr/openv/volmgr/bin/}

On Windows systems, the directory path to this command is \\
\texttt{install\_path\Volmgr\bin/}

DESCRIPTION

Physically inventory the media contents of a robotic library or standalone drive and update the EMM database. Based on information in the tape header, \texttt{vmphyinv} mounts each media that the search criterion specifies, reads the tape header, and updates the EMM database.

For more information about this command, refer to the \texttt{NetBackup Administrator's Guide, Volume I}.

Any authorized user can run this command.
For more information about NetBackup authorization, refer to the NetBackup Security and Encryption Guide.

OPTIONS

- **-rn robot_number**
  
  Specifies the Media Manager robot number whose media is inventoried. 
  
  *robot_number* should correspond to a robot with already configured drives. 
  
  *vmphyinv* inventories each of the media. It has the *robot_number* in the volume database of *robot_number*.

- **-rh robot_host**
  
  Specified the name of the host that controls the robot. If no host is specified, 
  the host where this command is executed is assumed.

- **-h device_host**
  
  Specifies the device host name. This option is used to obtain the Enterprise Media Manager Server name. If not specified, the current host is used to obtain the EMM server name.

- **-pn pool_name**
  
  Specifies the case-sensitive pool name of the volumes, which corresponds to the robot that the -rn option specifies, which need to be inventoried. Valid only when the -rn option is specified.

- **-priority number**
  
  Specifies a new priority for the inventory job that overrides the default job priority.

- **-v volume_group**
  
  Specifies the volume group of the volumes, that correspond to the robot that the -rn option specifies, which need to be inventoried. Valid only when the -rn option is specified.

- **-rc1 robot_coord1**
  
  Specifies the starting slot of the media that needs to be inventoried. Valid only when the -rn option is specified.

- **-number number**
  
  Specifies the number of slots that start from *robot_coord1* that need to be inventoried. Valid only when -rn and -rc1 are also specified.

- **-ml media_id1:media_id2: ... :media_id**
  
  Specifies a list of media, which need to be inventoried. Valid only when -rn option is specified. If the media ID that is specified does not belong to the specified robot, the media is skipped.
-slot_range from to
   Specifies a range of slots that need to be inventoried. If one or more slots are empty, those slots are skipped.

-slot_list s1:s2:...sN
   Specifies a list of slots that need to be inventoried. If one or more slots are empty, those slots are skipped.

-d density
   Specifies the density of the media. The user must specify the media density and inventory the media by slot range or slot list.

-u drive_number
   Specifies the drive index that needs to be inventoried. The drive must contain media and be ready. The number for the drive can be obtained from the Media and Device Management of the Administration Console.

-n drive_name
   Specifies the drive name that needs to be inventoried. The drive must contain media and be ready. The name for the drive can be obtained from the Media and Device Management of the Administration Console.

-non_interactive
   As the default, vmphyinv displays a list of recommendations and asks for confirmation before it modifies the volume database and EMM database (if required). If this option is specified, the changes are applied without any confirmation.

-mount_timeout timeout
   Specifies the mount timeout in seconds. If the media cannot be mounted within the specified time, the mount request is canceled. The default value is 15 minutes.

-drv_cnt count
   Specifies the maximum number of drives that can be used simultaneously by vmphyinv. The total number of configured drives and this value determine the actual number of drives vmphyinv uses. The number of drives that vmphyinv uses is the minimum of the specified drive count and the total number of configured drives. The default is to use all the drives.

-verbose
   Selects the verbose mode. When you specify this option, more information appears. For example, this information consists of the following: The number of available drives, what is found on each tape, and catalog identification if the media is a catalog.
EXAMPLES

Example 1 - Update the EMM database of robot 1 connected to host shark:

# vmphyinv -rn 1 -rh shark

Example 2 - Update the EMM database of robot 7 connected to host whale. Only the media that belongs to the pool name "some_pool" is inventoried:

# vmphyinv -rn 7 -rh whale -pn some_pool

Example 3 - Update the EMM database of robot 3 connected to host dolphin. Only the media A00001, A00002, A00003 is inventoried.

# vmphyinv -rn 3 -rh dolphin -ml A00001:A00002:A00003

Example 4 - Update the EMM database of robot 2 of type TLD that is connected to host phantom. It only inventories the media in slots 3 to 8.

# vmphyinv -rn 2 -rh phantom -slot_range 3 8 -d dlt

Example 5 - Update the EMM database of standalone drive (drive index 3) attached to host tigerfish:

# vmphyinv -u 0 -h tigerfish

SEE ALSO

See vmupdate on page 982.
See vmcheckxxx on page 956.
See vmoprcmd on page 962.
vmpool

vmpool – manage volume pools

SYNOPSIS

vmpool [-h EMM_server | volume_database_host] -list_all [-b|-bx] | -list_scratch | -list_catalog_backup | -create -pn pool_name -description description [-mpf mpf_max] | -update -pn pool_name [-description description] [-reason "string"] [-mpf mpf_max] | -delete pool_name | -set_scratch pool_name | -unset_scratch pool_name | -set_catalog_backup pool_name | -unset_catalog_backup pool_name

On UNIX systems, the directory path to this command is /usr/openv/volmgr/bin/

On Windows systems, the directory path to this command is install_path\Volmgr\bin\n
DESCRIPTION

Use this command to add, change, delete, or list volume pools.

The -h option is not required, but you must choose one and only one of the other seven options (for example, -list_scratch).

Any authorized user can run this command.

For more information about NetBackup authorization, refer to the NetBackup Security and Encryption Guide.

OPTIONS

-h EMM_server | volume_database_host

This option applies only to the NetBackup Enterprise Server.

Specifies the name of the Enterprise Media Manager database host that contains information about volumes. If no host is specified, the configured EMM server is used by default.

-list_all [-b | -bx]

Lists the information about all volume pools. Use the -b or -bx option to specify a brief format for volume pool information.
-list_scratch
Lists all configured scratch pools and the pool index number.

-list_catalog_backup
Lists the volume pool to be used for catalog backup.

-create -pn pool_name -description description -mpf mpf_max
Adds a new volume pool. Optionally limits the number of partially full media to be used in this pool by using -mpf. The default value is zero (0), which indicates that the number of partially full media is unlimited.

The -description option describes the volume pool. Double quote marks are required if the description contains any spaces.

-update -pn pool_name [-description description] [-mpf mpf_max]
Changes an existing volume pool. Optionally limits the number of partially full media to be used in this pool by using -mpf. The default value is zero (0), which indicates that the number of partially full media is unlimited.

The -description option describes the volume pool. Double quote marks are required if the description contains any spaces.

-delete pool_name
Deletes a volume pool.

-reason "string"
Indicates the reason why you perform this command action. The reason text string that you enter is captured and appears in the audit report. Enclose this string with double quotes ("...") and do not exceed 512 characters. The string cannot begin with a dash character (-) nor contain a single quotation mark (').

-set_scratch pool_name
If pool_name is a previously defined volume pool, pool_name becomes the scratch pool, and its description is not changed. The NetBackup, Datastore, Catalog Backup, and None volume pools cannot be changed to scratch pools.

If pool_name is a new volume pool, a new pool is created with "Scratch Pool" as the description.

Only one scratch pool at a time can be defined.

-unset_scratch pool_name
Undefines pool_name as the scratch pool and defines it as a regular volume pool. The pool can be deleted by using vmpool -delete pool_name.

-set_catalog_backup pool_name
Specifies the volume pool to back up the NetBackup catalog. You can also create a dedicated catalog backup pool to be used for catalog policies. A dedicated catalog volume pool reduces the number of needed tapes during
catalog restores since catalog backup media are not mixed with other backup media.

-unset_catalog_backup pool_name
   Defines a volume pool that you do not want to use to back up the NetBackup catalog.

NOTES

Only limited validation of the option parameters is done.

A pool cannot be both a scratch pool and Catalog Backup pool.

The -add and -change options have been deprecated. They can still be used, but do not set the mpf value.

EXAMPLES

Example 1 - Add a new pool named MyPool on the host that is named llama. It has the default host, user ID, and group ID permissions:

    vmpool -create -pn MyPool -description "description with spaces"
           -mpf 17

Example 2 - List all pools that are configured on the host where the command is executed:

    vmpool -list_all -b
**vmquery**

vmquery – query EMM database, or assign and unassign volumes

**SYNOPSIS**

```bash
vmquery [-h EMM_server | volume_database_host, ... -h EMM_server | -h volume_database_host, ... -h volume_database_host] [-vltcid vault_container_id] [-b | -w | -W | l] -a | -m media_id | -v volume_group | -rn robot_number | -rt robot_type | -mt media_type | -p pool_number | -pn pool_name | -res robot_type robot_number robot_control_host robot_coord1 robot_coord2 | -assignbyid media_id media_type pool_number stat asg_time | -deassignbyid media_id pool_number stat
```

On UNIX systems, the directory path to this command is `/usr/openv/volmgr/bin/`

On Windows systems, the directory path to this command is `install_path\Volmgr\bin\`

**DESCRIPTION**

Query the EMM database for volume information. The `-h`, `-b`, `-w`, and `-W` options are not required, but you must choose one and only one of the other (twelve) options.

The `-b` or `-W` option can be used with any of the other 11 options, but the `-b` or `-W` options cannot be specified together.

Any authorized user can run this command.

For more information about NetBackup authorization, refer to the NetBackup Security and Encryption Guide.

