VERITAS™

VERITAS NetBackup™ 5.1

Commands

for UNIX

N12318B

Disclaimer

The information contained in this publication is subject to change without notice. VERITAS Software Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VERITAS Software Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

Copyright

Copyright © 2002 - 2004 VERITAS Software Corporation. All rights reserved. VERITAS, VERITAS SOFTWARE, the VERITAS logo, VERITAS NetBackup, and all other VERITAS product names and slogans are trademarks or registered trademarks of VERITAS Software Corporation in the USA and/or other countries. VERITAS and the VERITAS logo Reg. U.S. Pat. and Tm. Off. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies.

VERITAS Software Corporation
350 Ellis Street
Mountain View, CA 94043
USA
Phone 650–527–8000
Fax 650-527-2901
www.veritas.com

Third-Party Copyrights

ACE 5.2A: ACE(TM) is copyrighted by Douglas C.Schmidt and his research group at Washington University and University of California, Irvine, Copyright (c) 1993-2002, all rights reserved.

IBM XML for C++ (XML4C) 3.5.1: Copyright (c) 1999,2000,2001 Compaq Computer Corporation; Copyright (c) 1999,2000,2001 Hewlett-Packard Company; Copyright (c) 1999,2000,2001 IBM Corporation; Copyright (c) 1999,2000,2001 Hummingbird Communications Ltd.; Copyright (c) 1999,2000,2001 Silicon Graphics, Inc.; Copyright (c) 1999,2000,2001 Sun Microsystems, Inc.; Copyright (c) 1999,2000,2001 The Open Group; All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

JacORB 1.4.1: The licensed software is covered by the GNU Library General Public License, Version 2, June 1991.

Open SSL 0.9.6: This product includes software developed by the OpenSSL Project * for use in the OpenSSL Toolkit. (http://www.openssl.org/)

TAO (ACE ORB) 1.2a: TAO(TM) is copyrighted by Douglas C. Schmidt and his research group at Washington University and University of California, Irvine, Copyright (c) 1993-2002, all rights reserved.

Contents

Preface . . . . . **ix**

What is in this manual? ix

Getting Help ix

Related Resources x

Glossary xi

Accessibility Features xi

Conventions xii

Introduction xiv

Chapter 1. NetBackup Commands **1**

acsd(1M) 1

backupdbtrace(1M) 3

backuptrace(1M) 5

bp(1) 7

bpadm(1M) 9

bparchive(1) 10

bpauthorize(1M) 15

bpauthsync(1M) 18

bpbackup(1) 21

bpbackupdb(1M) 27

bpcatarc(1M) 32

bpcatlist(1M) 33

bpcatres(1M) 36

bpcatrm(1M) 37

bpcd(1M) 38
bpchangeprimary(1M) 40
bpclient(1M) 45
bpconfig(1M) 48
bpdbjobs(1M) 58
bpdbm(1M) 65
bpdgclone(1M) 67
bpduplicate(1M) 69
bperror(1M) 77
bpexpdate(1M) 88
bpfis(1M) 94
bpgetconfig(1M) 97
bpgetdebuglog(1M) 100
bpimage(1M) 101
bpimagelist(1M) 106
bpimmedia(1M) 113
bpimport(1M) 123
bpinst(1M) 129
bpkeyfile(1) 137
bpkeyutil(1M) 139
bplabel(1M) 141
bplist(1) 144
bpmedia(1M) 151
bpmedialist(1M) 154
bpminlicense(1M) 165
bpmoverinfo(1M) 167
bpnbat(1M) 168
bpnbaz(1M) 173
bppficorr (1M) 188
bpplclients(1M) 190

bppldelete(1M) 197
bpplinclude(1M) 198
bpplinfo(1M) 203
bppllist(1M) 212
bpplsched(1M) 214
bpplschedrep(1M) 225
bppolicynew(1M) 232
bprd(1M) 238
bprecover(1M) 240
bprestore(1) 245
bpSALinfo(1M) 254
bpschedule(1M) 256
bpschedulerep(1M) 262
bpsetconfig(1M) 267
bpstuadd(1M) 269
bpstudel(1M) 276
bpstulist(1M) 278
bpsturep(1M) 283
bpsynth(1M) 289
bptpcinfo(1M) 291
bpverify(1M) 296
cat_convert(1M) 303
duplicatetrace(1M) 305
importtrace(1M) 308
jbpSA(1) 311
jnbSA(1M) 313
lmfd(1M) 315
ltid(1M) 319
nbdbsetport(1M) 321
nbdbsetpw(1M) 322

ndmpmoveragent(1M) 323
odld(1M) 325
restoretrace(1M) 327
set_ndmp_attr (1M) 329
tl4d(1M) 332
tl8d(1M) 334
tldd(1M) 338
tlhd(1M) 341
tlmd(1M) 344
tpautoconf(1M) 346
tpclean(1M) 350
tpconfig(1M) 353
tpformat(1M) 360
tpreq(1) 363
tpunmount(1) 366
ts8d(1M) 368
tsdd(1M) 370
tshd(1M) 372
verifytrace(1M) 374
vltadm(1M) 377
vltcontainers(1M) 379
vlteject(1M) 383
vltinject (1M) 387
vltoffsitemedia (1M) 389
vltopmenu (1M) 393
vltrun(1M) 394
vmadd(1M) 398
vmadm(1M) 401
vmchange(1M) 403
vmcheckxxx(1M) 411

vmd(1M) 413
vmdb_merge(1M) 416
vmdelete(1M) 419
vmoprcmd(1M) 421
vmphyinv(1M) 424
vmpool(1M) 428
vmquery(1M) 431
vmrule(1M) 435
vmupdate(1M) 437
vopie_util(1M) 440
vopied(1M) 444
xbp(1) 446

Index 449

Preface

The purpose of this document is to provide you with a book that contains all of the NetBackup "man page" commands. This enables you to find a printable version of the command quickly and easily without searching through multiple books in the NetBackup Library.

What is in this manual?

This document contains detailed information about each NetBackup command pertinent to a UNIX system. Each command contains a a brief description of the primary function of the command, a synopsis, and descriptions of each of the options listed in the synopsis. In addition, some commands contain notes and examples to help the user understand how to use the command.

Getting Help

VERITAS offers you a variety of support options.

Accessing the VERITAS Technical Support Web Site

The VERITAS Technical Support Web site allows you to do any of the following:

- Obtain updated information about NetBackup, including system requirements, supported platforms, and supported peripherals
- Contact the VERITAS Technical Support staff and post questions to them
- Get the latest patches, upgrades, and utilities
- View the NetBackup Frequently Asked Questions (FAQ) page
- Search the knowledge base for answers to technical support questions
- Receive automatic notice of product updates
- Find out about NetBackup training

- Read current white papers related to NetBackup

The address for the VERITAS Technical Support Web site follows:

`http://support.veritas.com`

Using VERITAS Telephone and E-mail Support

Telephone support for NetBackup is only available with a valid support contract. To contact VERITAS for technical support, dial the appropriate phone number listed on the Technical Support Guide included in the product box and have your product license information ready for quick navigation to the proper support group.

▼ To locate the telephone support directory on the VERITAS web site

1. Open `http://support.veritas.com` in your web browser.
2. Click the **Phone Support** icon. A page that contains VERITAS support numbers from around the world appears.

▼ To contact support using E-mail on the VERITAS web site

1. Open `http://support.veritas.com` in your web browser.
2. Click the **E-mail Support** icon. A brief electronic form appears and prompts you to:
   - Select a language of your preference
   - Select a product and a platform
   - Associate your message to an existing technical support case
   - Provide additional contact and product information, and your message
3. Click **Send Message**.

Related Resources

The following documents contain supporting information that relate to the commands documented in the book.

- *VERITAS NetBackup Installation Guide for UNIX*

  NetBackup_Install_UNIX.pdf

  Explains how to install NetBackup software on UNIX-based platforms.
- *VERITAS NetBackup System Administrator's Guide for UNIX, Volume I*

NetBackup_AdminGuideI_UNIXServer.pdf

Explains how to configure and manage NetBackup on a UNIX server, including managing storage units, backup policies, catalogs, and host properties.

- *VERITAS NetBackup System Administrator's Guide for UNIX, Volume II*

  NetBackup_AdminGuideII_UNIXServer.pdf

  Explains additional NetBackup features such as access control and enhanced authorization and authentication. The guide also discusses using NetBackup with AFS and Intelligent Disaster Recovery (IDR).

- *VERITAS NetBackup Media Manager System Administrator's Guide for UNIX*

  MediaMgr_AdminGuide_Unix.pdf

  Explains how to configure and manage the storage devices and media on UNIX servers running NetBackup. Media Manager is part of NetBackup.

Glossary

If you encounter unfamiliar terminology, consult the NetBackup online glossary. The glossary contains terms and definitions for NetBackup and all additional NetBackup options and agents.

The NetBackup online glossary is included in the NetBackup help file.

▼ **To access the NetBackup online glossary**

1. In the NetBackup Administration Console, click **Help** > **Help Topics**.
2. Click the **Contents** tab.
3. Click **Glossary of NetBackup Terms**.

Use the scroll function to navigate through the glossary.

Accessibility Features

NetBackup contains features that make the user interface easier to use by people who are visually impaired and by people who have limited dexterity. Accessibility features include:

- Support for assistive technologies such as screen readers and voice input (Windows servers only)

- Support for keyboard (mouseless) navigation using accelerator keys and mnemonic keys

For more information, see the *NetBackup System Administrator's Guide for Windows, Volume I* or the *NetBackup System Administrator's Guide for UNIX, Volume I*.

Conventions

The following section explains typographical and other conventions used in this guide.

Typographical Conventions

Here are the typographical conventions used throughout the manuals:

Conventions

Convention	Description
GUI Font	Used to depict graphical user interface (GUI) objects, such as fields, list boxes, menu commands, and so on. For example: Enter your password in the **Password** field.
Italics	Used for placeholder text, book titles, new terms, or emphasis. Replace placeholder text with your specific text. For example: Replace *filename* with the name of your file. Do *not* use file names that contain spaces. This font is also used to highlight NetBackup server-specific or operating system-specific differences. For example: *This step is only applicable for NetBackup Enterprise Server.*
`Code`	Used to show what commands you need to type, to identify path names where files are located, and to distinguish system or application text that is displayed to you or that is part of a code example.
Key+Key	Used to show that you must hold down the first key while pressing the second key. For example: Ctrl+S means hold down the Ctrl key while you press S.

You should use the appropriate conventions for your platform. For example, when specifying a path, use backslashes on Microsoft Windows and slashes on UNIX. Significant differences between the platforms are noted in the text.

Tips, notes, and cautions are used to emphasize information. The following samples describe when each is used.

Note Used for important information that you should know, but that shouldn't cause any damage to your data or your system if you choose to ignore it.

Caution Used for information that will prevent a problem.

Command Usage

The following conventions are frequently used in the synopsis of command usage.

brackets [ ]

The enclosed command line component is optional.

Vertical bar or pipe (|)

Separates optional arguments from which the user can choose. For example, when a command has the following format:

`command` *`arg1`*`|`*`arg2`*

In this example, the user can use either the *arg1* or *arg2* variable.

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:

- Select **Start** > **Programs** > **VERITAS NetBackup** > **NetBackup Administration Console**.

The corresponding actions could 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**.

Introduction

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 certain portions or options within a command apply specifically to one product such as NetBackup Enterprise Server. In these situations, you will see that a note has been inserted in the text to identify the information as only information that only applies to one NetBackup product. In most instances, NetBackup Enterprise Server-specific information is highlighted.

The command definitions are listed in alphabetical order in this book. However, the following tables separate the commands according to the part of NetBackup they belong with. For example, commands that pertain to the general functionality of NetBackup are grouped under NetBackup Commands. In addition, commands that describe tape functionality are grouped in the Media Manager Commands table. The following list identifies the groups of NetBackup commands. Refer to the Table of Contents for the exact page of a particular command.

- NetBackup System Administration Commands
- NetBackup Media Manager Commands
- NetBackup for NDMP Commands
- NetBackup Advanced Client Commands
- NetBackup Troubleshooting Command
- NetBackup Vault Commands

The following tables list all of the NetBackup commands. The tables group the commands according to the NetBackup function.