**OPTIONS**

- `-h EMM_Server | volume_database_host`

  This option is only applicable for NetBackup Enterprise Server.

  The name of the Enterprise Media Manager database host that contains information about volumes. If no host is specified, the configured EMM server is used by default.
-b
  Specifies the brief output format for volume information. This option can be
  used with any of the other 11 options.

-w
  Specifies the wide output format for volume information. This option includes
  any additional information that the -b option does not show and can be used
  with any of the other 11 options.

-a
  Shows all volumes.

-m media_id
  Queries the volumes by media ID. The media ID is a maximum of 6 ASCII
  characters.

-v volume_group
  Queries the volumes by volume group. A volume group is a logical grouping
  that identifies a set of volumes that reside at the same physical location.

-rn robot_number
  Queries the volumes by robot number. A robot number is a unique, logical
  identification number for the robot where the volume is located.

-rt robot_type
  Queries the volumes by the type of robot where the volume is located.
  Valid robot types for NetBackup Enterprise Server follow:
  none, acs, tld.
  Valid robot types for NetBackup Server follow:
  none, tld.

-mt media_type
  Queries the volumes by media type.
  Valid media types for NetBackup Enterprise Server follow:
  4mm, 8mm, 8mm2, 8mm3, dlt, dlt2, dlt3, dtf, hcart, hcart2, hcart3, qcart,
  4mm_clean, 8mm_clean, 8mm2_clean, 8mm3_clean, dlt_clean, dlt2_clean,
  dlt3_clean, dtf_clean, hcart_clean, hcart2_clean, hcart3_clean.

  Valid media types for NetBackup Server follow:
  4mm, 8mm, dlt, hcart, qcart, 4mm_clean, 8mm_clean, dlt_clean, hcart_clean.
-p pool_number
Queries the volumes by pool number. Pool number is an index into the volume pool. You can use vmpool -listall to determine the index for a given pool name.

-pn pool_name
Queries the volumes by pool name.

-res robot_type robot_number robot_host rob_slot
Queries the volumes by residence.

robot_host
Specifies the host that controls the robot where the volume is located.

rob_slot
Specifies the slot number in the robot (robot coordinate 1) where the volume resides.

-assignbyid media_id media_type pool_number stat asg_time
Assigns the volume by media ID, pool, and status. This option can only assign non-NetBackup media. Non-NetBackup media include the media that the following use: Veritas Storage Migrator, Veritas Data Lifecycle Manager, or by the users that work outside of the NetBackup policy framework (for example, those using tpreq directly).

The -assignbyid option cannot be used with media of status (stat) 0 (regular NetBackup tapes) or 1 (NetBackup catalog tapes).

stat
Status applies only to volumes that are assigned to NetBackup or Storage Migrator. Possible stat values are:

0 - the volume is assigned to NetBackup regular backups.
1 - Volume is assigned to NetBackup catalog backups.
2 - Volume is assigned to Storage Migrator.

asg_time
This option applies only to volumes that are assigned to NetBackup or Storage Migrator.

Specifies the time when the volume was assigned. It is the number of seconds since 00:00:00 UTC, January 1, 1970. asg_time was originally created by using the time() call.

-deassignbyid media_id pool_number stat
Unassigns the volume by media ID, pool, and status. This option can only deassign non-NetBackup media. Non-NetBackup media includes the media
that the following use: Veritas Storage Migrator, Veritas Data Lifecycle Manager, or the users that work outside of the NetBackup policy framework (for example, those using tpreq directly). To deassign NetBackup tapes, use the bpexpdate command.

The -deassignbyid option cannot be used with media of status (stat) 0 (regular NetBackup tapes) or 1 (NetBackup catalog tapes).

-vltcid vault_container_id
Lists the volumes that are stored in the container. The vault_container_id variable can be a string of up to 29 alphanumeric characters.

-W
Specifies the parsable output format for volume information.

The output data lines are space separated fields except in the following conditions:

■ The MediaID field is padded to six characters by adding spaces to the end of the string.

■ The MediaType field is padded to eight characters by adding spaces to the end of the string.

■ The MediaDescription field may contain spaces within the field.

■ For Vault containers, the output includes the length of the container description (DescriptionLength), the container description, and the container ID. The output header line is a space-separated line of column labels.

NOTES

Only limited validation of the option parameters is done.

EXAMPLES

Example 1 - List all volume information, in brief format from the EMM database on the host that is named llama:

```bash
# vmquery -h llama -b -a
```

Example 2 - Assign volume A23456, which is in pool 1 (NetBackup). It sets the status to 0 and the assign time to 12/31/98 15:50:22:

```bash
# vmquery -assignbyid A23456 8mm 1 0 915141022
```

Example 3 - Unassign volume A23456, which is in pool 2 (Storage Migrator), with a status of 0:

```bash
# vmquery -deassignbyid A23456
```
# vmquery -deassignbyid A23456 0

SEE ALSO

See `vmadd` on page 946.
See `vmchange` on page 949.
See `vmdelete` on page 960.
See `vmpool` on page 971.
vmrule

vmrule – manage barcode rules

SYNOPSIS

```bash
vmrule [-h EMM_server | volume_database_host] -listall [-b] | -add barcode_tag media_type pool_name max_mounts "description" | -change barcode_tag media_type pool_name max_mounts "description" | -delete barcode_tag
```

On UNIX systems, the directory path to this command is /usr/openv/volmgr/bin/

On Windows systems, the directory path to this command is install_path\Volmgr\bin\n
DESCRIPTION

Use `vmrule` to add, change, delete, or list barcode rules. The `-h` option is not required, but you must choose one and only one of the other four options.

Any authorized user can run this command.

For more information about NetBackup authorization, refer to the NetBackup Security and Encryption Guide.

OPTIONS

- **-h EMM_server | volume_database_host**
  
  This option is only applicable for NetBackup Enterprise Server.
  
  The name of the Enterprise Media Manager database host that contains information about the volumes in a robot. If no host is specified, the configured EMM server is used by default.

- **-listall [-b]**
  
  Lists the information about all barcode rules. You can use the `-b` option to specify a brief format for the barcode rule information that is displayed.
  
  The following describes the fields that are included in the output of a `vmrule -list_all [-b]` command:
  
  - Field 1 = Barcode tag of the media
Field 2 = Media type
Field 3 = Volume pool for the media
Field 4 = max mounts / cleanings. The maximum mounts or cleanings for the media.
Field 5 = Rule description

-add barcode_tag media_type pool_name max_mounts "description"
   Adds a new barcode rule.

-change barcode_tag media_type pool_name max_mounts "description"
   Changes a barcode rule.

-delete barcode_tag
   Deletes a barcode rule.

barcode_tag
   Specifies the barcode prefix that activates the barcode rule.

media_type
   Specifies the media type of the volume, a barcode rule attribute. This option affects whether the rule is used. It also affects the media type for the volumes that are added by using a robot inventory update.

Valid media types for NetBackup Enterprise Server follow:
4mm, 8mm, 8mm2, 8mm3, dlt, dlt2, dlt3, dtf, hcart, hcart2, hcart3, qcart, 4mm_clean, 8mm_clean, 8mm2_clean, 8mm3_clean, dlt_clean, dlt2_clean, dlt3_clean, dtf_clean, hcart_clean, hcart2_clean, hcart3_clean.

Valid media types for NetBackup Server follow:
4mm, 8mm, dlt, hcart, qcart, 4mm_clean, 8mm_clean, dlt_clean, hcart_clean.

pool_name
   Specifies the pool to which the volumes are added.

max_mounts
   Specifies the maximum number of mounts that are allowed for this volume (when the volume is added). This option is used only for non-cleaning media. When this limit is exceeded, the volume can only be mounted for read operations.

Note: Numbers larger than 99999 are stored in the database, but vmrule displays the max_mounts as 0 if the value is larger than 99999. A value of zero means that the number of mounts is unlimited.
"description"

Description of the barcode rule. The double quote marks are required if the
description contains any spaces.

NOTES

Only limited validation of the option parameters is done.

EXAMPLES

Example 1 - Create a rule that defines any tape with a barcode that starts with ABC is a DLT tape in the NetBackup pool. The tape can be mounted up to 100 times for writes and is given a description.

vmrule -add ABC dlt NetBackup 100 "DLT cleaning tape"

Example 2 - List all barcode rule information.

# vmrule -list_all [-b]
ABC,DLT,NetBackup,100,DataStore DLT Rule
EFG,DLT,DataStore,0,DataStore DLT Rule

The barcode tags are ABC and EFG. The media type is DLT. The volume pools are NetBackup and DataStore. The max mounts or cleanings are 100 and 0. The rule description is DataStore DLT rule.

SEE ALSO

See vmupdate on page 982.
vmupdate

vmupdate – inventory media contents of a robotic library and update the EMM database

SYNOPSIS


On UNIX systems, the directory path to this command is /usr/openv/volmgr/bin/

On Windows systems, the directory path to this command is install_path\Volmgr\bin\n
DESCRIPTION

Inventory the media contents of a robotic library and update the Enterprise Media Manager database. If no options are specified, the volume configuration is updated to match the robot contents.

Any authorized user can run this command.

For more information about NetBackup authorization, refer to the NetBackup Security and Encryption Guide.

OPTIONS

- empty_map
  Specifies that volumes in the media access port (map) are moved into the robot before the robot inventory is started. This option is only valid for TLD robot types.