NetBackup System Administration Commands

Commands	NetBackup Enterprise Server	NetBackup Server
bp(1)	X	X
bpadm(1M)	X	X
bparchive(1)	X	X
bpauthorize(1M)	X	X
bpauthsync(1M)	X	X

NetBackup System Administration Commands (continued)

Commands	NetBackup Enterprise Server	NetBackup Server
bpbackup(1)	X	X
bpbackupdb(1M)	X	X
bpcatarc(1M)	X	X
bpcatlist(1M)	X	X
bpcatres(1M)	X	X
bpcatrm(1M)	X	X
bpcd(1M)	X	X
bpchangeprimary(1M)	X	X
bpclient(1M)	X	X
bpconfig(1M)	X	X
bpdbjobs(1M)	X	X
bpdbm(1M)	X	X
bpduplicate(1M)	X	X
bperror(1M)	X	X
bpexpdate(1M)	X	X
bpfis(1M)	X	X
bpgetconfig(1M)	X	X
bpimage(1M)	X	X
bpimagelist(1M)	X	X
bpimmedia(1M)	X	X

NetBackup System Administration Commands (continued)

Commands	NetBackup Enterprise Server	NetBackup Server
bpimport(1M)	X	X
bpinst(1M)	X	X
bpkeyfile(1)	X	X
bpkeyutil(1)	X	X
bplabel(1M)	X	X
bplist(1)	X	X
bpmedia(1M)	X	X
bpmedialist(1M)	X	X
bpminlicense(1M)	X	X
bpnbat(1M)	X	X
bpnbaz(1M)	X	X
bpplclients(1M)	X	X
bppldelete(1M)	X	X
bpplinfo(1M)	X	X
bpplinclude(1M)	X	X
bpplist(1M)	X	X
bpplsched(1M)	X	X
bpplschedrep(1M)	X	X
bppolicynew(1M)	X	X
bprd(1M)	X	X

NetBackup System Administration Commands (continued)

Commands	NetBackup Enterprise Server	NetBackup Server
bprecover(1M)	X	X
bprestore(1)	X	X
bpSALinfo(1M)	X	X
bpschedule(1M)	X	X
bpschedulerep(1M)	X	X
bpsetconfig(1M)	X	X
bpstuadd(1M)	X	X
bpstudel(1M)	X	X
bpstulist(1M)	X	X
bpsynth(1M)	X	X
bpsturep(1M)	X	X
bpverify(1M)	X	X
cat_convert(1M)	X	X
jbpSA(1M)	X	X
jnbSA(1M)	X	X
nbdbsetport(1)	X	X
nbdbsetpw(1M)	X	X
vopied(1M)	X	X
vopie_util(1M)	X	X
xbp(1)	X	X

NetBackup Media Manager Commands

Commands	NetBackup Enterprise Server	NetBackup Server
acsd(1M)	X	
lmfd(1M)	X	
ltid(1M)	X	X
odld(1M)	X	
tl4d(1M)	X	X
tl8d(1M)	X	X
tldd(1M)	X	X
tlhd(1M)	X	
tlmd(1M)	X	
tpautoconf(1M)	X	X
tpclean(1M)	X	X
tpconfig(1M)	X	X
tpformat(1M)	X	
tpreq(1)	X	X
tpunmount(1)	X	X
ts8d(1M)	X	X
tsdd(1M)	X	X
tshd(1M)	X	
vmadd(1M)	X	X

NetBackup Media Manager Commands (continued)

Commands	NetBackup Enterprise Server	NetBackup Server
vmadm(1M)	X	X
vmchange(1M)	X	X
vmcheckxxx(1M)	X	X
vmd(1M)	X	X
vmdelete(1M)	X	X
vmoprcmd(1M)	X	X
vmphyinv(1M)	X	X
vmpool(1M)	X	X
vmquery(1M)	X	X
vmrule(1M)	X	X
vmupdate(1M)	X	X

NetBackup for NDMP Commands

Commands	NetBackup Enterprise Server	NetBackup Server
ndmpmoveragent(1M)	X	X
set_ndmp_attr(1M)	X	X

NetBackup Advanced Client Commands

Commands	NetBackup Enterprise Server	NetBackup Server
bpdgclone(1M)	X	X
bpmoverinfo(1M)	X	X
bppficorr(1M)	X	X
bptpcinfo(1M)	X	X

NetBackup Troubleshooting Command

Commands	NetBackup Enterprise Server	NetBackup Server
backupdbtrace(1M)	X	X
backuptrace(1M)	X	X
bpgetdebuglog(1M)	X	X
duplicatetrace(1M)	X	X
importtrace(1M)	X	X
restoretrace(1M)	X	X
verifytrace(1M)	X	X

NetBackup Vault Commands

Commands	NetBackup Enterprise Server	NetBackup Server
vltadm(1M)	X	
vltcontainers(1M)	X	
vlteject(1M)	X	
vltinject(1M)	X	
vltoffsitemedia(1M)	X	
vltopmenu(1M)	X	
vltrun(1M)	X	

NetBackup Commands 1

The chapter lists and describes all of the NetBackup commands for UNIX platforms in alphabetical order.

acsd(1M)

NAME

acsd - Automated Cartridge System (ACS) daemon

SYNOPSIS

```
/usr/openv/volmgr/bin/acsd [-v]
```

DESCRIPTION

`acsd` interfaces with Media Manager to automatically mount and unmount tapes that are under Automated Cartridge System (ACS) control. It is initiated by `ltid` (the Media Manager device daemon), if the Media Manager device configuration shows drives in an ACS robot.

Stopping `ltid` stops `acsd`. You can start or stop `acsd` independently of `ltid` using `/usr/openv/volmgr/bin/vmps` or your server's `ps` command to identify `acsd`'s process id and then entering 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`) which communicates with the server that controls the Automated Cartridge System.

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 Automated Cartridge System errors exist, `acsd` changes the robot to the DOWN state. In this state, `acsd` is still running and returns the robot to the UP state when the problem no longer exists.

Drives are addressed and defined in Media Manager using the following: ACS number, LSM number, Panel number, and Drive number.

Drive cleaning for ACS robots must be configured using ACS library software. Cleaning volumes cannot be defined using Media Manager. In addition, you cannot use the `tpclean(1M)` command for cleaning operations on drives under ACS robotic control.

The Internet service port number for `acsd` must be in `/etc/services`. If you are using NIS (Network Information Service), you should place the entry in this host's `/etc/services` file in the master NIS server database for services. To override the services file, create the file `/usr/openv/volmgr/database/ports/acsd` with a single line containing the service port number for `acsd`. The default service port number is 13702.

You must have root privileges to execute this command.

OPTIONS

`-v`

Logs debug information using `syslogd`. If you start `ltid` with `-v`, `acsd` also starts with `-v`.

NOTES

This command applies only to NetBackup Enterprise Server.

ERRORS

`acsd` returns an error message if there is a copy of `acsd` running.

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 directory `/usr/openv/volmgr/debug/acsssi`.

SEE ALSO

`ltid(1M), syslogd(8), tpconfig(1M), vmadm(1M)`

backupdbtrace(1M)

NAME

backupdbtrace – trace debug logs of backupdb (NetBackup image catalog backup) job[s]

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/backupdbtrace [-server name]
          [-job_id number] [-start_time hh:mm:ss] [-end_time
          hh:mm:ss] [-install_path path] mmddyy [mmddyy ...]
```

DESCRIPTION

`backupdbtrace` consolidates the debug log messages for the specified backupdb job[s] and writes them to standard output. The messages will be sorted by time. `backupdbtrace` will attempt to compensate for time zone changes and clock drift between remote servers and clients.

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

If -job_id is specified, `backupdbtrace` uses this option as the sole criterion for selecting the backupdb job to trace. If option -job_id is not used, then `backupdbtrace` selects all the backupdb jobs executed on all the days specified by day stamps (*mmddyy*). If –start_time/-end_time options are used then the debug logs in the specified time interval are examined.

`backupdbtrace` writes error messages to standard error.

You must have root privileges to execute this command.

OPTIONS

`-server`
: Name of the media server where the `backupdb` command is executed. 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 time stamp to start analyzing the logs. Default is 00:00:00.

`-end_time`
: Latest time stamp to finish analyzing the logs. Default is 23:59:59.

`-install_path`
: The NetBackup install path on a Windows NT or Windows 2000 server. Default is c:\Program Files\VERITAS.

  Note that the install path must be enclosed in quotes if the path includes a space.

`mmddyy`
: One or more day stamps. This identifies the log file names (log.mmddyy for UNIX, mmddyy.log for Windows NT or Windows 2000) that will be analyzed.

OUTPUT FORMAT

The format of an output line is:

<daystamp>.<millisecs>.<program>.<sequence> <machine> <log_line>

`daystamp`
: The day of the log in yyyymmdd format.

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

`program`
: The name of program (ADMIN, BPBKAR, 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 actually appears in the debug log file.

EXAMPLES

Example 1

The following example analyzes the log of backupdb job with job ID 5 executed on August 6, 2002.

```
backupdbtrace -job_id 5 080602
```

Example 2

The following example analyzes the log of all backupdb jobs that are executed on August 5, 2002 and August 17, 2002.

```
backupdbtrace 080502 081702
```

backuptrace(1M)

NAME

backuptrace – consolidate the debugs logs for a NetBackup job.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/backuptrace [-master_server
         name] [-job_id number] [-birth_time number]
         [-policy_name name] [-client_name name] [-start_time
         hh:mm:ss] [-end_time hh:mm:ss] [-install_path path]
         mmddyy [mmddyy...]
```

DESCRIPTION

The `backuptrace` utility can be used to consolidate the debug logs for a specified NetBackup job[s]. The debug log messages relevant to the specified backup job[s] will be written to standard output. The messages will be sorted by time. The backuptrace utility will attempt to compensate for time zone changes and clock drift between remote servers and clients. The output is formatted so that it should be relatively easy to sort or grep by time stamp, program name, and/or server/client name.

At a minimum, you must enable debug logging for bpsched on the master server, for `bpbrm`, `bptm`/`bpdm` on the media server and `bpbkar` on the client. For best results, set the verbose logging level to 5 and enable debug logging for `bpdbm` and `bprd` on the master server and for `bpcd` on all servers and clients in addition to the processes already identified.

The `backuptrace` utility can be used for regular file system, database extension and alternate backup method backup jobs.

You must have root privileges to execute 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 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 time stamp to start analyzing the logs.

`-end_time hh:mm:ss`
: Latest time stamp to finish analyzing the logs.

`-install_path path`
: The NetBackup install path on a Windows NT/2000 server. Default is "c:\Program Files\VERITAS".

  Note that the install path must be enclosed in quotes if any component of the path includes a space.

`mmddyy [mmddyy]`
: One or more day stamps. This identifies the log file names (log.mmddyy for UNIX, mmddyy.log for Windows NT/2000) that will be analyzed.

NOTES

Media Manager logs are not analyzed.

EXAMPLES

```
/usr/openv/netbackup/bin/admincmd/backuptrace -job_id 289 041102 >
/tmp/job.log.289
```

This invocation of the utility will consolidate logs for all jobs started for the policy *weekly_bkups* on *07/12/02*. Use the `-start_time`/`-end_time` arguments to limit the window for which the jobs are to be evaluated.

bp(1)

NAME

bp - Start the NetBackup menu interface for users.

SYNOPSIS

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

```
/usr/openv/netbackup/bin/bp [ -b |-a | -r | -ra] [-verbose]
```

DESCRIPTION

The bp command starts a menu interface that lets users archive, back up, and restore files, directories, or raw partitions from their client workstations. This interface can be run from any character-based terminal (or terminal emulation window) for which the user has a termcap or terminfo definition.

The bp online help provides detailed operating instructions.

OPTIONS

The menu that appears at startup depends on the option used with the bp command. Running the bp command without specifying an option starts the utility 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 The following options for SAP, DB2, and SQL-BackTrack apply only to 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

`bparchive(1),bpbackup(1),bplist(1),bprestore(1)`

bpadm(1M)

NAME

`bpadm` - Start the NetBackup menu interface for administrators.

SYNOPSIS

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

DESCRIPTION

The `bpadm` utility has a menu interface that an administrator can use to configure NetBackup and monitor its operations. `bpadm` requires root privileges. This interface 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 System Administrator's Guide* and the `bpadm` online help for detailed operating instructions.

FILES

`/usr/openv/netbackup/help/bpadm/*`

`/usr/openv/netbackup/logs/admin/*`

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

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

SEE ALSO

`bprd(1M)`

bparchive(1)

NAME

`bparchive` - This command archives files to the NetBackup server.

SYNOPSIS

```
/usr/openv/netbackup/bin/bparchive [-p policy] [-s schedule][-L
          progress_log [-en]] [-S master_server1,master_server2,...]]
          [-t policy_type] [-w [hh:mm:ss]] [-help] [-k
          "keyword_phrase"] -f listfile | filenames
```

DESCRIPTION

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

By default, you are returned 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 this behavior so `bparchive` works in the foreground and returns 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 prior to running 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 `/usr/openv/netbackup/logs/bparchive/` directory with public-write access, `bparchive` creates a debug log file in this directory to use for troubleshooting.

In addition, if a nonroot user specifies `USEMAIL =` *mail_address* in their `$HOME/bp.conf` file or a root user specifies it in the `/usr/openv/netbackup/bp.conf` file, NetBackup sends mail on the archive completion status to *mail_address*. This message is sent when the archive process is complete.

The following restrictions apply to this command:

- To archive a file with the `bparchive` command, you must be either root or the owner and a member of the primary group (as owner) to delete the file. 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.
- 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 also does not archive disk-image backups.

OPTIONS

`-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.

`-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 is using (see the `-p` option).

`-S` *master_server*

Specifies the name of the NetBackup master server. The default is the first `SERVER` entry in the `/usr/openv/netbackup/bp.conf` file.