- full
  Specifies full the inventory. The -full and -if options cannot be specified together.
-h EMM_server | volume_database_host
   This option is only applicable for NetBackup Enterprise Server.
   The name of the Enterprise Media Manager database host that contains
   information about the volumes in a robot. If no host is specified, the configured
   EMM server is used by default.

-if inventory_filter_value
   This option is only applicable for NetBackup Enterprise Server.
   Specifies the inventory filter values. Multiple -if options may be specified. The
   inventory filter value is an ACS scratch pool ID.
   The -if and -full options cannot be specified together.

-interactive
   Prompts you before it updates the volume configuration.

-involgrp volume_group
   Specifies the volume group for the media that is moved into the robot.

-mp media_id_prefix
   Specifies the prefix that is used as a seed to generate new media IDs for media
   with no bar codes. This prefix should be between 1 and 5 characters in length
   and contain only valid media ID characters (alpha-num, "+", ",", and ":" if
   it is not the first character).

-mt media_type
   Specifies the media type of the volume.
   Valid media types for NetBackup Enterprise Server follow:
   4mm, 8mm, 8mm2, 8mm3, dlt, dlt2, dlt3, dltf, hcart, hcart2, hcart3, qcart,
   4mm_clean, 8mm_clean, 8mm2_clean, 8mm3_clean, dlt_clean, dlt2_clean,
   dlt3_clean, dltf_clean, hcart_clean, hcart2_clean, hcart3_clean.
   Valid media types for NetBackup server follow:
   4mm, 8mm, dlt, hcart, qcart, 4mm_clean, 8mm_clean, dlt_clean, hcart_clean.

-outvolgrp volume_group
   Specifies the volume group for the media that is moved out of the robot.

-p pool_name
   Specifies the name of the volume pool to which new media are assigned.

-recommend
   Lists the changes that are required to update the volume configuration.
-rh robot_host
   Name of the host that controls the robot. If no host is specified, the host where
   you execute this command is assumed.

-rn robot_number
   Unique, logical identification number for the robot to inventory.

-rt robot_type
   Specifies the robot type of the robot to inventory.
   Valid robot types for NetBackup Enterprise Server follow:
   none, acs, tld.
   Valid robot types for NetBackup server follow:
   none, tld.

-use_barcode_rules
   Specifies that barcode rules are used for assigning attributes to new media.

-use_seed
   Specifies the automatic generation of media IDs for media with no barcodes.

NOTES

Only limited validation of the option parameters is done.

EXAMPLES

Example 1 - Update the volume configuration on the EMM server named mymaster
   to match the contents of TLD robot 7 connected to the host macris:

   # vmupdate -rt tld -rn 7 -rh macris -h mymaster

SEE ALSO

See vmcheckxxx on page 956.
vnetd

vnetd – The NetBackup communication daemon

SYNOPSIS

vnetd -standalone | -terminate

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\

DESCRIPTION

vnetd is the NetBackup network communications service (daemon) used to create firewall-friendly socket connections. It allows all socket communication to take place while it connects to a single port. Start vnetd as a continuously running service (daemon). Note that inetd no longer launches vnetd.

When you install NetBackup on a client, the installation process typically adds entries for vnetd to the following:

- UNIX client: /etc/services
- Windows client: %SystemRoot%\system32\drivers\etc\services

OPTIONS

The following options are available for vnetd:

-standalone

  Instructs vnetd to run continuously. -standalone is the default condition for NetBackup startup.

-terminate

  Stop the running vnetd service.

SEE ALSO

See bpcd on page 73.
vssat

vssat – configure authentication service (AT) and its options.

SYNOPSIS

vssat addldapdomain -d DomainName -s server_URL -u user_base_DN -g group_base_DN -m admin_user_DN [-w admin_user_password] [-f trusted_CA_file_name] [-t rfc2307 | msad | {-c user_object_class -a user_attribute -q user_GID_attribute -un user_display_name_attribute -ui user_ID_attribute -ud user_description_attribute -x group_object_class -y group_attribute -z group_GID_attribute -gn group_display_name_attribute -gi group_ID_attribute -gd group_description_attribute [-k DN | UID]}]

vssat listldapdomains

vssat removeldapdomain -d DomainName

vssat validategroup --groupname name --domain type:name --broker host:1556:nbatd

vssat validateprpl --prplname prpl_name --domain type:name --broker host:1556:nbatd

On UNIX systems, the directory path to this command is /usr/openv/netbackup/sec/at/bin

On Windows systems, the directory path to this command is install_path\NetBackup\sec\at\bin

DESCRIPTION

Use the vssat addldapdomain command to add an LDAP domain to the authentication broker. You must have administrator privileges to run the vssat command. You must determine the information that is shown to add an LDAP domain:

- The type of LDAP directory in use.
  The type of LDAP directory dictates the type of scheme to use. Some of the possible types of LDAP directory types are: Microsoft Active Directory, OpenLDAP, iPlanet, and so on.
- The URL to the LDAP directory.
For example, ldap:// my_ldap_host.mydomain.myenterprise.com:389 or ldaps:// my_ssl_ldap_host.mydomain.myenterprise.com. Be aware that an LDAP URL must start with ldap:// for non-SSL, or ldaps:// for SSL-enabled LDAP directory.

■ The distinguished name (DN) of the users container.
  Normally, the users container is in one of the naming contexts. For most LDAP directories, you can use the ldapsearch utility, provided by the directory vendor, to find out the naming contexts. For example:
  
  ```
  ldapsearch --group_object_class -h my_host --server_url base --auth_type "" namingContexts
  ```
  
  For Microsoft Active Directory, the users container resembles this example:
  
  ```
  cn=users,dc=domain_name,dc=enterprise_name,dc=com
  ```

■ The distinguished name (DN) of the groups container.
  Normally, the groups container is in one of the naming contexts. For most LDAP directories, you can use the ldapsearch utility, provided by the directory vendor, to find out the naming contexts. For example:
  
  ```
  ldapsearch --group_object_class -h my_host --server_url base --auth_type "" namingContexts
  ```
  
  For Microsoft Active Directory, the groups container looks like this example:
  
  ```
  cn=users,dc=domain_name,dc=enterprise_name,dc=com
  ```

■ The schema to facilitate users and groups.
  If the enterprise has migrated their NIS data to the LDAP directory according to Request For Comments 2307, it must use the RFC 2307 schema. RFC 2307 uses the posixAccount object class to facilitate user objects. It uses the posixGroup object class to facilitate group objects. If the enterprise uses Microsoft Active Directory, it must use the Microsoft Active Directory schema. In this schema, the user object class facilitates both user objects and group objects.
  
  If the enterprise uses neither RFC 2307 nor Microsoft Active Directory, you must determine the items shown:

  ■ The LDAP object class to facilitate user objects.

  ■ The LDAP object class to facilitate group objects.

  ■ The user attribute in the user object class to facilitate user name or ID.

  Veritas uses the rules that are shown to construct the DN to the user entry: user_attribute=user_name, user_container_DN. For example, if the user attribute is configured to cn and users container DN is configured to dc=mydomain, dc=myenterprise, dc=com and the user name for the
authenticate call is jdoe, the LDAP DN for jdoe is:
cn=jdoe,dc=mydomain,dc=myenterprise,dc=com

- The group identifier (GID) attribute in the user object class to identify the
groups to which the given user belongs.

- The group attribute in the group object class to facilitate group name.
Veritas uses the rules that are shown to construct the DN to the group entry:
group_attribute=group_name,group_container_DN For example, if the group
attribute is configured to cn and groups container DN is configured to
dc=mydomain,dc=myenterprise, dc=com and the group name is adm, the LDAP
DN for adm is: cn=adm,dc=mydomain,dc=myenterprise,dc=com.

- The group ID attribute in the group object class to facilitate group ID for the
given group.

You are not required to restart the broker after you add the LDAP domain.

Use the vssat listldapdomains command to list all the LDAP domains in the
authentication broker. This command needs no additional parameters. An example
of this command is shown in the examples section.

Use the vssat removeldapdomain to remove an LDAP domain from the
authentication broker.

Use the vssat validategroup command to check the existence of a user group
in domain provided.

Use the vssat validateprpl command to check the existence of a user in domain
provided.

Note: You can only run the vssat command on the active node of a cluster.

OPTIONS

-a, --user_attribute user_attribute

Specify the user attribute within the user object class using the syntax that is
shown: user_attribute=prplname,user_base_DN. The LDAP DN for jdoe is:
cn=jdoe,dc=mydomain,dc=myenterprise,dc=com where:

- The user_attribute is cn.
- The prplname is jdoe.
- The user_base_DN is dc=mydomain,dc=myenterprise,dc=com.

Do not use this option if you use the -t option.
--broker host:1556:nbtd
   The host and the port of the broker.

-c, --user_object_class user_object_class
   Specify the LDAP object class of the user object, which is posixAccount. If
   schema_type is defined, user_object_class should not be used. If
   schema_type is not defined, user_object_class should be used.

-d, --domain DomainName
   A symbolic name that uniquely identifies an LDAP domain.

--domain type:name
   The name of the domain that holds the group or the principal that you want to
   validate. Use the domain type ldap wherever required.

-f, --server_trusted_ca_file trusted_CA_file_name
   The complete path to the file that contains the trusted CA certificates in PEM
   format. You must use this parameter when the LDAP server URL starts with
   ldaps:// and the certificate authority that signed the LDAP server security
   certificate is other than the following:
   - CyberTrust
   - digicert
   - GeoTrust
   - Certification Services Division
   - VeriSign Trust Network
   - RSA Security Inc.
   - GlobalSign
   - Symantec Corporation

-g, --group_base_dn group_base_DN
   The LDAP-distinguished name for the group container. For example,
   ou=group,dc=mydomain,dc=myenterprise,dc=com.

-gd, --group_description_attr group_description_attribute
   Attribute name that defines the group’s description in directory service.

-gi, --group_id_attr group_ID_attribute
   Attribute name that defines the group’s unique identifier in directory service.

-gn, --group_dispname_attr group_display_name_attribute
   Attribute name that defines the group’s display name in directory service.
--groupname name
The name of the group that you want to validate.

-k, --group_gid_attribute_type DN | UID
Specify the storage type of group GID attribute.

-m, --admin_user admin_user_DN
This option is a string that contains the DN of the administrative user or any user that has search permission to the user container, or user subtree as specified by UserBaseDN. If the user container is searchable by anyone including an anonymous user, you can configure this option as an empty string. For example, --admin_user=. This configuration allows anyone to search the user container.

--prplname prpl_name
The name of the principal that you want to validate.

-q, --user_gid_attribute user_GID_attribute
Specify the attribute within the user object class to retrieve the groups the user belongs to. Do not use this option if you use the -t option.

-s, -server_url server_URL
The URL of the LDAP directory server for the given domain. The LDAP server URL must start with either ldap:// or ldaps://. Starting with ldaps:// indicates that the given LDAP server requires SSL connection. For example ldaps://my-server.myorg.com:636.

-t, --schema_type schema_type
Specify which type of LDAP schema to use. If you use the -t option, you must omit the following options: -a, -i, and -o. These values are set automatically based upon the schema type chosen. If you do not use -t, neither the rfc2307 nor the msad parameters are set automatically. You must provide the values yourself. Two default schema types are supported:

- rfc2307: The schema that is specified in RFC 2307. With RFC2307, use the schema that is shown:
  - User Object Class: posixAccount
  - User Search Attribute: uid
  - User unique ID attribute: uidNumber
  - User display name attribute: cn
  - User description attribute: description
  - User GID Attribute: gidNumber
- Group Object Class: posixGroup
- Group Search Attribute: cn
- Group unique ID attribute: gidNumber
- Group display name attribute: cn
- Group description attribute: description
- Group GID Attribute: memberUid

- msad: Microsoft Active Directory schema. With Microsoft Active Directory, use the schema that is shown:
  - User Object Class: user
  - User Search Attribute: sAMAccountName
  - User unique ID attribute: objectSid
  - User display name attribute: displayName
  - User description attribute: description
  - User GID Attribute: memberOf
  - Group Object Class: group
  - Group Search Attribute: sAMAccountName
  - Group unique ID attribute: objectSid
  - Group display name attribute: displayName
  - Group description attribute: description
  - Group GID Attribute: cn

-u, --user_base_dn  user_base_DN
   The LDAP-distinguished name for the user container. For example, ou=user,dc=mydomain,dc=myenterprise,dc=com.

-ud, --user_description_attr user_description_attribute
   Attribute name that defines the user’s description in directory service.

-ui, --user_id_attr user_ID_attribute
   Attribute name that defines the user’s unique identifier in directory service.

-un, --user_dispname_attr user_display_name_attribute
   Attribute name that defines the user’s display name in directory service.

-w, --admin_user_password admin_user_password
   This attribute is a string that contains the bind password of the user that is specified in the -m option. If -m is an empty string, this option must also be an
empty string. For example, --admin_user_password=. The password is passed in plain text but it is stored in encrypted form. If you have not provided the password for the -w option, NetBackup prompts for the password.

-x, --group_object_class group_object_class
Specify the LDAP object class for the group object which is posixGroup. Do not use this option if you use the -t option.

-y, --group_attribute group_attribute
Specify the group attribute within the group object class, using the syntax that is shown: group_attribute=group_base_DN. For example, the LDAP DN for adm is cn=adm,dc=mydomain,dc=myenterprise,dc=com where:

- The group_attribute is cn.
- The group is adm.
- The group_base_DN is dc=mydomain,dc=myenterprise,dc=com.

Do not use this option if you use the -t option.

-z, --group_gid_attribute group_GID_attribute
Specify the attribute within the group object class to retrieve the group. Do not use this option if you use the -t option.

EXAMPLES

Example 1: Use of the vssat command to list the LDAP domains in the authentication broker.

vssat listldapdomains

Listldapdomains
----------------------
----------------------
Found: 1
Domain Name: VSS
Server URL: ldap://your_ldap_server.com
SSL Enabled: No
User Base DN: distinguish name of your user container
User Object Class: posixAccount
User Attribute: uid
User GID Attribute: gidNumber
Group Base DN: distinguish name of your group container
Group Object Class: posixGroup
Group Attribute: cn
Group GID Attribute: gidNumber
Example 2: Stores the AT configuration parameters in a configuration file.

vssat addldapdomain --domainname MYADDOMAIN --server_url ldap://
my_ad_host.mydomain.myenterprise.com --user_base_dn cn=users,dc=mydomain,
dc=myenterprise,dc=com --group_base_dn dc=users,dc=mydomain,dc=myenterprise,
dc=com --schema_type msad --admin_user cn=Administrator,cn=users,dc=
mydomain,dc=myenterprise,dc=com
vwcp_manage

vwcp_manage – install or uninstall the NetBackup plug-in for VMware vSphere Web Client

SYNOPSIS

vwcp_manage [--register -v vCenter_server -u vCenter_username -p passfile [-o port]] [-l url] [--acceptVCenterCertificates | -t thumbprints]

vwcp_manage [--upgrade -v vCenter_server -u vCenter_username -p passfile [-o port]] [-l url] [--acceptVCenterCertificates | -t thumbprints]

vwcp_manage [--validate -v vCenter_server -u vCenter_username -p passfile [-o port]] [--acceptVCenterCertificates | -t thumbprints]

vwcp_manage [--unregister -v vCenter_server -u vCenter_username -p passfile [-o port]] [--acceptVCenterCertificates | -t thumbprints]

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/goodies/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\goodies\

DESCRIPTION

Use the vwcp_manage command to install or uninstall the NetBackup plug-in for VMware vSphere Web Client.

Note: On a NetBackup 8.1 or later master server, you can enter vwcp_manage without options to launch the plug-in installation screens. On the NetBackup appliance, you must log on to the appliance as a NetBackupCLI user. Then you enter vwcp_manage with its options, to specify the action, vCenter server, and so forth (see OPTIONS).

For further information on installing the plug-in, see the NetBackup Plug-in for VMware vSphere Web Client Guide.
OPTIONS

--acceptVCenterCertificates
Use this option if you want to accept all the certificates that NetBackup receives from the vCenter server.

If you have enabled the VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED configuration option and have specified either --acceptVCenterCertificates or --thumbprints option, the vCenter server certificate validation takes place using the command-line interface.

If you have enabled the VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED configuration option, but have not specified either --acceptVCenterCertificates or --thumbprints option, the NetBackup plug-in for vSphere Client console is launched. You can use this console for vCenter server certificate validation.

-h, --help
Displays the help message.

-l url --url=url
The URL for the netbackup-vwc-plugin.zip file on the plug-in package host (web server).
This option is only required to install the plug-in from a custom location, such as from a NetBackup media server and a separate plug-in package host.

-o port --port=port
The vCenter port. The default is 443.

-p passfile passfile=passfile
The passfile is the path to a text file that contains only the vCenter password.
The password file should not have world readable or writable permissions. After the operation is completed, for security reasons you should delete the password file.

--register
Registers and installs the plug-in.

-t thumbprint --thumbprints=thumbprint
If the specified thumbprint matches the vCenter server certificate thumbprint, the associated certificate is used for host communication.
If you have enabled the `VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED` configuration option and have used either `--acceptVCenterCertificates` or `--thumbprints` option, the vCenter server certificate validation takes place using the command-line interface.

If you have enabled the `VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED` configuration option, but have not specified `--acceptVCenterCertificates` and `--thumbprints` options, the NetBackup plug-in for vSphere Client console is launched. You can use this console for vCenter server certificate validation.

- `-u username, --username=username`
  The vCenter user name.

- `--unregister`
  Unregisters and uninstalls the plug-in.

- `--upgrade`
  Use this option to upgrade the plug-in.

- `-v vCenter_server, --vcenter=vCenter_server`
  The vCenter server where the plug-in is to be installed.

- `--validate`
  Verifies the connection to the vCenter server and validates the vCenter credentials.