`-t` *policy_type*

Specifies one of the following numbers corresponding to the policy type. The default for Windows clients is `13`, for Netware clients the default is `10`, and the default for all others is `0`:

`0` = Standard

`4` = Oracle

`6` = Informix-On-BAR

`7` = Sybase

`10` = NetWare

`13` = MS-Windows-NT

`14` = OS/2

`15` = MS-SQL-Server

`16` = MS-Exchange-Server

`19` = NDMP

Note *The following policy types apply only to NetBackup Enterprise Server.*

`11` = DataTools-SQL-BackTrack

`17` = SAP

`18` = DB2

`20` = FlashBackup

`21` = Split-Mirror

`22` = AFS

`-L` *progress_log* `[-en]`

Specifies the name of an existing file in which to write progress information. The file name must begin with `/`.

For example: `/home/tlc/proglog`.

The default is to not use a progress log.

Include the `-en` option to generate a log in English. The name of the log will contain the string `_en`. This option is useful to support personnel assisting in a distributed environment where differing locales may create logs of various languages.

`-w` [*hh:mm:ss*]

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

The date and time format depend on the user's locale. See NOTES.

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.

`-help`

Prints a command line usage message when `-help` is the only option on the command line.

`-k` *keyword_phrase*

Specifies a keyword phrase that NetBackup associates with the image created by this archive operation. You can then restore the image by specifying the keyword phrase with the `-k` option on the `bprestore` 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 ('...') to avoid conflict with the UNIX shell.

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

`-f` *listfile*

Specifies a file (*listfile*) containing 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 format required for the file list depends on whether the files have spaces or newlines in the names.

To archive files that do not have spaces or newlines in the names, use this format:

filepath

Where *filepath* is the path to the file you are archiving. For example:

```
/home
/etc
/var
```

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

filepathlen filepath

Where *filepath* is the path to the file you are archiving and *filepathlen* is the number of characters in the file path.

For example:

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

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.

NOTES

The format that you must use for date and time values in NetBackup commands varies according to the locale setting.

If you are uncertain of the NetBackup command requirements for your locale, enter the command with the `-help` option and check the usage. The following is part of the `bparchive` usage statement output that shows the `-w` option:

```
[-w [hh:mm:ss]]
```

Notice the hours:minutes:seconds requirements. These are for a locale setting of C and can be different for other locales.

For more information on locale, see the `locale(1)` man page for your system.

EXAMPLES

Example 1

To archive a single file, enter:

```
bparchive /usr/user1/file1
```

Example 2

To archive files listed in a file named `archive_list`, enter:

```
bparchive -f archive_list
```

Example 3

To associate the keyword phrase "Archive My Home Directory 02/02/02" to the archive of the directory `/home/kwc` and use a progress log named `/home/kwc/arch.log` enter the following (the backslash continues the command as if it were on one line):

```
bparchive -k "Archive My Home Directory 02/02/02" \-L
/home/kwc/arch.log  /home/kwc
```

FILES

`$HOME/bp.conf`

`/usr/openv/netbackup/logs/bparchive/log.`*mmddyy*

SEE ALSO

`bp(1),bpbackup(1),bplist(1),bprestore(1)`

bpauthorize(1M)

NAME

`bpauthorize` - Manage the `authorize.txt` file on remote servers.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpauthorize [-M nb_server] [-g
        user_if_host] [-debug] [-verbose] [-get_privileges] file

usr/openv/netbackup/bin/admincmd/bpauthorize [-M nb_server]
        [-debug] [-verbose] -get_authorize file

/usr/openv/netbackup/bin/admincmd/bpauthorize [-M nb_server]
        [-debug] [-verbose] -set_authorize file
```

DESCRIPTION

This command is available only on NetBackup master servers and sets up authentication files on NetBackup servers and clients according to the options that are specified on the command.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-debug`

Issues debug messages to standard error.

`-g` *user_if_host*

When used with `-get_privileges`, indicates the job monitoring capabilities of the specified host:

```
MONITOR_OK = 0 | 1
```

Where `1` indicates that the host specified can use the more efficient job monitoring capabilities of NetBackup 4.5.

`-g` option is used internally by the Java interface (`jnbSA`).

`-get_privileges` *file*

Displays the privileges you have on the remote server.

If *file* is specified, output is written to this file. By default, output is written to standard output.

If `-verbose` is not indicated, the output would look similar to the following example:

```
1 1 1 1 0
```

The privileges appear in the following order: (`-verbose` indicated)

`IS_SERVER = 0 | 1`

Where 1 indicates that the local host name is in the remote machine's SERVER list in `bp.conf`.

`IS_MEDIA_SERVER = 0 | 1`

Where 1 indicates that the local host name is in the remote machine's MEDIA_SERVER list in `bp.conf`.

`IS_ADMIN =0 | 1`

Where 1 indicates that the user is an administrator according to the `authorize.txt` file on the remote machine.

`IS_OPERATOR =0 | 1`

Where 1 indicates that the user is an operator according to the `authorize.txt` file on the remote machine.

AUTHENTICATION_REQUIRED = `0 | 1`

`1` = Authentication to the server is required

`0` = Authentication to the server is not required

Note If the server is a NetBackup version prior to 4.5, authentication required returns `1`.

`-get_authorize` *file*

Displays the contents of the `authorize.txt` file on the remote server.

If *file* specified, output is written to this file. By default, output is written to standard output.

`-M` *nb_server*

Indicates the remote server to check. The default is the master server.

`-set_authorize` *file*

Updates the contents of the `authorize.txt` file on the remote server.

If *file* is specified, input is read from this file. By default, input is read from standard input.

To use, first write the `authorize.txt` file from a NetBackup server to a temporary file:

`./bpauthorize -M` *nb_server* `-get_authorize /tmp/` *filename.txt*

Then, edit and save the file:

`vi /tmp/` *filename.txt*

Finally, use `-set_authorize` to update the `authorize.txt` file of the NetBackup server with the edited file:

`./bpauthorize -M` *nb_server* `-set_authorize /tmp/` *filename.txt*

`-verbose`

Select verbose mode to include more detailed descriptions when using `bpauthorize` with `-get_privileges` or `-get_authorize` options.

bpauthsync(1M)

NAME

`bpauthsync` - Synchronize authentication files on NetBackup servers and clients.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpauthsync [-verbose]
        [-methods] [-names] [-vopie] [-methods_allow path_name]
        [-methods_deny path_name] [-names_allow path_name ]
        [-names_deny path_name] [-clients [client1 client2 ...
        clientN] ] [-servers [server1 server2 ... serverN] ]
```

DESCRIPTION

This command is available only on NetBackup master servers and sets up authentication files on NetBackup servers and clients according to the options that are specified on the command.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-verbose`
: Issue additional messages.

`-methods`
: Push the `methods_allow.txt` and `methods_deny.txt` files to the specified clients and servers.

`-names`
: Push the `names_allow.txt` and `names_deny.txt` files to the specified clients and servers.

`-vopie`
: Synchronize the `VOPIE` key files between the specified servers and the specified clients.

Note If none of `-methods`, `-names`, and `-vopie` is specified, all three are default.

`-methods_allow` *path_name*
: Specifies the local copy of the `methods_allow.txt` file to push to the servers and clients. If this option is not included, NetBackup uses the `/usr/openv/var/auth/methods_allow.txt` file.

`-methods_deny` *path_name*
Specifies the local copy of the `methods_deny.txt` file to push to the servers and clients. If this option is not included, NetBackup uses the `/usr/openv/var/auth/methods_allow.txt` file.

`-names_allow` *path_name*
Specifies the local copy of the `names_allow.txt` file to push to the servers and clients. If this option is not included, NetBackup uses the `/usr/openv/var/auth/methods_allow.txt` file.

`-names_deny` *path_name*
Specifies the local copy of the `names_deny.txt` file to push to the servers and clients. If this option not included, NetBackup uses the `/usr/openv/var/auth/methods_allow.txt` file.

`-clients [` *client1 client2 ... clientN* `]`
Names the clients to update. If `-clients` is specified without listing any client names, all unique client names in the NetBackup catalog are updated. A client name can also be specified in this format:

name:*host*

Where *name* is the client name and *host* is the network host name of the client. This is useful for specifying NetBackup clients that use dynamic network addressing like DHCP.

`-servers [` *server1 server2 ... serverN* `]`
Names the servers to update.

If `-servers` is specified but no server names are listed, all server names in the NetBackup configuration are updated.

Note The following cases also apply to using the `-clients` and `-servers` options:

If neither `-clients` nor `-servers` is used, all clients and all servers are updated.

If `-servers` is used but `-clients` is not, no clients are updated.

If `-servers` is not used but `-clients` is used along with `vopie` (either specifically or by default), the local server is updated.

If `-servers` is not used but `-clients` is used along with `-names` or `-methods`, no servers are updated.

FILES

`/usr/openv/netbackup/logs/admin/log.*`

`/usr/openv/var/auth/methods.txt`

`/usr/openv/var/auth/methods_allow.txt`

```
/usr/openv/var/auth/methods_deny.txt
/usr/openv/var/auth/names_allow.txt
/usr/openv/var/auth/names_deny.txt
/usr/openv/var/auth/vopie/*
```

SEE ALSO

vopied(1M),vopie_util(1M)

bpbackup(1)

NAME

bpbackup - Back up files to the NetBackup server.

SYNOPSIS

```
/usr/openv/netbackup/bin/bpbackup [-p policy] [-s schedule] [-S
        master_server [,master_server,...]] [-t policy_type] [-L
        progress_log [-en]] [-w [hh:mm:ss]] [-help] [-k
        "keyword_phrase"] -f listfile | filenames

/usr/openv/netbackup/bin/bpbackup -i [-p policy] [-h hostname] [-s
        schedule] [-S master_server [,master_server,...]] [-t
        policy_type] [-L progress_log [-en]] [-w [hh:mm:ss]] [-k
        "keyword_phrase"]

/usr/openv/netbackup/bin/bpbackup -dssu storage unit name
```

DESCRIPTION

bpbackup starts either of the following processes:

On clients

Using the first form of the command above, bpbackup starts a user backup that is the equivalent to what is performed by using the interface on the client. This type of backup can be started from any NetBackup client in order to back up files from that client.

The bpbackup command 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 or directory name. If the named files include a directory, bpbackup backs up all files and subdirectories of that directory starting at the directory itself.

On master servers

Using the second form of the command shown above, bpbackup starts an immediate-manual backup of a client. This variation requires the -i option on the bpbackup command and is available only to the administrator on the master server. It is the equivalent of starting a manual backup from the NetBackup administrator's interface. Use the -h option to specify the host.

Since progress logs are written only on clients, and since this form of the bpbackup command 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 directories owned by other users if you have the necessary permissions.
- If you specify a UNIX 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 are returned 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 and returns completion status after a specified time period.

`bpbackup` writes informative and error messages to a progress-log file if you create the file prior to running the `bpbackup` command and then specify the file with the `-L` *progress_log* option. If `bpbackup` cannot back up the requested files or directories, use the progress log to determine the reason for the failure.

If you create a directory named `/usr/openv/netbackup/logs/bpbackup/` with public-write access, `bpbackup` creates a debug log file in this directory that can be used for troubleshooting.

In addition, if a nonroot user specifies `USEMAIL =` *mail_address* in their `$HOME/bp.conf` file or a root user specifies it in the `/usr/openv/netbackup/bp.conf` file, NetBackup sends mail on the backup completion status to *mail_address*. This message is sent when the backup process is complete.

OPTIONS

`-p` *policy*

Names the policy to use for the backup.

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

The `-p` option is required for an immediate-manual backup (`-i` option).

`-i`

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

`-dssu` *storage unit name*

NetBackup manually starts an immediate running of the schedule associated with the disk staging storage unit. The `-i` option is the implied behavior and therfore is not necessary.

`-h` *hostname*

It 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.

`-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 it is using (see the `-p` option).

`-S` *master_server* `[,` *master_server*`,...]`

Specifies the name(s) of the NetBackup master server(s). The default is the first `SERVER` entry found in the `/usr/openv/netbackup/bp.conf` file.

`-t` *policy_type*

Specifies one of the following numbers corresponding to the policy type. The default for NT clients is `13`,for Netware clients the default is `10`, and the default for all others is `0`:

`0` = Standard

`4` = Oracle

`6` = Informix-On-BAR

`7` = Sybase

`10` = NetWare

`13` = MS-Windows-NT

`14` = OS/2

`15` = MS-SQL-Server

`16` = MS-Exchange-Server

`19` = NDMP

Note The following policy types apply only to NetBackup Enterprise Server.

`11` = DataTools-SQL-BackTrack

`17` = SAP

`18` = DB2

`20` = FlashBackup

`21` = Split-Mirror

`22` = AFS

`-L` *progress_log* `[-en]`

Specifies the name of a file in which to write progress information. NetBackup creates the file if it doesn't exist.

For example: `/home/tlc/proglog`

The default is to not use a progress log.

Include the `-en` option to generate a log in English. The name of the log will contain the string `_en`. This option is useful to support personnel assisting in a distributed environment where differing locales may create logs of various languages.

`-w` [*hh:mm:ss*]

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

The date and time format depend on the user's locale. See NOTES.

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.

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

If you include `-i` with `-w`, NetBackup waits until all initiated jobs have completed before returning status. However, if more than one job starts, the status is unpredictable. If the multiple jobs are due to there being more than one client and the policy does not have Allow Multiple Data Streams selected, you can include the `-h` option to restrict the operation to one client and obtain predictable status. However, if the policy has Allow Multiple Data Streams selected and there is more than one job from the selected client, the status is still unpredictable.

`-help`

Prints a command line usage message when `-help` is the only option on the command line.

`-k` *keyword_phrase*

Specifies a keyword phrase that NetBackup associates with the image being created by this backup operation. You can then 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. 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.

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

`-f` *listfile*

Specifies a file (*listfile*) containing a list of files to be backed up. This option can be used instead of the *filenames* option, but cannot be used with the `-i` option. List each file on a separate line.

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

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

filepath

Where *filepath* is the path to the file you are backing up. For example:

```
/home
/etc
/var
```

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

filepathlen filepath

Where *filepath* is the path to the file you are backing up and *filepathlen* is the number of characters in the file path.

For example:

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

filenames

Names one or more files to be backed up. This option can be used instead of the `-f` option, but cannot be used with the `-i` option. Any files that you specify must be listed at the end, following all other options.

NOTES

The format that you must use for date and time values in NetBackup commands varies according to the locale setting.

If you are uncertain of the NetBackup command requirements for your locale, enter the command with the `-help` option and check the usage. The following is part of the `bpbackup` usage statement output that shows the `-w` option:

```
[-w hh:mm:ss]
```

Notice the hours:minutes:seconds requirement. These are for a locale setting of C and may be different for other locales.

For more information on locale, see the `locale`(1) man page for your system.

EXAMPLES

Example 1

To perform a user backup of a single file, enter:

```
bpbackup /usr/user1/file1
```

Example 2

The following command starts a user backup of the files that are listed in a file named `backup_list`.

bpbackup -f backup_list

Example 3

The following command (all on one line) starts an immediate-manual backup 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.

```
bpbackup -p cis_co -i -h diablo -S hoss -t 0
```

Example 4

The following command (all on one line, or using the backslash continuation character) associates the keyword phrase “Backup My Home Directory 01/01/01” to the user backup of the directory `/home/kwc`. The progress log is:

```
/home/kwc/bkup.log.bpbackup -k \"Backup My Home Directory 01/01/01"

-L /home/kwc/bkup.log  /home/kwc
```

Example 5

The following command (all on one line) associates the keyword phrase “Policy Win NT 01/01/01” to the immediate-manual backup of the client host named slater in the policy named win_nt_policy.

```
bpbackup -k "Policy Win NT 01/01/01" -i -h slater \

-p win_nt_policy -t 13
```

FILES

`$HOME/bp.conf`

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

SEE ALSO

`bp(1),bparchive(1),bplist(1),bprestore(1)`

bpbackupdb(1M)

NAME

bpbackupdb - Back up NetBackup image catalogs.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpbackupdb [-dpath disk_path]
          [-nodbpaths] [-v] [path...]

/usr/openv/netbackup/bin/admincmd/bpbackupdb [{-tpath
          tape_device_path [-m media_ID]}] [-nodbpaths] [-v] [path..
          ]

/usr/openv/netbackup/bin/admincmd/bpbackupdb [{-opath
          optical_device_path [-m media_ID]}] [-nodbpaths] [-v]
          [path...]
```

DESCRIPTION

bpbackupdb initiates a backup of one or more NetBackup image catalogs specified on the bpbackupdb command line. bpbackupdb also backs up the default set of NetBackup catalogs, unless the command line contains -nodbpaths. If the command line specifies a destination, the backup is stored there.

Otherwise, the backup is stored at the default location for backups of the NetBackup internal databases, which are called catalogs.

You can specify the default set of catalogs and the backup destination:

- The default paths to the NetBackup image catalogs are part of the NetBackup configuration. bpbackupdb uses the set of configured NetBackup catalog paths as the default value for the path option.
- The NetBackup configuration includes two destinations (media IDs or disk pathnames) for NetBackup catalog backups. bpbackupdb uses the less-recently used of the two destinations as its default value for the backup destination.

The *NetBackup System Administrator's Guide* explains how to configure and display these values.

You must have root privileges to execute this command.

Only one copy of bpbackupdb can run at a time. The bpbackupdb command fails if it determines that a NetBackup catalog backup is already running. If bpbackupdb fails because other backups are in progress, retry when no other NetBackup activity is occurring.

If `bpbackupdb` fails with the message "cannot find Internet service bpcd/tcp," then the service/protocol pair `bpcd`, `tcp` is not among the set of services defined on the local system. On UNIX, `netstat -a` displays the defined set of services. On Windows, look for a `bpcd/tcp` entry in the *install_path*`\system32\drivers\etc\services` file.

The *NetBackup System Administrator's Guide* provides additional information on backing up NetBackup catalogs. The NetBackup utility `bprecover` recovers catalogs that `bpbackupdb` has backed up. The NetBackup troubleshooting guide (UNIX version) provides information on restoring the NetBackup catalogs if a disaster recovery is required.

OPTIONS

You can either specify a list of NetBackup image catalogs with the following options or default to the catalogs specified in the NetBackup configuration:

`-dpath` *disk_path*

`-tpath` *tape_device_path*

`-opath` *optical_device_path*

`-tpath` specifies a tape raw device path as the destination for the backup.

`-opath` specifies an optical raw device path as the destination for the backup.

`-dpath` Specifies a raw disk path as the destination for the backup.

If the media for the catalog backup is non-robotic, a mount request occurs and the catalog backup waits until the mount request is either granted or denied. The `MEDIA_MOUNT_TIMEOUT` attribute does not apply to this request.

The Media Manager device and volume daemons, `/usr/openv/volmgr/bin/ltid` and `/usr/openv/volmgr/bin/vmd`, need not be active when you use one of the destination options.

Note: The table names and database names in the database pathname are case-sensitive. The database catalog backups will fail if typed without regard to case. For example:

```
host1:DB=isdb/RollUpJobSummary
```

On UNIX, NetBackup assumes it is using a Berkeley-style close device for the `-tpath` option. This is the device path with b in the device name. For example, on Solaris the device name could be `/dev/rmt/0cbn`. `bpbackupdb` will fail with an I/O error if it does not use a Berkeley-style close device on a platform that requires it. See the *Media Manager Device Configuration Guide* for more information.

If `-tpath` or `-opath` is used, the device name can be an NDMP device name. The syntax for an NDMP device name is *client*:*drivename*. An NDMP device name can contain `/` but it cannot contain `/ndmp`.

`-m` *media_ID*

This is option specifies the media ID for the NetBackup database backup. This option is meaningful when either `-tpath` or `-opath` is used. Media Manager uses the media ID for removable media to verify that the correct media is mounted. The media ID string length is between one and six characters and the string can be either uppercase or lowercase.

`-help`

Prints a command line usage message when `-help` is the only option on the command line.

`-nodbpaths`

Do not back up the configured NetBackup catalogs. If this option is present, you must specify at least one catalog path on the command line. If this option is absent, `bpbackupdb` backs up the catalogs configured by NetBackup for catalog backups, as well as any catalog listed by the *path* option.

`-v`

Selects verbose mode. This option causes `bpbackupdb` 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 debug logging enabled (`/usr/openv/netbackup/logs/admin` directory defined).

path...

Back up these NetBackup catalogs. This is a list of absolute pathnames. The catalog backup paths must not contain any soft links. When NetBackup backs up its catalogs, it does not follow soft links. If you have moved any of the catalog files or directories and created soft links to their new locations, you must delete any path that has a link in it and add the actual path. Otherwise, the catalog backup aborts.

To back up a NetBackup catalog on the master server, specify the catalog backup path as an absolute pathname, for instance, `/usr/openv/volmgr/database`.

To back up a NetBackup catalog on a media server other than the master server (this configuration is supported only by NetBackup Enterprise Server), specify the catalog backup path as *hostname*:*pathname*. For instance, *`hostname:`*`/usr/openv/volmgr/database`.

There must be at least one path specified if `-nodbpaths` is present.

RETURN VALUES

An exit status of 0 means that the backup ran successfully.

Any exit status other than 0 means that an error occurred.

EXAMPLES

These examples assume that NetBackup has been configured so that `bpbackupdb` can use the default values for catalogs and destination.

Example 1

The following example backs up the NetBackup catalogs

```
bpbackupdb
```

If the backup succeeds, the NetBackup mail administrator receives an email that contains the details of the backup.

If the backup fails, the NetBackup mail administrator receives an email that contains the reason for the failure.

Example 2

The following example backs up the NetBackup catalogs to the tape device `/dev/rmt/0mbn`.

```
bpbackupdb -tpath /dev/rmt/0mbn
```

MESSAGES

If `bpbackupdb` succeeds, it logs one of the following messages:

NB database backup to path *destination* SUCCEEDED

NB database backup to media id *destination* SUCCEEDED

NB database backup SUCCEEDED

If `bpbackupdb` fails, it logs one of the following messages:

NB database backup to path *destination* FAILED

NB database backup to media id *destination* FAILED

NB database backup FAILED

`bpbackupdb` also sends mail to the NetBackup administrator reporting the results of the backup.

FILES

`/usr/openv/netbackup/db/*`

`/usr/openv/netbackup/logs/admin/log.`*mmddyy*

```
/usr/openv/volmgr/database/*
```

SEE ALSO

bpadm(1M),bprecover(1M),netstat(1M),services(4)

bpcatarc(1M)

NAME

`bpcatarc` - Back up NetBackup catalog.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpcatarc [-version] [-help]
```

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.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-version`
: Display the `bpcatarc` version and exit.

`-help`
: Display the help text.

SEE ALSO

`bpcatlist(1M), bpcatres(1M), bpcatrm(1M)`

bpcatlist(1M)

NAME

`bpcatlist` - List selected parts of the NetBackup catalog.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/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] [-help] -online -offline
```

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 wish to work. All files-file (also called image .f files), the largest files in a NetBackup catalog, selected for `bpcatarc`, `bpcatres`, or `bpcatrm`, are first selected with `bpcatlist`. The output of `bpcatlist` is piped to the action you wish to perform.

OPTIONS

`-server` *server_name*

Indicate the name of the NetBackup server. Default: *server_name* is the first SERVER name listed in the `bp.conf` file.

`-client` *client_name*

Create 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*]]

List backup images since the specified time expressed in ctime (for example, `Fri Sep 13 00:00:00 2002`).

If no year is specified, `bpcatlist` uses the current year by default.

The following command lists all images after December 31, 2002:

```
bpcatlist -since 2002
```

Additional examples are found in the following “Examples” section.

`-before` [*ctime* | [`-since-days` *nnn* | `-since-weeks` *nnn* | `-since-months` *nnn* | `-before-days` *nnn* | `-before-weeks` *nnn* | `-before-months` *nnn*]]
List backup images before the specified time expressed in ctime (for example, `Fri Sep 13 00:00:00 2002`). If no year is specified, `bpcatlist` uses the current year by default. For example:

`-date` *ctime*
List of backup images for the specified date expressed in ctime (for example, `Fri Sep 13 00:00:00 2002`). If no date is specified, `bpcatlist` uses the current date by default.

Additional examples are found in the following "Examples" section.

`-catarc` *catarc_id*
List the files-file that were archived with the specified *catarc_id*. For example:

```
-catarc 1022754972
```

`-policy` *policy_name*
List the backups created by the indicated *policy_name* for the specified client.

`-sched` *sched_name*
List the backups created following *schedule_name* for the specified client.

`-id` *backup_id*
Create a list for the specified *backup_id*.

`-online`
List only files-file that are online.

`-offline`
List only files-file that are offline.

`-version`
Display the `bpcatlist` version and exit.

`-help`
Display the help text.

EXAMPLES

Dates are displayed and must be specified in ctime() date format. Displayed dates may be cut and specified without modification.

To list a backup for a specific date and time, specify:

```
bpcatlist -date Mon Sep 16 14:16:28 2002
```

(When no year is specified, the current year is used by default.)

To list all backups between two dates of the current year, specify:

```
bpcatlist -before Mon Sep 10 00:00:00 2002 -since Fri Oct 4
00:00:00 2002
```

To list backups that are two to three months old, specify:

```
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 following setting: `-since-days 14`

is equivalent to: `-since-weeks 2`

SEE ALSO

`bpcatarc(1M), bpcatres(1M), bpcatrm(1M)`

bpcatres(1M)

NAME

`bpcatres` - Restore NetBackup catalog.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpcatres [-version] [-help]
```

DESCRIPTION

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

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-version`
: Display the `bpcatres` version and exit.

`-help`
: Display the help text.

SEE ALSO

`bpcatarc(1M), bpcatlist(1M), bpcatrm(1M)`

bpcatrm(1M)

NAME

`bpcatrm` - Delete NetBackup catalog

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpcatrm [-version] [-help]
```

DESCRIPTION

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

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-version`
: Display the `bpcatrm` version and exit.