**EXAMPLES**

Example 1: Install the NetBackup vSphere Web Client plug-in on a vCenter server.

```
vwcp_manage --register -v vcenter.example.com -u admin_01 -p /home/nbusers/passfile.txt
```

Example 2: Uninstall the NetBackup vSphere Web Client plug-in from a vCenter server.

```
vwcp_manage --unregister -v vcenter.example.com -u admin_01 -p /home/nbusers/passfile.txt
```
**vxlogcfg**

vxlogcfg – modify unified logging configuration settings

**SYNOPSIS**

```
vxlogcfg -a -p ProductID -c ConfigPath -n Names [-q]
vxlogcfg -a -p ProductID -o OriginatorID -s keyname=value [-q]
vxlogcfg -a -p ProductID -g LogSet -s keyname=value [-q]
vxlogcfg -d -p ProductID
vxlogcfg -l [-p ProductID [-o OriginatorID]] [-q]
vxlogcfg -l [-p ProductID [-g LogSet]] [-q]
vxlogcfg -r -p ProductID [-o OriginatorID] [-s keyname] [-q]
vxlogcfg -r -p ProductID [-g LogSet] [-s keyname] [-q]
vxlogcfg -v
```

On UNIX systems, the directory path to this command is
/usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is
install_path\NetBackup\bin

**DESCRIPTION**

Use the `vxlogcfg` command to change the logging settings for NetBackup unified logging. It registers and unregisters the product log configurations during installation and uninstallation.

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

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

For more information about the unified logging naming format, and the logging originator IDs, refer to the NetBackup Logging Reference Guide.
OPTIONS

Specify the product log configuration to register or unregister. Use fully-qualified path names for all directory paths. If a directory name contains spaces, use quotes around the path name for that directory (for example, "the Program Files" directory).

-a, --add
Registers or creates the product log configuration settings. Any existing log settings are overwritten. Do not use this option to add a product to the list of those that use unified logging. Instead, use it only to modify existing unified logging settings. See examples.

-c, --config ConfigPath
Provides the absolute path from which the product log configuration settings should be read.

On UNIX systems, use the absolute path to the product log configuration file (for example, /opt/vrts/ProductA/log.conf.)

On Windows systems, use the path to the product log registry settings (for example, \\SOFTWARE\VERITAS\PRODUCTA\)

-d, --delete
Unregisters and removes the product log configuration settings from the main logging configuration file, if there are no originator IDs configured for the product. The corresponding product log configuration file is also deleted.

-g, --logset LogSet
Creates or modifies log configuration settings for the specified LogSet. LogSet is supplied as the text string "Default" or the text string "ALL." If the LogSet is "Default," then the -s configuration settings are the default settings. If the LogSet is "ALL," then the -s configuration settings are given to all the originators of a given product ID.

-l, --list
Lists one of the following:

- All of the configured products.
- All of the originator IDs and LogSet
- All of the configuration settings that are defined for a product ID and originator ID pair, or a product ID and LogSet

-n, --names Name
Specifies abbreviated or short names for the product. Separate multiple names with a comma.
-o, --orgid OrgID
    Creates or modifies log configuration settings for the specified originator ID. The Originator ID can be supplied as a valid originator ID (a number), or, the text string "Default," or the text string "ALL." If the Originator ID is "Default," then the -s configuration settings are the default settings. If the Originator ID is "ALL," then the -s configuration settings are given to all the originators of a given product ID.

-p, --prodid ProductID
    Creates or modifies the log configuration settings for a productID.

-q, --quiet
    Prevents the display of error or informational messages (Quiet Mode).

-r, --remove
    Unregisters and removes the log configuration settings for the specified OID and product from the product logging configuration file. Individual settings can be removed with the "-s, --setting keyname=value" option.

---

**Caution:** Always use the -r option with the -o option. Otherwise, all of the existing NetBackup log settings are removed and no further logging is performed for all of NetBackup.

-s, --setting keyname=value
    Sets the individual configuration settings when used with -a (add option). keyname is the configuration setting’s name and value is the value for that setting. You can use multiple -s keyname=value arguments on the command line.

-s, --setting keyname
    Removes a configuration setting when it is used with the -r option. Use only one keyname with the -r option. To remove multiple settings, provide multiple -s options. See the Keynames and Values section for particular keynames.

-v, --version
    Displays the version information for this command.

---

**KEYNAMES AND VALUES**

Following are the keynames and values that can be specified on the -s option. For NetBackup, the vxlogcfg command places these keynames and values in the /usr/openv/netbackup/nblog.conf file on UNIX and in install_path\NetBackup\nblog.conf on Windows. For PBX, these are placed
in /etc/vx/VxICS/icsul.conf on UNIX and in the registry entry
SOFTWARE\Veritas\VxICS\logcfg on Windows.

Keynames and the values for UNIX and Windows

**LogDirectory**

Provides an absolute path or relative path to a directory. No default value. If
you specify a relative path for an originator ID, the path is relative to the product
ID log directory that is specified by Default.LogDirectory in the log configuration
file.

---

**Caution:** When you use the LogDirectory keyname to redirect unified logs
to an alternate directory, stop and restart the NetBackup services. This action
makes redirection take effect.

---

**DebugLevel**

Sets the verbosity level for the debug log messages. (Debug logs are intended
for Veritas engineers.) Valid values are 0 through 6.

**DiagnosticLevel**

Sets the verbosity level for the diagnostic log messages. (Diagnostic logs are
intended for NetBackup administrators and users.) Valid values are 0 through
6. Zero (0) means no debug messages.

**DynaReloadInSec**

Dynamically reloads debug and diagnostic settings. Integers 0-60 reload after
60 seconds. Integers greater than 60 reload at the specified number of seconds.

**LogToStdout**

Sends all log messages to standard output (by default the terminal) and to the
log file. Valid values are true and false (default value).

**LogToStderr**

Sends the application log messages to Stderr (by default the terminal) and
to the log file. Valid values are true and false (default value).

**LogToOslog**

Sends the application log messages to the operating system log (syslog on
UNIX and the event logs on Windows). Valid values are true and false (default
value).

**RolloverMode**

Specifies when log files are rolled over. If you roll over a log file, it closes the
current log file and opens a new one. The purpose is to keep log file size low
and allow older log files to be deleted or archived. Valid values are FileSize,
LocalTime, Periodic, FileSize | LocalTime, FileSize | Periodic and None.
FileSize indicates that the rollover occurs when the log reaches the size that the MaxLogFileSizeKB sets. FileSize is the default value.

LocalTime indicates the log file should be rolled over one time per day at a specified time by RolloverAtLocalTime.

Periodic indicates the log file should be rolled over after the number of specified seconds by RolloverAtLocalTime.

FileSize | LocalTime indicates that the log files are logged over when FileSize or LocalTime is reached, whichever occurs first.

FileSize | Periodic indicates that the log files are logged over when FileSize or Periodic is reached, whichever occurs first.

None indicates that log files are not rolled over.

MaxLogFileSizeKB
Specifications the maximum size that is allowed for the log file (in kilobytes) before rollover occurs, if the RolloverMode is set to FileSize. Valid values are 1 through 4294967295. The default value is 51200 (51.2 MB).

RolloverPeriodInSeconds
Specifies a period of time in seconds after which the log file is rolled over, if the RolloverMode is set to Periodic. Valid values are 1 through 2147483648. The default value is 43200 (12 hours).

RolloverAtLocalTime
Specifies the time of day at which the log file is rolled over, if the RolloverMode is set to LocalTime. Valid values are 00:00 through 23:59. The default value is 00:00 (Midnight local time).

NumberOfLogFiles
Specifies the maximum number of files to retain in the log directory for each unified logging originator. Valid values are 1 through 4294967295.

The vxlogmgr --auto command uses NumberOfLogFiles to determine how many log files to delete or move that starts with the oldest files. For example, a log directory contains seven files that a particular originator created. NumberOfLogFiles is set to 5. The vxlogmgr --auto --del command deletes the two oldest files that the originator created.

LogRecycle
Valid values are true, false. The default value is false. If true, the number of log files does not exceed the NumberOfLogFiles.
OIDNames
Specifies one or more alternate names for the unified logging originator that the -o option specifies. These names can be used in place of Originator IDs when you perform searches by using the vxlogview command. Each name can be up to 80 characters in length. Multiple names can be specified, separated by a space.

L10nLib
Specifies the absolute path and file name of the external localization library. This option is for Veritas internal use only. Use of this option can disable unified logging.

L10nResource
Specifies the name of a localization resource that is associated with a unified logging product or originator. This option is for Veritas internal use only. Use of this option can disable unified logging.

L10nResourceDir
This setting specifies the name of a localization resource directory that is associated with a unified logging product or originator. This option is for Veritas internal use only. Use of this option can disable unified logging.

The following four keynames operate only on UNIX systems.

LogFilePermissions
An octal number that specifies the UNIX file permissions that are assigned to log the files that the originator created, which the -o option specified. In most cases, this option is not needed.

SyslogIdent
Specifies a string that is attached to the beginning of every syslog message when LogToOslog is set to true. SyslogIdent can be any string up to 80 characters long. In most cases, this option is not needed.

SyslogOpt
Specifies the syslog option value that is passed to the syslog openlog function. Log messages are directed to the UNIX syslog when LogToOslog is enabled. Valid values are 0 through 4294967295. In most cases, this option is not needed.

SyslogFacility
Specifies the syslog facility value that is associated with log messages directed to the syslog. Log messages are directed to the syslog when LogToSyslog is enabled. In most cases, this option is not needed.

Valid values are: LOG_KERN, LOG_USER, LOG_MAIL, LOG_DAEMON, LOG_AUTH, LOG_LPR, LOG_NEWS, LOG_UUCP, LOG_CRON,
LOG_LOCAL0, LOG_LOCAL1, LOG_LOCAL2, LOG_LOCAL3, LOG_LOCAL4, LOG_LOCAL5, LOG_LOCAL6, LOG_LOCAL7. The default is LOG_USER.

The following three keynames operate only on Windows systems.