`-help`
: Display the help text.

SEE ALSO

`bpcatarc(1M), bpcatlist(1M), bpcatres(1M)`

bpcd(1M)

NAME

`bpcd` - NetBackup client daemon. Enables NetBackup clients and servers to accept requests from NetBackup servers.

SYNOPSIS

```
/usr/openv/netbackup/bin/bpcd [-standalone] [-debug] [-portnum
         number] [-keyfile] [-restrict_if host_or_ip]
```

DESCRIPTION

bpcd is communications daemon that is activated by the NetBackup Client Service bpinetd(1M) on Windows systems. Typically, bpcd is activated by inetd(1M) on UNIX systems.

The bpcd daemon accepts requests from NetBackup servers. Requests include initiating backup and restore jobs and getting and setting NetBackup configuration parameters.

When you install NetBackup on a Windows client, the installation process adds entries for bpcd to `C:\WINNT\system32\drivers\etc\services`.

When you install NetBackup on a UNIX client, the installation process typically adds entries for bpcd to `/etc/services` and `/etc/inetd.conf`.

The `services` entry looks like this:

```
bpcd 13782/tcp       bpcd
```

The `inetd.conf` entry on UNIX looks like this:

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

OPTIONS

`-standalone`
: Available only on UNIX clients and specifies that `bpcd` will run continuously rather than being started by `inetd`.

`-debug`
: Available only on UNIX clients and implies `-standalone`. This option prevents `bpcd` from forking and does not disconnect it from standard input, output, and error.

`-portnum` *number*
: Available only on UNIX clients and implies `-standalone`. Specifies the port number where `bpcd` listens for requests. The default is the `bpcd` entry in: `/etc/services`.

`-restrict_if host_or_ip`

Available only on UNIX clients and implies `-standalone`. Specifies the local network interface that `bpcd` will accept connections from. Default is to accept connections from all local network interfaces. You can specify either a host name or an IP address.

`-keyfile`

Available only on UNIX clients and implies "-standalone". When specified, you will be prompted for the NetBackup key file pass phrase that will allow bpcd to access the NetBackup encryption key file. See the section "Additional Key File Security (UNIX clients only)" in the *VERITAS NetBackup Encryption System Administrator's Guide* for additional information.

SEE ALSO

`bpclient(1M),bpkeyfile(1M)`

bpchangeprimary(1M)

NAME

`bpchangeprimary` - Promote a copy of a backup to be the primary copy.

SYNOPSIS

`/usr/openv/netbackup/bin/admincmd/bpchangeprimary -copy` *number* | `-pool` *volume_pool* | `-group` *volume_group* `[-id` *backup_id*`]` `[-M` *master_server*`]`

`/usr/openv/netbackup/bin/admincmd/bpchangeprimary -copy` *number* | `-pool` *volume_pool* | `-group` *volume_group* `[-sl` *schedule_name*`]` `[-pn` *policy_name*`]` `[-st` *schedule_type*`]` `[-pt` *policy_type*`]` `[-cl` *client_name*`]` `[-kw` *keyword*`]` `[-sd` *date*`]` `[-ed` *date*`]` `[-M` *master_server*`]`

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 has been sent offsite, change the primary copy to be the copy that remains on site.

The bpchangeprimary command finds all backups that match the specified criteria, and for those images found, 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 and changes to primary, all copies that reside on those media.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

One of the following three options is required; using one precludes use of the others.

`-copy` *number*

Specifies that *copy_number* is the number of the backup copy you want to promote to primary.

`-pool` *volume_pool*
: Specifies that the copy that is on media belonging to *volume_pool* should be promoted to primary.

`-group` *volume_group*
: Specifies that the copy that is on media belonging to *volume_group* should be promoted to primary.

Combinations of one or more of the following criteria can be applied to specify which copies will be made primary. None of the following options are required.

`-cl` *client_name*
: Specifies that backups of *client_name* will be affected. For those backup images, the copy that corresponds to the specified `-pool`, `-group`, or `-copy` option will be promoted to primary. The default is all clients.

`-sd` *date*

`-ed` *date*
: Specifies the start date (`-sd`) or end date (`-ed`) of the backup images for which the primary copy will be changed.

  The default start date is January 1, 1970, effectively causing a search for all images. If you run `bpchangeprimary` without using the `-sd` option, you are prompted for confirmation that you want to change the primary copy for backups created after January 1, 1970.

  The format of date depends on the user's locale setting. See the NOTES section for more information. For the C locale, the date syntax is as follows:

  mm/dd/yy [hh[:mm[:ss]]]

  The default end date 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.

`-id` *backup_id*
: Specifies the backup id of the backup image for which the primary copy will be changed. For that backup image, the copy that corresponds to the specified `-pool`, `-group`, or `-copy` option will be changed.

  If you specify this option, you can specify an alternate master server (using the `-M` option). You must specify one of `-pool`, `-group`, or `-copy`. No other options are used with `-id`.

`-kw` *keyword_phrase*
: Specifies a keyword phrase for NetBackup to use when identifying backup images for which the primary copy will be changed.

`-M` *master_server*

Specifies that backups belonging to *master_server* will be affected. For those backup images, the copy that corresponds to the specified `-pool`, `-group`, or `-copy` option will be promoted to primary.

If you use this option, then any other options you specify determine which backup images on the specified master server will be affected. The *master_server* must allow access by the system issuing the `bpchangeprimary` command. The default is the master server for the system running the `bpchangeprimary` command.

`-pn` *policy_name*

Specifies the name of the backup policy of the backups for which the primary copy will be changed. The default is all policies.

`-pt` *policy_type*

Specifies the type of the backup policies of the backups for which the primary copy will be changed. The default is all policy types.

The *policy_type* is one of the following character strings:

`Informix-On-BAR`

MS-Exchange-Server

MS-SQL-Server

MS-Windows-NT

NetWare

Oracle

OS/2

Standard

Sybase

NDMP

The following policy types apply only to NetBackup Enterprise Server.

AFS

Auspex-FastBackup

DataTools-SQL-BackTrack

DB2

FlashBackup

SAP

Split-Mirror

`-sl` *schedule_name*

Specifies the *schedule name* (label) for the selection of the backup images for which the primary copy will be 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 will be changed.

By default, the `bpchangeprimary` command uses any schedule type. Valid vales 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)

NOTES

The format that you must use for date and time values in NetBackup commands varies according to your locale setting.

If you are uncertain of the NetBackup command requirements for your locale, enter the command with the `-help` option and check the USAGE. For example, the following is the output for the `-sd` and `-ed` options:

```
[-sd mm/dd/yyyy HH:MM:SS] [-ed mm/dd/yyyy HH:MM:SS]
```

Notice the month/day/year and hours:minutes:seconds requirements. These are for a locale setting of C and can be different for other locales. See the `locale`(1) man page for detailed information.

EXAMPLES

Example 1

The following command will promote all copies on media belonging to the volume pool, SUN, created after 08/01/2003 to be the primary copy.

```
bpchangeprimary -pool SUN -sd 08/01/2003
```

Example 2

The following command will promote copy 2 of all backups of client, oak, created after 01/01/2003 to be the primary copy:

```
bpchangeprimary -copy 2 -cl oak -sd 01/01/2003
```

Example 3

The following command will promote copy 4 of all backups that were created by the backup policy, Offsite, after 08/01/2003 to be the primary copy:

```
bpchangeprimary -copy 4 -pn Offsite -sd 08/01/2003
```

bpclient(1M)

NAME

`bpclient` - Manage client entries on a master server.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpclient [-All] [-M
        master_server] [-L|-H]

/usr/openv/netbackup/bin/admincmd/bpclient -client client_name
        [-M master_server] [-L|-H]

/usr/openv/netbackup/bin/admincmd/bpclient -client client_name
        [-M master_server] -add|-update[-connect_nr_port 0|1]
        [-no_callback 0|1][-dynamic_address 0|1][-current_host
        host_name [:ip_address]|:ip_address][-free_browse
        0|1|2][-list_restore 0|1|2|3][-max_jobs [1-99]]

/usr/openv/netbackup/bin/admincmd/bpclient -client client_name
        [-M master_server] -delete
```

OPTIONS

`-add`
: Add a new client entry.

`-All`
: List all client entries. Only client entries added explicitly using the `bpclient` command are displayed.

`-client` *client_name*
: Where *client_name* is the name of the client to list or update.

`-connect_nr_port 0|1`
: `0` = Connect to the client's `bpcd` using a reserved (less than 1024) port number (default).

  `1` = Connect to the client's `bpcd` using a non-reserved port number. If you select this option, enable **Allow Nonreserved Ports** for the selected client. (See the Universal Settings dialog under **Host Properties** > **Clients**.)

`-current_host` *host_name*`[:`*ip_address*`]|:`*ip_address*
: The host name/IP address of the client. This is only meaningful in the situation where the option `-dynamic_address 1` is used. Usually, you do not have to enter a `-current_host` value. The client normally contacts the master server to set the host name/IP address.

`-delete`

Delete 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).

`-free_browse 0|1|2`

`-free_browse` is a method that allows users to get around the checking that the server does when browsing images (owner/group). By default, normal users are not allowed to browse into scheduled backups on NT.

`0` = Allow

`1` = Deny

`2` = Use

By default, both the client and the server should be set up to `0` (allow). In order to free browsing to occur, either the client or the server must be setup to `2` (use) and neither can be setup for `1` (deny).

`-H`

List host specific client information.

`-L`

List all client information.

`-M` *master_server*

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

`-no_callback 0|1`

`0` = When connecting to the client's `bpcd`, the client connects back to the server on a random port number (default).

`1` = When connecting to client's `bpcd`, the client connects back to the server on the `vnetd` port number.

`-list_restore 0|1|2|3`

`-list_restore` can be set up on the server to disallow list and/or restore requests from a particular client. The value that is found 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

`-max_jobs [1-99]`
: Specify the maximum number of jobs allowed to run concurrently on this client, up to 99. This item can be configured in the NetBackup-Java Administration Console and is labeled “Maximum data streams”. To perform this function using this GUI, select the following: Host Properties > Master Servers > (double-click the master server name) > Client Attributes > Then select the client.

`-update`
: Update an existing client entry.

NOTES

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator’s Guide*.

bpconfig(1M)

NAME

`bpconfig` - Modify or display the global configuration attributes for NetBackup.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpconfig [-cd seconds] [-ha
        hours] [-kl days] [-kt days] [-ma address] [-mdtm drives]
        [-mj number] [-period hours] [-prep hours] [-to seconds]
        [-max_copies 2...10] [-tries times] [-wi minutes] [-v] [-M
        master_server, ...]

/usr/openv/netbackup/bin/admincmd/bpconfig [-L | -l | -U] [-v]
        [-M master_server, ...]
```

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 should be adequate for most installations. The section on NetBackup Global Attributes, in the *NetBackup System Administrator's Guide* describes the implications of setting the attribute values.

- 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 the section DISPLAY FORMATS for more detail on the displays.

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

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-cd` *seconds*

The number of seconds that is the Compress-image-Database time interval. When seconds is a positive integer, an image will be compressed after this number of seconds has elapsed since the creation of the image. On Windows NT, NetBackup uses NTFS file compression only if the database is in an NTFS partition. Otherwise, it is not compressed.

The effect of compression is that less disk space is needed for the image database. However, when browsing the image database for restoring, the images need to be decompressed before they can be searched. While browsing for a restore, the compressed images will not be found. To decompress the images, you must use bpimage(1M).

The default is 0, which means no compression is done.

`-mdtm` *drives*

The maximum drives for this master, the maximum number of drives for this master and remote media server cluster that the master server should consider available when scheduling backups. An appropriate value for this attribute is the physical number of drives, counting shared drives only once, in the master and media server cluster. *drives* must be less than or equal to the number permitted by the version of NetBackup that is installed on the server (that is, 2 for NetBackup Server and unlimited for NetBackup Enterprise Server). *drives* is a non-negative integer. The default is 0 (unlimited).

`-ha` *hours*

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 instance, if *hours* ago is 24 and if you request a Backup Status report at 10:00 a.m., the report includes all backups run 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. The default value is 24 hours.

`-kl` *days*

The number of days to keep logs. This 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, so this value limits the period that these reports can cover. The default is 28 days.

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 determines how long to keep TIR information for those policies that have specified that TIR information is to be collected. The default is 1 day.

`-L`

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

`-l`

The list type is short. This 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,...*

A list of master servers. This 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 issuing the command. If an error occurs for any master server, processing stops at that point in the list. The default is the master server for the system where the command is entered.

`-ma` *address*

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

If no address is provided, the current setting of the Admin Mail Address is cleared. This means that notification no longer will be sent by email to the NetBackup administrator.

`-max_copies` *2...10*

Specify the maximum number of copies per backup. Copies can range from between 2 and 10. The default is 2.

`-mhto` *seconds*

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

`-mj` *number*

Specifies the maximum jobs per client. This is the maximum number of jobs that a client may perform concurrently. number must be a positive integer. The default is 1.

`-period` *hours*

The time interval associated with the configured number of tries for a backup (see `-tries`). This is the period, in hours, during which NetBackup will attempt a backup job for a client/policy/schedule combination for as many tries as configured. hours must be a positive integer. The default is 12 hours.

Note This attribute does not apply to user-directed backups and archives.

`-prep` *hours*

The preprocessing interval. This is the minimum time in hours between client queries to discover new paths if NetBackup is using auto-discover-streaming mode. For additional information, see the "Setting the Preprocess Interval for Auto Discovery" section in the topic on File-List Directives for Multiple Data Streams in the *NetBackup System Administrator's Guide*.

The default Preprocessing Interval value is 4 hours. If the preprocessing interval is changed, it can be changed back to the default by specifying `-prep -1`.

The preprocessing interval can be set for immediate preprocessing by specifying `0` as the preprocess interval for auto discovery on the `bpconfig` command line.

The maximum Preprocessing Interval is 48 hours.

`-to` *seconds*

This is the media-mount timeout, the length of time, in seconds, that NetBackup waits for the requested media to be mounted, positioned, and become ready on backups and restores. Use this timeout to eliminate excessive waits when it is necessary to manually mount media (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 must be 300 (5 minutes) or greater.

`-tries` *times*

The number of retries for a backup, during the configured time period (see `-period`). NetBackup tries to run a backup job for a given client/policy/schedule combination this many times in the configured period. This allows you to limit the number of backup attempts should repeated failures occur.

Note This attribute does not apply to user-directed backups and archives.

Usually the number of tries should be greater than 0. Specifying 0 for the number of tries is legal but stops all scheduled backups. The default is 2 tries. If defaults are used for both `-tries` and `-period`, NetBackup will attempt the backup 2 times in 12 hours.

`-U`

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

`-v`

Select verbose mode for logging. This is only meaningful when running with debug logging turned on (the `/usr/openv/netbackup/logs/admin` directory is defined).

`-wi` *minutes*

This is the wakeup Interval, the length in time in minutes that the scheduler waits before checking if any automatic backups are scheduled to begin. A long wakeup interval can cause the scheduler to miss too much of the backup window to complete its backups. The default is 10 minutes.

DISPLAY FORMATS

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

- User Display Format (`-U`)

If the command line contains `-U`, the display format is user. The user display format is the format used by `bpadm` and the NetBackup graphical-user interfaces. This option produces a listing with one global attribute per line. Each line has the form *global attribute descriptor*: *value*. This listing is similar to the `-L` format, except that the global attribute descriptors are more explicit:

Admin Mail Address

Wakeup Interval

Max Simultaneous Jobs/Client

Backup Tries (x tries in y hours)

Keep Error/Debug Logs

Max drives this master

Keep TrueImageRecovery Info

Compress Image DB Files

Maximum Backup Copies

Media Mount Timeout

Display Reports

Preprocess Interval

- Long Format (`-L`)

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

Mail Admin

Wakeup Interval

Max Jobs/Client

Backup Tries (x in y hours)

Keep Logs

Max drives/master

Compress DB Files

Maximum Backup Copies

Media Mnt Timeout

Postprocess Image

Display Reports

Keep TIR Info

Prep Interval

- Short Format (`-l`)

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

NetBackup administrator email address

Wakeup interval (minutes)

Time period (hours)

Maximum simultaneous jobs per client

Tries per period

Keep logs (days)

Maximum drives this master

Compress image database interval (seconds; 0 denotes no compression)

Media mount timeout (seconds; 0 denotes unlimited)

Multihosted-media-mount timeout (seconds; 0 denotes unlimited)

Postprocess images flag (0 denotes deferred, otherwise immediate)

Display reports from <x> hours ago (hours)

Keep TIR information (days)

Preprocessing interval (hours)

- Example of How the Formats Differ

Here is an example of how the display formats differ. `bpconfig` runs with each of the three display formats on a NetBackup installation. The NetBackup global attributes are the same for the three displays.

The first display format, `-U`, looks like this:

```
bpconfig -U
Admin Mail Address:
Wakeup Interval:              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 Image DB Files:      (not enabled)
Media Mount Timeout:          0 minutes (unlimited)
Display Reports:              24 hours ago
Preprocess Interval:          0 hours
Maximum Backup Copies:    10
```

The second display format, `-L`, looks like this:

```
bpconfig -L
Mail Admin:          *NULL*
Wakeup Interval:     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)
Postprocess Image:   immediately
Display Reports:     24 hours ago
Keep TIR Info:       1 days
Prep Interval:       0 hours
Maximum Backup Copies: 10
```

The third display format, `-l`, looks like this:

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

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

NetBackup administrator email address has not been set

Wakeup interval 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 image database interval is 0 seconds; 0 denotes no compression

Media mount timeout is 0seconds; 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 1 day

Preprocessing interval is 0 hours

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 administrative logging is enabled, the exit status is logged in the administrative daily log under the directory `/usr/openv/netbackup/logs/admin` in the form:

`bpconfig: EXIT status =` ***exit status***

If an error occurred, a diagnostic precedes this message.

EXAMPLES

Example 1

While running on the master server kiwi, display the global attribute settings on the master server plum:

```
bpconfig -U -M plum

Admin Mail Address:           ichabod@null.null.com
Wakeup Interval:              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 Image DB Files:      (not enabled)
Media Mount Timeout:          30 minutes
Display Reports:              24 hours ago
Preprocess Interval:          0 hours
   Maximum Backup Copies:      10
```

Example 2

Set the Compress-image-database interval to 604800 seconds, so that NetBackup compresses images more than 7 days old:

```
bpconfig -cd 604800
bpconfig -U

Admin Mail Address:
Wakeup Interval:               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 Image DB Files:       older than 7 day(s)
Media Mount Timeout:           0 minutes (unlimited)
Display Reports:               24 hours ago
Preprocess Interval:           0 hours
Maximum Backup Copies:          10
```

Example 3

Set the Media Mount Timeout to 1800 seconds.

```
bpconfig -to 1800
bpconfig -U

Admin Mail Address:            sasquatch@wapati.edu
Wakeup Interval:               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
Maximum Backup Copies:          10
```

FILES

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/config/behavior`

SEE ALSO

`bpimage(1M)`

See the *NetBackup Media Manager System Administrator's Guide* for information on MultiHosted Drives.

bpdbjobs(1M)

NAME

`bpdbjobs` - Interact with the NetBackup jobs database.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpdbjobs [-report] [-M
        master_servers] [-vault | -lvault | -all_columns |
        -most_columns | -gdm] [-file pathname] [-append]
        [-noheader] [-mastertime] [-jobid job1,job2,...jobn]

/usr/openv/netbackup/bin/admincmd/bpdbjobs -summary [-M
        master_servers] [-U | -L | -all_columns] [-file pathname]
        [-append]

/usr/openv/netbackup/bin/admincmd/bpdbjobs -resume | -suspend |
        -delete | -cancel | -restart job1,job2,...jobn
        |type=jobtype|type=all [-M master_server] [-quiet]

/usr/openv/netbackup/bin/admincmd/bpdbjobs -cancel_all [-M
        master_server]

/usr/openv/netbackup/bin/admincmd/bpdbjobs -clean [-M
        master_server] [-keep_hours hours | -keep_days days]
        [-keep_successful_hours hours | -keep_successful_days
        days] [-verbose]

/usr/openv/netbackup/bin/admincmd/bpdbjobs -version

/usr/openv/netbackup/bin/admincmd/bpdbjobs -help
```

DESCRIPTION

`bpdbjobs` interacts with the jobs database and is useful in scripts or as a command line administration tool. Use `bpdbjobs` to print the entire jobs database, print a summary, delete done jobs, cancel uncompleted jobs, and clean old jobs.

It is possible to customize the output of bpdbjobs by adding column definition entries (`BPDBJOBS_COLDEFS`) in the bp.conf file. For more information about the bp.conf file and a complete list of the definitions and the `BPDBJOBS_COLDEFS` entries, refer to the *NetBackup System Administrator's Guide, Volume II.*

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-all_columns`

Summary displays all columns. Some of the more useful fields of this command are:

field2 = jobtype
(0=backup, 1=archive, 2=restore, 3=verify, 4=duplication, 5=import, 6=dbbackup, 7=vault)

field3 = state
(0=queued, 1=active, 2=requeued, 3=done)

field5 = policy
(The policy that this job is associated with.)

field6 = schedule
(The schedule that this job is associated with.)

field21 = subtype
(0=immediate, 1=scheduled, 2=user-initiated)

field24 = priority
(The priority assigned to this job, as configured in the policy attributes.)

The output of this command consists of a single line, per backup job. Each line of the output is a comma-delimited list in the following format:

```
jobid,jobtype,state,status,class,schedule,client,server,started,el
apsed,ended,stunit,try,operation,kbytes,files,pathlastwritten,perc
ent,jobpid,owner,subtype,classtype,schedule_type,priority,group,ma
sterserver,retentionunits,retentionperiod,compression,kbyteslastwr
itten,fileslastwritten,filelistcount,[files]...,trycount,[trypid,t
rystunit,tryserver,trystarted,tryelapsed,tryended,trystatus,trysta
tusdescription,trystatuscount,[trystatuslines]...,trybyteswritten,
tryfileswritten]...
```

Refer to Example 1 for an example on how to interpret the `-all_colums` output.

`-append`

Appends the output to the file specified by the `-file` option. If no `-file` option is provided, the output goes to `stdout`.

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

Causes `bpdbjobs` to cleanly cancel active jobs with a Status 150, displayed in the Activity Monitor. For example:

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

`-cancel_all`

Causes `bpdbjobs` to cleanly cancel all uncomplete jobs with a Status 150, displayed in the Activity Monitor. For example:

```
bpdbjobs -cancel_all
```

`-clean`

Causes `bpdbjobs` to delete done 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`

Causes completed jobs that are displayed in the Activity Monitor to be deleted. Multiple jobids can be deleted in one command. For example:

```
bpdbjobs -delete 11328
bpdbjobs -delete 11328,11329,11330
```

Or, delete jobs specified by *job1,job2,...jobn,* or all eligible jobs indicated by *jobtype,* or all eligible jobs if `type=all` is specified.

Enter one of the following as *jobtype*. (The letters following the capitalized letters are ignored):

```
REStore
BACkup
ARChive
DUPlicate
IMPort
LABel
VAUlt
VERify
DBbackup | CATalogbackup
```

`-file` *pathname*

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

`-gdm`

Displays less information than `-most_columns`.

`-help`

Prints a command line usage message when `-help` is the only option on the command line.

`-jobid` *job1,job2,...jobn* |`type=`*jobtype*|`type=all`

This option reports on multiple job ID's.

`-keep_days` *days*
: Use with the `-clean` option to specify how many days `bpdbjobs` keeps done jobs. Default is 3 days.

`-keep_hours` *hours*
: Use with the `-clean` option to specify how many hours `bpdbjobs` keeps done jobs. Default is 72 hours.

`-keep_successful_days` *days*
: Use with the `-clean` option to specify how many days `bpdbjobs` keeps successful done jobs. Default is 3 days.

  This value must be less than the `-keep_days` value.

`-keep_successful_hours` *hours*
: Use with the `-clean` option to specify how many hours `bpdbjobs` keeps successful done jobs. Default is 72 hours.

  This value must be less than the `-keep_hours` value.

`-L`
: Report in long format.

`-lvault`
: Displays additional columns specific to Vault jobs.

`-M` *master_servers*
: Applies to an environment where there are multiple masters servers. Use the `-M` option to:

  Summarize jobs for a specific master server.

  Delete jobid(s) for a specific master server.

  Cancel jobid(s) for a specific master server.

  Cancel all active jobids for a specific master server.

`-mastertime`
: By default, bpdbjobs translates the start/end times to be relative to the local clock so a job that starts 3 minutes ago looks like it starts 3 minutes ago regardless of any time zone and clock differences with the master server. This option circumvents that translation so time values are consistent between admin clients.

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

`-noheader`
: This option prevents the header from being printed.

`-quiet`

Use this option when you do not want to report the number of jobs resumed/suspended/deleted/canceled.

`-report`

Provides a report of data 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`

Allows bpdbjobs to cleanly restart a job indicated by the jobtype. This command 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 specified by *job1,job2,...jobn,* all eligible checkpointed backups or restore jobs indicated by *jobtype,* or all eligible jobs if `type=all` is specified.

Enter one of the following as *jobtype*. (The letters following the capitalized letters are ignored):

`REStore`

`BACkup`

`ARChive`

`DUPlicate`

`IMPort`

`LABel`

`VAUlt`

`VERify`

`DBbackup | CATalogbackup`

`-summary [-U | -L | -all_columns]`

Causes a summary line to be printed to `stdout` of all jobs 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/filename. For example:

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

`-suspend` *job1,job2,...jobn* |`type=`*jobtype*|`type=all`

Suspends the jobs specified by *job1,job2,...jobn,* or all eligible checkpointed backups or restore jobs indicated by *jobtype,* or all eligible jobs if `type=all` is specified.

Enter one of the following as *jobtype*. (The letters following the capitalized letters are ignored):

`REStore`