**NtEventLogCategory**

Specifies the category number that are associated with log messages that are directed to the Windows event log if LogToOslog is enabled. In most cases, there should be no need to use this option.

**LogFileSDDL**

Specifies the Windows Security Descriptor Definition Language (SDDL) string. This string sets the Access Control List (ACL) for the log files that the originator created, which the -o option specified. In most cases, there should be no need to use this option.

**NtEventLogSourceName**

Specifies the Windows Event log that log messages are directed to if the LogToOslog option is enabled on Windows. This option is for internal use only. Use of this option can disable unified logging.

**EXAMPLES**

Example 1 - Set the LogDirectory for NetBackup and originator ID 111 on UNIX:

```bash
# vxlogcfg -a --prodid 51216 --orgid 111 -s LogDirectory=/usr/openv/logs
```

Example 2 - Set the DebugLevel and DiagnosticLevel for all unified logging originators in NetBackup:

```bash
# vxlogcfg -a --prodid 51216 -o ALL -s DebugLevel=3 -s DiagnosticLevel=3
```

Example 3 - Set the default RolloverMode for product ID 1:

```bash
# vxlogcfg -a --prodid 1 -o Default -s RolloverMode=FileSize
```

Example 4 - Display configuration settings for originator 2 for product ID 1.

```bash
# vxlogcfg -l --prodid 1 --orgid 2
```

Example 5 - List all the originators that are configured for product ID 1.

```bash
# vxlogcfg -l --prodid 1
```

Example 6 - List all configured products.
FILES

UNIX systems:
/usr/openv/netbackup/nblog.conf
/etc/vx/VxICS/icsul.conf

SEE ALSO

See vxlogmgr on page 1005.
See vxlogview on page 1010.
vxlogmgr

vxlogmgr – manages the log files generated by the products that support Unified Logging

SYNOPSIS

vxlogmgr { -c | -m } -f AbsoluteDir [-a]
vxlogmgr { -d | -F } [-a]
vxlogmgr {-c | -m | -A filename} -f AbsoluteDir [-p ProductID] [-o OriginatorID] [-n Days] [-t Time] [-b StartDate] [-g LogSet] [-e EndDate] [-q] [-z]
vxlogmgr {-c | -m | -A filename} -f AbsoluteDir -w QueryString [-q] [-z]
vxlogmgr {-d | -F | -s} [-p ProductID] [-o OriginatorID] [-n Days] [-t Time] [-b StartDate] [-g LogSet] [-e EndDate] [-q] [-z]
vxlogmgr {-d | -F | -s} -w QueryString [-q] [-z]
vxlogmgr -v

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\n
DESCRIPTION

The vxlogmgr utility manages the log files that the unified logging-enabled applications generate. Log file management includes actions such as deleting or moving the log files that are based on log management configuration settings.

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

productID-originatorID-hostID-date-rotation.log

For more information about the unified logging naming format, and the logging originator IDs, refer to the NetBackup Logging Reference Guide.
OPTIONS

Specify the log management action to perform.

-A, --arch FileName
Creates an archive named FileName for the specified set of conditions. The
compressed zip file requires WinZip and wzzip on Windows to produce a zip
file. On UNIX, a tar utility and GnuZip are required to produce a tar.gzip file.

-a, --auto
Retrieves the log files that are based on individual configuration settings for
NumberOfLogFiles. The actions are taken based on the given action type (such
as move, copy, or delete). When the -a option is specified, the other options
cannot be used.

-b, --stdate 'StartDate'
Manages the log files that are created at the specified start date.
The required date and time values format in NetBackup commands varies
according to your locale. The /usr/openv/msg/.conf file (UNIX) and the
install_path\VERITAS\msg\LC.CONF file (Windows) contain information such
as the date-time formats for each supported locale. The files contain specific
instructions on how to add or modify the list of supported locales and formats.
See the "About specifying the locale of the NetBackup installation" topic in the
It is surrounded by single quotes in UNIX and double quotes in Windows. For
example:
UNIX: --stdate '1/1/2013 12:00:00 AM'
Windows: --stdate "1/1/2013 12:00:00 AM"

-c, --cp
Copies log files from the folder that is configured by the product to the specified
folder.

-d, --del
Deletes the log files from the folder that the product configures.

-e, --endate 'EndDate'
Manages the log files that are created up to the specified EndDate.
The required date and time values format in NetBackup commands varies
according to your locale. The /usr/openv/msg/.conf file (UNIX) and the
install_path\VERITAS\msg\LC.CONF file (Windows) contain information such
as the date-time formats for each supported locale. The files contain specific
instructions on how to add or modify the list of supported locales and formats.
See the "About specifying the locale of the NetBackup installation" topic in the NetBackup Administrator’s Guide, Volume II for more information.

This option must be surrounded by single quotes in UNIX and double quotes in Windows.

UNIX: --enddate '1/1/2013 12:00:00 PM'
Windows: --startdate "1/1/2013 12:00:00 AM"

-f, --dir AbsoluteDir
   Specifies the absolute name of the directory into which the log files are to be copied.

   On UNIX systems, this directory must be on the same device as the opt/openv/netbackup/logs directory, because the logs are hard linked rather than copied.

   This option is valid only with the -c option.

-F, --flush
   Deletes all log files for the host that originates this command except the most current log file. If the host that runs this command uses a shared directory, all log files for all hosts that use the same directory are removed. Only the most current file is preserved for the host that originated the flush command.

-m, --mv
   Moves log files from the folder that the product that is configured to the specified folder.

-n --days NumberOfDays
   Manages the log files that are created in last NumberOfDays days for the specified action.

-o, --origid OriginatorID
   Manages the log files that are identified by a given originator ID (OriginatorID).

-p, --prodid ProductID
   Manages the log files that are identified by a given product ID (ProductID) for the specified action. Instead of an identifier, the user can provide the product name.

-q, --quiet
   Prevents messages from being displayed (Quiet Mode).

-s, --vw
   Views the log files for a given query.

-t, --tail hh:mm:ss
   Manages the log files for the last hh:mm:ss hours.
-v, --version
  Displays the version information for this command.

-w, --where QueryString
  Retrieves a subset of logs that is based on a query string or condition
  (QueryString).

-z, --displaytimezone
  Displays the time zone information along with the log file display.

**EXIT STATUS**

The following exit values are returned:

0 Successful completion.

-1 An error occurred.

**QUERY STRINGS**

A query string is a text expression, similar to a database WHERE clause, that is used to retrieve log entries from the unified logging system. The expression is a combination of relational operators, constant integers, constant strings, and names of log fields that evaluate to a single value. Logical operators, such as AND and OR, are used to group expressions.

Supported relation operators include:

< Less than
> Greater than
<= Less than and equal to
>= Greater than and equal to
= Equal to
!= Not equal to

Supported logical operators include && (logical AND) and || (logical OR).

Predefined log fields include:

PRODID Product identifier (integer or string)
ORGID Originator identifier (integer or string)
STDATE Locale-specific start date (long integer or string [such as ‘mm/dd/yy’])
ENDATE Locale-specific end date (long integer or string [such as ‘mm/dd/yy’])
PREVTIME Previous time (string [hh:mm:ss])
EXAMPLES

Example 1 - Automatically move the older log files that NetBackup created to the folder /tmp/nblogs. The --auto option depends on the configuration setting NumberOfLogFiles.

   # vxlogmgr -m --auto --dir /tmp/nblogs

Example 2 - Delete the last 15 days of NetBackup log files:

   # vxlogmgr -d --prodid NB -n 15

Example 3 - Copy the log files created from date 01/22/12 by NetBackup:

   # vxlogmgr -c --where "(prodid = NB) && (stdate >= '01/22/12')"

   UNIX systems:

      --dir /usr/openv/logs

   Windows systems:

      --dir c:\temp\logfiles

Example 4 - Copy the log files that are created between 10/10/11 and 10/28/11 inclusive by product ID 100:

   # vxlogmgr -c --where "(PRODID == 100) && ((STDATE >= '10/10/11') && (ENDATE <= '10/28/11'))" --dir /usr/openv/logs

   UNIX systems:

      && (ENDATE <= '10/28/11'))" --dir /usr/openv/logs

   Windows systems:

      && (ENDATE <= '10/28/11'))" --dir c:\temp\logfiles

SEE ALSO

See vxlogcfg on page 997.
See vxlogview on page 1010.
vxlogview

vxlogview – display logs generated by the unified logging component

SYNOPSIS


vxlogview -q QueryName -f FileName {[-d DisplayOption,...] [-R ResourceDirectory] [-z TimeZone] [-l Locale]}

vxlogview -p ProductID -g LogSet | -i FileID {[-d DisplayOption,...] [-R ResourceDirectory] [-z TimeZone] [-l Locale]}


vxlogview -v

On UNIX systems, the directory path to this command is /usr/openv/netbackup/bin/

On Windows systems, the directory path to this command is install_path\NetBackup\bin\

DESCRIPTION

The vxlogview utility lets you view the logs that unified logging generates. Search criteria can be specified by using command-line options to view specific logs.

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

productID-originatorID-hostID-date-rotation.log

For more information about the unified logging name format and the logging originator IDs, refer to the NetBackup Logging Reference Guide.
OPTIONS

Specify the logs you want to view.

-A, --audit
Displays the audit messages.

-a, --all
Displays all log messages from log files that multiple Veritas products generate.