```
BACkup
ARChive
DUPlicate
IMPort
LABel
VAUlt
VERify
DBbackup | CATalogbackup
```

`-U`
: Report in user format. This is the report format used by NetBackup report-generating tools such as the NetBackup-Java Reports application.

`-vault`
: Displays 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: `/usr/openv/netbackup/logs/bpdbjobs/*`

`-version`
: Causes `bpdbjobs` to print the version string, then halt. Any other switches are ignored.

EXAMPLES

Example 1

The following is a sample of the logic that you can use to decode the output of the `-all_columns` option to produce the backup initiation time of a successful backup job that succeeded, but not on the first try.

Field 9 = start time (The time the job was first queued.)

This time is virtually worthless, unless you want to know when the job was queued.

Up to Field 32, all fields are fixed. Then Field 32 tells you how many entries there are in the filelist fields.

Field 32 = filelistcount (The number of files that are listed in the filelist.)

Then, if you add that value to 33, you'll get the field that shows you the number of tries.

Field 33 + filelistcount = trycount (The number of tries that have occurred.)

If there's only one try, and you want its start-time, then add 33, filelistcount + 4, and you've got the field that shows you the start-time of the first try:

Field 33 + filelistcount + 4 = [first]trystarted (The starttime of the first try.)

But, if there were _two_ tries, then you have go past the status entries. First, you need the number of entries in the status field. To get that number, add 9 to 33 and the filelistcount:

Field 33 + filelistcount + 9 = trystatuscount (The number of status entries in the first try.)

Then, to get the start-time of the second try, add 33, filelistcount, 9, trystatuscount, and 6:

Field 33 + filelistcount + 9 + trystatuscount+6 = [second]trystarted (The start-time of the second try)

FILES

`/usr/openv/netbackup/logs/bpdbjobs/*`

bpdbm(1M)

NAME

bpdbm - NetBackup database manager daemon.

SYNOPSIS

```
/usr/openv/netbackup/bin/bpdbm [-verbose] [-terminate]
```

DESCRIPTION

bpdbm responds to queries related to the NetBackup internal databases, which are called catalogs. bpdbm must be running in order 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, starts bpdbm. You can also start it with the /usr/openv/netbackup/bin/initbpdbm script.

The following events occur when bpdbm starts:

1. bpdbm logs a message indicating that it has started, and then verifies that no other instance of bpdbm is running. If another bpdbm process is found, the program terminates.

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

   ```
   bpdbm 13721/tcp
   ```

3. After binding to its port, bpdbm starts responding to queries from bprd and the NetBackup administrative utilities. A child process is created to respond to each query.

OPTIONS

-verbose
: Specifies that bpdbm will write additional information in its daily debug log for debugging purposes.

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

FILES

/usr/openv/netbackup/db/*

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

SEE ALSO

bpadm(1M),bprd(1M)

bpdgclone(1M)

NAME

bpdgclone - creates or removes clones of Volume Manager (VxVM) volumes.

SYNOPSIS

```
/usr/openv/netbackup/bin/bpdgclone [-h] [-v] [-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]
```

DESCRIPTION

For backups using the array-specific snapshot methods (EMC TimeFinder, Hitachi ShadowImage, HP BusinessCopy), where client data is configured over a Volume Manager volume, NetBackup uses the bpdgclone command to create a temporary disk group or clone of the disk(s) containing the mirror image of the volume. To avoid a naming conflict in the Volume Manager, bpdgclone names the temporary disk group as follows: 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. But if a system failure prevents NetBackup from removing the clone, you must use the bpdgclone command with the -c option to remove the clone. Then you must resynchronize the mirror disk with the primary disk.

Note If the backup has completed but the clone is not removed, subsequent backups of the client's data will fail. For assistance removing a clone, see the example below.

OPTIONS

`-g`

Specifies the name of the target disk group.

`-n`

Specifies the name of the target volume.

`-d`

Lists the primary and 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, the additional device pairs are separated by colons (:).

`-c`

Deletes the cloned disk group and volume. Note that the primary and secondary disks must be resynchronzied once the clone is deleted.

`-h`
: Prints command usage.

`-v`
: Sets 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

- A clone should not be removed while the snapshot backup using that clone is still in progress. Barring any system failures, NetBackup will remove the clone when the backup completes.
- If you use the `bpdgclone` command to remove a left over disk clone, you must resynchronize the mirror disk 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 (in this example, the actual clone would be named `clone_wil_test_clone`).

For detailed assistance, refer to"Removing a VxVM Volume Clone" in the Troubleshooting chapter of the *NetBackup Advanced Client System Administrator's Guide*.

bpduplicate(1M)

NAME

`bpduplicate` - Create a copy of backups created by NetBackup.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpduplicate -npc
        new_primary_copy -backupid backup_id [-local] [-client
        name]

/usr/openv/netbackup/bin/admincmd/bpduplicate [-number_copies
        number] [-dstunit
        destination_storage_unit_label[,copy2, . . . , copyn] [-dp
        destination_pool_name[, copy2, . . . , copyn] [-p | -pb | -PD |
        -PM] [-Bidfile file_name] [-v] [-local] [-client name]
        [-st sched_type] [-sl sched_label] [-L output_file [-en]]
        [-shost source_host] [-policy name] [-s date] [-e date]
        [-pt policy_type] [-hoursago hours] [[-cn copy_number] |
        [-primary]][-M master_server] [-altreadhost hostname]
        [-backupid backup_id] [-id media_id] [-rl
        retention_level[, rl-copy2, . . . , rl-copyn]] [-fail_on_error
        0|1[,...,0|1]] [-mpx] [-set_primary copy_index]
```

DESCRIPTION

The `bpduplicate` command allows a copy of a backup to be created. The `bpduplicate` command can also change the primary copy in order 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(1M)` command.

Use `bpduplicate` to create up to 10 copies of unexpired backups.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-altreadhost` *hostname*

Specify an alternate host from which to read the media. The default 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.

`-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 is ignored.

`-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 specified with the `-npc` option in order to change the primary copy, this indicates that NetBackup will first search for the backup ID belonging to the specified client. This 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` indicates to `bpduplicate` to search or duplicate the primary copy.

`-dp` *destination_poolname [,copy2,...,copyn]*

Specifies the volume pool for the duplicates. NetBackup does not verify that the media ID 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 specified.

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

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 specified.

`-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 prior to the current date and time.

The format of date depends on the user's locale setting. See the NOTES section for more information. For the C locale, the date syntax is as follows:

mm/dd/yy [hh[:mm[:ss]]]

`-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 other copies

Specify one for each copy specified.

`-hoursago` *hours*

Specifies number of hours prior to 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 to not use a progress file.

Include the `-en` option to generate a log in English. The name of the log will contain the string `_en`. This option is useful to support personnel assisting in a distributed environment where differing locales may create logs of various languages.

`-local`

When `bpduplicate` is initiated from a host other than master server and the `-local` option is *not* used (default), `bpduplicate` 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 the `-local` option to prevent the creation of a remote copy on the master server and to run the `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:

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 NetBackup Server master 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.

`-mpx`

Specifies that when duplicating multiplexed backups, NetBackup will create multiplexed backups on the destination media. This reduces the time to duplicate multiplexed backups.

Multiplexed duplication is not supported for:

- Non-multiplexed backups

- Backups from disk type storage units

- Backups to disk type storage units

- FlashBackup or NDMP backups

If backups in the above categories are encountered during duplication, NetBackup duplicates them first and uses non-multiplexed duplication. Then, the multiplexed backups are duplicated by using multiplexed duplication.

If all the backups in a multiplexed group are not duplicated, the duplicated multiplexed group will have a different layout of fragments. (A multiplexed group is a set of backups that were multiplexed together during a single multiplexing session.)

If this option is not specified, all backups are duplicated using non-multiplexed duplication.

For more information on multiplexing, see the *NetBackup System Administrator's Guide*.

`-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 installed, the value can only be set to 1. 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

`-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 the backups are sorted and displayed by date and time (newest to oldest).

`-PM`

Displays 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 why (for example, because the backup already has two copies). It then 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 (0 or 1):

1 = Primary copy

0 = Not primary copy

`-policy` *name*

Search for backups to duplicate in the specified policy. The default is all policies.

`-pt` *policy_type*

Search for backups created by the specified policy type. The default is any policy type.

Valid values are:

`Informix-On-BAR`

`Oracle`

`Macintosh`

`MS-Exchange-Server`

```
MS-Windows-NT
MS-SQL-Server
NDMP
Netware
OS/2
Standard
Sybase
```

Note The following policy types apply only to NetBackup Enterprise Server.

```
AFS
DataTools-SQL-BackTrack
DB2
FlashBackup
SAP
Split-Mirror
```

`-rl` *retention_level*`[,` *rl-copy2*`, . . . ,` *rl-copyn*`]`

Provides a retention level for each copy specified.

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 November 14, 2003, and its retention period is one week, the new copy's expiration date is November 21, 2003.

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 will be the primary copy

`2` = Second new copy will be the primary copy

`3` = Third new copy will be the primary copy, and so on.

copy_index cannot be greater than the `bpduplicate -number_copies` value.

If the copy specified to be the primary copy fails, but other copies are successful, the primary copy will not change from its current value.

`-shost` *source_host*
: Specifies that only the backups 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 were created by the specified schedule. The default is all schedules.

`-st` *sched_type*
: Search for backups to duplicate that were created by the specified schedule type. 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 verbose mode. When specified, the debug and progress logs include more information.

NOTES

The format that you must use for date and time values in NetBackup commands varies according to your locale setting.

If you are uncertain of the NetBackup command requirements for your locale, enter the command with the `-help` option and check the USAGE. For example, the following is the output for the `-s` and `-e` options:

```
[-s mm/dd/yyyy HH:MM:SS] [-e mm/dd/yyyy HH:MM:SS]
```

Notice the month/day/year and hours:minutes:seconds requirements. These are for a locale setting of C and can be different for other locales. See the `locale`(1) man page for detailed information.

EXAMPLES

Example 1

The following command (all on one line) lists backups with a copy number of 1, that were backed up by the policy named stdpolicy, and created between July 1, 2003, and August 1, 2003.

```
bpduplicate -PM -cn 1 -policy stdpolicy -s 07/01/01 -e 08/01/01
```

Example 2

The following command (all on one line, or using a backslash continuation character) duplicates copy 1 of the backups listed in file `/tmp/bidfile`. The destination storage unit is unit1 and the destination pool is dup_pool. Progress information is written to `/tmp/bpdup.ls`.

```
bpduplicate -dstunit unit1 -Bidfile /tmp/bidfile
-L /tmp/bpdup.ls -dp dup_pool -cn 1
```

Example 3

The following command (all on one line, or using a backslash continuation character) is the same as the prior example, except multiplexed backups are duplicated using multiplexed duplication.

```
bpduplicate -dstunit unit1 -Bidfile /tmp/bidfile
-mpx -L /tmp/bpdup.ls -dp dup_pool -cn 1
```

FILES

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/images/*`

bperror(1M)

NAME

bperror - Display NetBackup status and troubleshooting information or entries from the NetBackup error catalog.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bperror {-S | -statuscode
        status_code} [-r|-recommendation] [[-p Unx |
        NTx]|[-platform Unx | NTx]] [-v]

/usr/openv/netbackup/bin/admincmd/bperror [-all | -problems
        |-media | {-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]