-b, --stdate StartDate
Displays the messages that are logged at the given start date and time.

The required date and time values format in NetBackup commands varies according to your locale. The /usr/openv/msg/.conf file (UNIX) and the install_path\VERITAS\msg\LC.CONF file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

See the "About specifying the locale of the NetBackup installation" topic in the NetBackup Administrator's Guide, Volume II for more information.

Surround the date by single quotes in UNIX and double quotes in Windows. For example:

-b '1/1/2013 12:00:00 AM'

If -b is not specified, messages are displayed from the beginning of the log file to the given end time (see the -e option).

-D, --debug
Displays debug log messages.

-d, --display DisplayOption,...
Displays the specified message fields. Separate multiple DisplayOptions with commas.

DisplayOption may be one or more of the following:

D - Display date
T - Display timestamp
m - Display message type
p - Display process ID
t - Display thread ID
P - Display product ID
O - Display originator ID
c - Display context token
s - Display application log entry severity
u - Display application or diagnostic Unique Message ID
x - Display actual log message text
w - Display who logged the diagnostic or the debug message
i - Display short name for a product
o - Display short name for an originator
all - Display all fields of the log record

If -d is not specified, the following fields are displayed by default.
- Date
- Time
- Who (for diagnostic and debug messages only)
- Severity (application messages only)
- UMI (application and diagnostic messages only)
- message text

-e, --enddate EndDate
Displays the messages that are logged up to a given end day and time.

The required date and time values format in NetBackup commands varies according to your locale. The /usr/openv/msg/.conf file (UNIX) and the install_path\VERITAS\msg\LC.CONF file (Windows) contain information such as the date-time formats for each supported locale. The files contain specific instructions on how to add or modify the list of supported locales and formats.

See the "About specifying the locale of the NetBackup installation" topic in the NetBackup Administrator's Guide, Volume II for more information.

Surround the date with single quotes in UNIX and double quotes in Windows. For example:

```
--enddate '1/1/2013 12:00:00 PM'
```

If the -e option is unspecified, vxlogview displays messages from the given start date-time (see the -b option) to the end of the log file.

-f, --filename FileName
Specifications the path name and file name of a file that contains one or more queries. Use with the -q option.
-G, --logdir Directory
Displays logs from the specified directory instead of a configured log directory. An absolute path must be specified for the directory.

-g, --logset LogSet
Displays log configuration settings for the specified LogSet.

-I, --diag
Displays diagnostic log messages.

-i, --fileid FileID
Displays the messages that a given file ID or shared originator ID logged. It searches only the log files that the specified process has created. By limiting the log files that it has to search, vxlogview returns a result faster. By comparison, the vxlogview -o option searches all unified log files for messages that the specified process logs.

-K, --hostname HostName
Displays the messages that the specified host name logged.

-L, --app -C | -E | -F | -M | -W
Displays the application log messages. The following parameters can be used with -L to specify the severity level:
-C, --crit : A critical error has occurred which may impact the availability of the application.
-E, --err : An error has occurred that does not affect the entire application.
-F, --info : An informational message.
-M, --emerg : An emergency condition exists that may result in an operating system failure or shutdown.
-W, --warning : A warning is issued for a problem that has been detected.

-l, --locale Locale
Displays the messages in the specified locale. The default is English. The messages are displayed in the current system locale if this option is not given.

-m, --who Entity
Displays the messages that are logged by the given entity method name or function name.

-N, --level Level -D | -I
Displays debug messages (-D) or diagnostic log messages (-I) for a given level (Level).

-n, --days NumberOfDays
Displays the messages that are logged for the last NumberOfDays days.
-o, --orgid OriginatorID
   Displays the messages that the specified originator ID has logged. You can
   use the ID number or the short name for the originator. For example, the Policy
   Execution Manager can be specified by nbpem or by 116, its originator ID
   number.

-P, --pid ProcessID
   Displays the messages that the specified process ID has logged.

-p, --prodid ProductID
   Displays the messages that the product (identified by a given product ID)
   logged. Instead of an identifier, the user can provide the abbreviated name of
   product. The NetBackup product ID is 51216, and the PBX product ID is 50936.

-R, --resdir ResourceDirectory
   Uses the resources from the specified directory instead of a configured
   localization resource directory.

-r, --result Result
   Displays the audit messages that have the specified result. Result can be either
   0 or 1.

-S, --tailloop
   Continuously displays the new messages that a given product ID and file ID
   pair log. The product ID (-p ProductID) and file ID (-i FileId) must accompany
   the tailloop option (-S) on the command line. The file ID can be a shared
   originator ID or an originator ID that is not shared with any other ID. tailloop
   starts by displaying to the console the last 10 messages that have been logged.
   It then displays any new log messages. Use Ctrl-C at any time to stop the
   loop.

-s, --subject Subject
   Displays the audit messages that have the specified Subject.

-T, --tid ThreadID
   Displays the messages that the specified thread ID has logged.

-t, --tail hh:mm:ss
   Displays the messages for the last hh:mm:ss time period.

-v, --version
   Displays the version information for this command.

-w, --where QueryString
   Specifies a WHERE clause to use when you query the log messages such that
   a subset of messages can be displayed. For more detail on QueryString, refer
   to the NetBackup Logging Reference Guide.
-X, --ctx ContextToken
Displays the messages that belong to the given context instance. Context
tokens identify context instances. If the context token is specified as "all," it
displays all of the context names and associated tokens.

-y, --displayhost
Displays the host name with each displayed log message. Use this option if
the log files come from different hosts and you want to display which message
came from which host.

-z, --timezone GMT+hh:ss | GMT-hh:ss
Displays the messages with time adjusted as per the given timezone.

EXIT STATUS
The following exit values are returned:
0 -- Successful completion.
-1 -- An error occurred.

QUERY STRINGS
A query string is a text expression, similar to a database WHERE clause, that is
used to retrieve log entries from the Unified Logging system. The expression is a
combination of relational operators, constant integers, constant strings, and names
of log fields that evaluate to a single value. Logical operators, such as AND and
OR, are used to group expressions.

Supported relational operators include: < (less than), > (greater than) <= (less than
or equal to, >= (greater than and equal to), = (equal to), and != (not equal to).

Supported logical operators include && (logical AND) and || (logical OR).

Predefined log fields can be in all uppercase or all lowercase (for example: PID | pid). These fields consist of the following:

- CTXTOK -- Context token (string)
- ENDATE -- Locale-specific end date (long integer or string)
- FILEID -- Shared originator ID (integer)
- HOSTNAME -- Name of source host (string with quotes)
- LEVEL -- Debug and diagnostic level. Default is to display all (integer 0-6)
- MSGTYPE -- The following message types are supported:
DEBUG | debug
DIAG | diag
APP | app
AUDIT | audit

ORGID -- Originator identifier (integer or string)
PID -- Process Identifier (integer)
PREVTIME -- Previous time (string $hh:mm:ss$
PRODID -- Product identifier (integer or string)
RETURNVAL -- The audit message outcome field (0 or 1)
SEV -- Severity level. The following severity types are supported:

INFO | info
WARNING | warning
ERR | err
CRIT | crit
EMERG | emerg

STDATE -- Locale-specific start date (long integer or string)
SUBJECT -- Audit message subject field (string)
TID -- Thread ID (integer)
WHO -- Who logged the message (string)

EXAMPLES

The following examples are valid for UNIX, which uses single quotes to enclose option arguments. In Windows, use double quotes.

Example 1 - Display the log messages for all the installed products:

# vxlogview -a

Example 2 - Display the log messages for PBX (product ID 50936). You must be an authorized user with administrator (root) privileges. It displays only the date, time, message type, and message text:

# vxlogview --prodid 50936 --display D,T,m,x

Example 3 - Display the log messages for NetBackup that were logged between the dates 11/18/10 and 11/21/10:

# vxlogview --where "(prodid = 'NB') && (stdate >= '11/18/10 0:0:0 AM' && endate <= '11/21/10 10:12:00 AM')"
Example 4 - Display the log messages that were created on or after the date and time 1/03/13, 11:00:00 a.m.:

# vxlogview -b '1/03/13 11:00:00 AM'

Example 5 - Display the log messages that were logged within the last hour:

# vxlogview --tail 1:00:00

Example 6 - Display the audit log messages that have a result of 0:

# vxlogview --audit -r 0

Example 7 - Display the context log messages for the "job_context" instance:

# vxlogview --ctx 'jobid=4'

SEE ALSO

See vxlogcfg on page 997.
See vxlogmgr on page 1005.
**W2KOption**

W2KOption—run the utility program that modifies normal backup and restore behavior on Windows systems

**SYNOPSIS**

```
W2KOption -backup -display [-server server_name] -system_state value
| -kms_activated_server value | -snapshotprovider_type value |
-ignore_unresolved_volumes volume[:volume...]
W2KOption -display

W2KOption -restore -display [-server server_name] same_hardware value
| -mounted_devices value | -sysvol value | -hard_links value |
-active_directory value | -system_state value
```

The directory path to this command is `install_path\NetBackup\bin\`

**DESCRIPTION**

This command operates only on Windows systems.

The W2KOption utility lets you modify normal backup and restore behavior.

**OPTIONS**

- **-ad, active_directory value**
  Controls how the Active Directory is restored. By default, Active Directory are restored in an authoritative manner. If you want to perform an Active Directory restore in a catchup manner, use this utility to change the behavior from authoritative to catchup.
  - 1 - Run an authoritative restore, which replaces all existing Active Directory objects.
  - 4 - Run a non-authoritative (catchup) restore. The restore merges with changes on other controllers in the domain.

- **-b, -backup**
  Lets you modify values for one or more of the backup options. The backup options are system_state, kms_activated_server, snapshotprovider_type, and ignore_unresolved_volumes.
-d, --display
Displays the program usage and shows how the options operate.

-hl, --hard_links 0 | 1
Controls how hard links are restored. By default, if the file is not present on the system, NetBackup tries to restore the file after the current restore completes. This action is called a secondary restore. You can change the behavior to shut off the secondary restore.

- 0 - Do not perform the secondary restore.
- 1 - Perform the secondary restore.

-iuv, --ignore_unresolved_volumes volume[:volume...]
Deletes the log files from the folder that the product configures.

-kas, --kms_activated_server 0 | 1
Specifies if NetBackup treats the computer as a Key Management Service (KMS) activated host during backups.

- 0 - Do not treat the host as a KMS activated server.
- 1 - Treat the host as a KMS activated server.

-md, --mounted_devices 0 | 1
Determines if the mounted devices registry key is restored.

- 0 - Restore the mounted device configuration.
- 1 - Do not restore the mounted device configuration.

-r, --restore options
Lets you modify values for one or more of the restore options. The restore options are --same_hardware, --mounted_devices, -sysvol, -hard_links, --active_directory, and --system_state.

-sh, --same_hardware 0 | 1
Determines how to restore the registry system hive. A normal restore operation does not restore all the registry items. However, when you restore to the same hardware, you can safely restore all these items.

- 0 - Assume different hardware. Do not restore all the registry items.
- 1 - Assume the same hardware. Restore all the registry items.

-s, --server server_name
Displays or sets the options on a computer other than the local computer. The default is the local computer.

-spt, --snapshotprovideridtype 0 | 1 | 2 | 3
Selects the snapshot provider type.
- 0 - Automatic provider selection
- 1 - Use the system provider
- 2 - Use a software provider
- 3 - Use a hardware provider

-ss, -system_state 0
Changes the backup method from the legacy system state method back to the normal VSS system state method. Selecting the legacy system state method is not allowed.

- 0 - Disallow legacy system state restore.

-sv, -sysvol 2 | 4
Determines how the Active Directory SYSVOL is restored. By default, NetBackup restores as if the SYSVOL being restored is the primary version. You can change this setting from the primary version to the non-authoritative version.

- 2 - Non-authoritative version.
- 4 - Primary version.

EXAMPLES

Example 1 - Ignore volumes H, K, and I during backup.

W2KOption -backup -ignore_unresolved_volumes H:K:I:

Example 2 - Treat the host as a KMS activated server.

W2KOption -backup -kms_activated_server 1
A
ACS library
  Automated Cartridge System 24
acs command 23
add_media_server_on_clients command 25
ASA database files 616

B
backupdbtrace command 26
backuptrace command 28
Bare Metal Restore (BMR)
  bmrc 30
  bmrcconfig 33
  bmrepadm 39
  bmrrprep 42
  bmr 45
  bmrsrtadm 48
BMR client program 30
BMR database 620
bmrc command 30
bmrcconfig command 33
bmrepadm command 39
bmrrprep command 42
bmr command 45
bmrsrtadm command 48
bp command 49
bparchive command 51
bpbackup command 57
bpbackupdb command 66
bpcatarc command 67
bpcatlist command 68
bpcatres command 71
bpcatrm command 72
bpcd command 73
bpchangeprimary command 75
bpcclient command 79
bpclimagelist command 86
bpcintcmd command 90
bpclusterutil command 94
bpcompatd command 97
bpconfig command 99

bpdbjobs command 108
bpdbm command 115
bpdgclone command 118
bpdown 120
bpduplicate command 121
b perror command 131
bpexpdate command 140
bpfs 149
bpfrlist command 151
bpgetconfig command 158
bpgetdebuglog command 164
bpimage command 166
bprimagelist command 171
bpimmedia command 180
bpimport command 192
bpinst command
  man page 200
  recreate a key file 203
bpkeyfile command 207
bpkeyutil command 209
bplabe command 211
bplist command 215
bpmedia command 223
bpmmedicalist command 227
bpmlicense command 239
bpnbcat command 242
bpnbaz command 251
bppficorr command 269
bpplacdrinfo command 272
bppclients command 276
bppldelte command 287
bpplinclud command 289
bpplinfo command 297
bpplist command 324
bppsched command 332
bppschedrep command 350
bppschedwin command 360
bppolicynew 363
bpps 372
bprd command 377
bprecov command 379
bprestore command 382
bpretlevel command 398
bpschedule command 401
bpschedulerep command 409
bpsetconfig command 416
bpstsinfo command 419
bpstuardd command 425
bptstudel command 435
bpstulist command 438
bpsturep command 446
bptestbpard command 455
bptestnetconn command 460
bptpcinfo command 466
bpup 471
bpverify command 472

C
cat_convert utility 481
cat_export utility 487
cat_import utility 490
configureCerts command 492
configureCertsForPlugins command 494
configureMQ command 496
configurePorts 498
configureWebServerCerts command 500
configuring
  encryption
    using bpinst command 200
create_nbdb command 505
crypt_option 201
crypt_strength option 201
csconfig cldinstance command 508
csconfig cldprovider command 528
csconfig meter command 530
csconfig reinitialize command 536
 csconfig throttle command 532

D
DES
  keys
    generating from bpkeyfile 207
device allocator 677
duplicatetrace command 537

E
Enterprise Media Manager 677

G
generating DES encryption keys 207

I
importtrace command 541
Inline Tape Copy option 126
installation
  using bpinst command 200

J
jbpSA 545
jnSA 547

K
key file 203
  pass phrase 203

L
LEGACY_CRYPT option 200
licenses
  managing with bpminlicense command 239
ltid command 549, 877

M
Media Contents Report 229
Media List Report 227
Media Manager commands
  acsd 23
Media Summary Report 229
mklogdir command 553

N
nbauditreport command 555
nbcatsync command 563
NBCC 566
NBCCR 571
nbcertcmd command 574
nbcertupdater command 588
nbcloudutil command 592
nbcloudrestore command 595
nbcomponentupdate command 599
nbcplogs command 606
nbcredkeyutil command 610
nbdb2adutl command 626
nbdb admin command 611
nbdb_backup command 616
nbdb_move command 618
nbdb ping command 620
nbdb_restore command 621
nbdb_unload command 623
nbdc command 631
nbdecommission command 634
nbdelete command 637
nbdeployutil command 642
nbdevconfig command 650
nbdevquery command 663
nbdiscover command 669
nbdms_start_server command 629
nbdms_start_stop command 630
nbdeva command 673
nbemm command 677
nbemmcmd command 678
nbffindfile command 697
nbfirescan command 701
nbftadm command 703
nbftconfig command 704
nbgetconfig command 714
nbhba command 717
nbholdutil command 720
nbhostidentity command 723
nbhostmgmt command 727
nbhypervtool command 732
nbidpcmd command 734
nbimageshare command 736
nbinstallcmd command 737
nbjm command 746
nbkmiutil command 747
nbkmcmd command 751
nbkmsutil command 758
nbmlb command 780
nboraadm command 762
nbora command 771
nbpem command 774
nbpemreq command 776
nbperfchk command 781
nbplupgrade command 785
nrb command 788
nrbutil command 789
nbregops command 795
nbreplicate command 797
nbrepo command 800
nbrestorevm command 802
nbseccmd command 822
nbsetconfig command 831
nbssnapimport command 833
nbssnapreplicate command 835
nbsqladm command 837
nbstl command 845
nbstlutil command 854
nbstop 864
nbsu command 867
nbsvgrp command 871
NetBackup Access Management 32, 38
NetBackup Encryption 200
   Legacy Encryption 200
NetBackup Policy Execution Manager 774
NetBackup Policy Execution Manager Requisition 776
NetBackup Resource Broker 788–789
NetBackup troubleshooting commands
   backupdbtrace 26
   backuptrace 28
NetBackup Vault 126

P
pass phrase 203
passphrase_prompt option 202
passphrase_stdin option 202
policy_encrypt option 202
policy_names option 202

R
resilient_clients command 874
restoretrace command 875

S
scripts
   drive_mount_notify 914
   stopltid command 877

T
tldcd command 882
tld command 878, 882
tpauseconf command 886
tpcleam command 889
tpcconfig command 892
tpext command 913
tpereq command 914
tpunmount command 917

U
Unified logging 997
   vxlogmgr 1005, 1018
   vxlogview 1010
upgrade policies to VMware or Hyper-V 785
**V**
verifytrace command 919  
vltadm command 922  
vltcontainers command 924  
vlt eject command 929  
vlt inject command 933  
vlt offsite media 935  
vlt op menu command 939  
vlt run 941  
vmad d command 946  
vmc change command 949  
vmc check xxx command 956  
vmd command 958  
vmd elete command 960  
vmo prcmd command 962  
vmp s command 967  
vmp ool command 971  
vmp query command 974  
vmr ule command 979  
vmu pdate command 982  
vnt d command 985  
vssat command 986  
vwcp _manage command 994  
vxlogcfg 997  
vxlogcfg command 997  
vxlogmgr command 1005  
vxlogview command 1010  

**W**
W2KOption command 1018