/usr/openv/netbackup/bin/admincmd/bperror [-s
        {severity[+]}|severity ...] [-t 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]
```

DESCRIPTION

bperror displays information from either the same source as the online troubleshooter (in the Activity Monitor or Reports applications) or from the NetBackup error catalog. bperror 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, bperror 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/or 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 /usr/openv/netbackup/logs/admin directory. You can use the information in this directory for troubleshooting.

The output of bperror goes to standard output.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

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.

For `-all`: The type is ALL, and severity is ALL. Running `bperror` with this option and `-U` produces an All Log Entries report.

For `-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`. Running bperror with this option and `-U` produces a Backup Status report.

For `-media`: The type is MEDIADEV, and severity is ALL. Running `bperror` with this option and `-U` produces a Media Logs report.

For `-problems`: The type is ALL, and severity is the union of WARNING, ERROR, and CRITICAL. Running `bperror` with this option and `-U` produces 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 attempt 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 and end date range for the listing.

`-d` specifies a start date and time for the listing. The resulting list shows only images in back ups or archives that occurred at or after the specified date and time. The format of date depends on the user's locale setting. See the NOTES section for more information. For the C locale, the date syntax is as follows:

mm/dd/yy [hh[:mm[:ss]]]

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.

The method you use to specify the date and time is dependent on the `locale` setting for your system. See NOTES.

`-e` specifies an end date and time for the listing. The resulting list shows only files from backups or 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 end date must be greater than or equal to the start date.

`-help`

Prints a command line usage message when `-help` is the only option on the command line.

`-hoursago` *hours*

Specifies a start time of this many hours ago. This is equivalent to specifying a start time (`-d`) of the current time minus hours. Hours is an integer. The default is 24, meaning 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`

Report in long format.

`-l`

Report in short format. This produces a terse listing. This option is useful for scripts or programs that rework the listing contents into a customized report format. This is the default list type.

`-M` *master_server*

A list of master servers. This 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 issuing the command. If an error occurs for any master server, processing 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`

Display 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 using this option.

`-r | -recommendation`

Display the recommended action for the specified status code from the troubleshooting guide. The default is not to display the recommended action. The `-S` or `-statuscode` option must be specified when using this option.

`-S` *status_code*

`-statuscode` *status_code*

Display the message that corresponds to the status code. There is no default for this option.

`-s` *severity*

`-s` *severity*+

Specifies the severity of log messages to display. The defined values are `ALL`, `DEBUG`, `INFO`, `WARNING`, `ERROR`, and `CRITICAL`.

There are two ways to specify severity. 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 between the elements in the list must be a blank (" "). The second way is a single severity value with "+" appended, meaning 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 either upper or lower case.

`-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 messages logged for this server, which also satisfy the other criteria specified by `bperror` options. For instance, if `-server plum` and `-hoursago 2` are `bperror` options, the display contains messages logged for the media server plum in the past two hours.

The server name must match the server name recorded in the log messages. For instance, if the logs record the server name as `plum.null.null.com`, specifying `-server plum` will not display the logs, but `-server plum.null.null.com` will.

The query goes to the error catalog residing on the master server (either the local master server or the master server specified by -M). The master server must allow access by the system running bperror.

The default is to display log messages for all media servers 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 in either upper or lower case. The type value 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 elements in the list must be a blank (" ").

`-U`

Report in user format. This is the report format used by NetBackup report-generating tools such as the NetBackup-Java Reports application.

`-v`

Selects verbose mode. This option causes `bperror` 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 debug logging enabled (`/usr/openv/netbackup/logs/admin` directory defined). The default is not to be verbose.

DISPLAY FORMATS

- Status code display (for example, `bperror -S` *status_code*):

  `bperror` queries the NetBackup online troubleshooter on the local system for the message that corresponds to the status code. `bperror` displays the message text on one line and an explanation on a second line.

  If `-r` or `-recommendation` is an option, `bperror` also queries for the troubleshooting recommendation that corresponds to the status code. `bperror` displays the recommendation following the status message, on one or more lines.

- Error catalog display (for example, `bperror -all`; `bperror -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 returned from querying the error catalog on the master server(s). The results are limited to catalog entries that satisfy all the `bperror` options. For instance, if the `bperror` command line contains options for client, start time, and end time, then `bperror` reports only the jobs run for that client between the start and end times. For the display variant that shows individual message entries from the error catalog, the display can appear

in long (`-L`), user (`-U`), or short (`-l`) format. For the display variant that categorizes by status code, the display can appear in user (`-U`) format only. The display content for each of these formats is as follows:

- 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:

  Line 1: Date and time

  V:NetBackup version

  S:Server

  C:Client

  J:Job ID

  (U:Job group ID and an unused field) If multi-streaming is enabled for a policy, the job group ID is the job ID of the first job that spawned a collection of multi-streaming backups; if multi-streaming is disabled for the policy, the job group ID is always zero.

  Line 2: Severity (severity name and severity code in hexadecimal)

  Type (type name and type code in hexadecimal)

  Who (name of the entity that added the log entry)

  Line 3: Text (beginning of the log message text, continued on succeeding lines if necessary)

- Error catalog display, individual message entries, user format (for example., `bperror -media -U`). The user format produces a header line showing column names, and then one or more lines per log entry, with the following contents:

  Line 1: Date and time

  Server

  Client

  Text (beginning of the log message text, continued on succeeding lines if necessary)

- 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 categorized by status code. 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 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 succeeding lines if necessary)

  Line 2: The list of clients for which this status occurred.

NOTES

The format that you must use for date and time values in NetBackup commands varies according to your locale setting.

If you are uncertain of the NetBackup command requirements for your locale, enter the command with the `-help` option and check the USAGE. For example, the following is the part of the `bperror` usage output:

```
USAGE: bperror ...
            [-d mm/dd/yyyy hh:mm:ss|-hoursago hours]
            [-e mm/dd/yyyy hh:mm:ss] [-client client_name] ...
```

Notice the month/day/year and hours:minutes:seconds requirements for the `-d` and `-e` options. These are for a locale setting of C and can be different for other locales.

For more information on locale, see the `locale(1)` man page for your system.

EXAMPLES

Example 1

Here `bperror` displays 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 recommended for NetBackup status code 9.

```
bperror -d 12/23/2003 16:00:00 -e 12/23/2003 17:00:00 -t backstat -U
STATUS    CLIENT    POLICY    SCHED    SERVER    TIME COMPLETED
9         plum      dhcrypt   user     plum      12/23/2003 16:38:09
```

```
      (an extension package is needed, but was not installed)
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

Here `bperror` reports, in User format, the problems that have occurred in the previous 24 hours.

```
      bperror -U -problems
   TIME            SERVER CLIENT - TEXT
      11/23/2003 16:07:39 raisin - no storage units configured
      11/23/2003 16:07:39 raisin -  scheduler exiting - failed reading
      storage unit database information (217)
      11/23/2003 16:17:38 raisin -  no storage units configured
      11/23/2003 16:17:38 raisin -  scheduler exiting - failed reading
      storage unit database information (217)
      11/23/2003 16:26:17 raisin -  WARNING:  NetBackup database backup
      is currently disabled
      11/23/2003 18:11:03 raisin nut  bpcd on nut exited with status 59:
      access to the client was not allowed
      11/23/2003 18:11:20 raisin -  WARNING:  NetBackup database backup
      is currently disabled
```

Example 3

The following example displays status for type backstat for jobs run in the previous 24 hours. The option `-by_statcode` produces a display organized by status code.

The display shows that one or more jobs for each of the clients chives, guava, plum, and raisin completed successfully (the status code is 0). In addition, one or more jobs for client nut failed because nut did not allow access by the master or media server (the status code is 59).

```
   bperror -U -backstat -by_statcode
    0   the requested operation was successfully completed
      chives guava plum raisin
    59   access to the client was not allowed
      nut
```

Example 4

The following example identifies and retrieves 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.

```
bperror -hoursago 2002 -L | grep 'S:' | egrep 'J\:[1-9]'

12/21/2003 17:24:14 V1 S:plum C:plum J:1 (U:0,0)

12/23/2003 16:31:04 V1 S:plum C:plum J:1 (U:0,0)

12/23/2003 16:31:06 V1 S:plum C:plum J:1 (U:0,0)

12/23/2003 16:38:04 V1 S:plum C:plum J:3 (U:0,0)

12/23/2003 16:38:07 V1 S:plum C:plum J:3 (U:0,0)

12/23/2003 16:38:08 V1 S:plum C:plum J:3 (U:0,0)

12/23/2003 16:38:09 V1 S:plum C:plum J:3 (U:0,0)

01/07/2002 13:12:31 V1 S:plum C:plum J:34 (U:0,0)

01/07/2002 13:12:36 V1 S:plum C:plum J:34 (U:0,0)

01/07/2002 13:12:40 V1 S:plum C:plum J:34 (U:0,0)

01/07/2002 13:12:41 V1 S:plum C:plum J:34 (U:0,0)


bperror -d 1/7/2002 -jobid 34 -U
 TIME            SERVER CLIENT - TEXT

01/07/2002 13:12:31 plum plum  started backup job for client
plum, policy jdhcrypt, schedule user on storage unit jdhcrypt

01/07/2002 13:12:36 plum plum  begin writing backup id
plum_0947272350, copy 1,fragment 1

01/07/2002 13:12:40 plum plum  successfully wrote backup id
plum_0947272350,copy 1, fragment 1, 32 Kbytes at 11.057
Kbytes/sec

01/07/2002 13:12:41 plum plum  CLIENT plum  POLICY jdhcrypt
SCHED user EXIT STATUS 0 (the requested operation was
successfully completed)
```

Example 5

The following example shows the media entries in the error catalog for the past 2000 hours.

```
bperror -hoursago 2000 -media -U

TTIME            SERVER CLIENT - TEXT
```

```
12/23/2003 16:31:04 plum plum  Media Manager terminated during
mount of media id A00000, possible media mount timeout

12/24/2003 04:31:20 plum -  media id A00000 removed from Media
Manager database (manual deassign)
```

Example 6

The following example tallies and reports 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
```

Example 7

The following example reports the performance, in Kbytes per second, for each of today's backups:

```
bperror -all | grep Kbytes

0912013673 1 4 4 hat 0 0 0 hat bptm successfully wrote backup id
hat_0912013584, copy 1, fragment 1, 32256 Kbytes at 891.222
Kbytes/sec

0912014210 1 4 4 hat 0 0 0 hat bptm successfully wrote backup id
hat_0912014132, copy 1, fragment 1, 32256 Kbytes at 1576.848
Kbytes/sec

0912016068 1 4 4 hat 0 0 0 hat bptm successfully wrote backup id
hat_0912015780, copy 1, fragment 1, 603136 Kbytes at 2645.960
Kbytes/sec
```

Example 8

Here `bperror` displays the status message and the recommended action for status code 0:

```
bperror -S 0 -r

the requested operation was successfully completed

There were no problems detected with the requested operation.

None, unless this was a database backup performed through a
database  extension product (for example, NetBackup for Oracle
or NetBackup for  SQL Server). In those instances, code 0 means
the backup script that  started the backup ran without error.
However, you must check other  status as explained in the
related NetBackup manual to see if the  database was
successfully backed up.
```

FILES

/usr/openv/netbackup/logs/admin/log.*mmddyy*

/usr/openv/netbackup/db/error/*log files*

/usr/openv/msg/*locale*/netbackup/TrbMsgs

/usr/openv/msg/C/netbackup/TrbMsgs

/usr/openv/msg/.conf

bpexpdate(1M)

NAME

`bpexpdate` - Change the expiration date of backups in the image catalog and media in the media catalog.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpexpdate -m media_id -d date
        [-host name] [-force] [-M master_server[,...,]]

/usr/openv/netbackup/bin/admincmd/bpexpdate -deassignempty [-m
        media_id] [-host name] [-force] [-M master_server[,...,]]

/usr/openv/netbackup/bin/admincmd/bpexpdate -backupid backup_id
        -d date |0|infinity [-client name] [-copy number]
        [-force] [-M master_server[,...,]]

/usr/openv/netbackup/bin/admincmd/bpexpdate -recalculate
        [-backupid backup_id] [-copy number] -d date |0|infinity]
        [-client name] [-policy name] [-ret retention_level]
        [-sched type] [-M master_server[,...,]]
```

DESCRIPTION

NetBackup maintains internal databases with backup image and media information. These internal databases are called catalogs. Both an image record in the image catalog and a media ID in the media catalog contain an expiration date. The expiration date is the date and time when NetBackup removes the record for a backup or 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. It 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 deassigned in the Media Manager volume database, regardless of the media's prior state (FROZEN, SUSPENDED, and so on).

Changing the expiration can be done on a media ID basis or on an individual backup ID basis. Changing the expiration date of a media ID also causes the expiration date of all backups on the media to be changed. `bpexpdate` also provides options to deassign media from the media catalog if they no longer contain valid backups and to recalculate the expiration date based on the configured or a supplied retention level.

The different formats of the command are described below.

- `-m`

Changes the expiration date or removes the media ID from the media catalog and associated backups from the NetBackup catalog. A separate expiration date is maintained in the image catalog for each copy of a backup. When this format is used, only the expiration of the copy on the media is affected. If the media ID is removed from the media catalog by specifying a zero date, the media ID is also deassigned in the Media Manager volume database.

- `-deassignempty`

  Searches the catalog for removable media that no longer contain valid backups, removes it from the media catalog, and deassigns the media IDs in the Media Manager catalog. The media is then available to be used again. You can use the NetBackup Images on Media report to determine if there are assigned media that no longer contain valid backups.

- `-backupid`

  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 expiration date given by the `-d` option is greater than the current expiration of the media ID, the expiration date of the media ID in the media catalog is also changed. 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.

- `-recalculate`

  Allows the expiration date of backups to be changed based on the specified retention level or you can specify a new expiration date. When the expiration is changed according to retention level, the new date is calculated based on the creation date of the backup plus the value of the retention level. The expiration can be changed 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 date of the media ID in the media catalog is changed, providing the expiration date on this command is greater than the current expiration of the media ID.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-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, which is useful if the client name has changed.

For the `recalculate` operation, this option causes NetBackup to recalculate the expiration date 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

or

`0`

or

`infinity`

If `0` is specified, the backup or media is expired immediately. If `infinity` is specified the backup is never expired.

The format of *date* depends on the user's locale setting. See the NOTES section for more information. For the C locale, the date syntax is as follows:

mm/dd/yy [hh[:mm[:ss]]]

`-deassignempty`

Expires removable media from the media catalog when that media no longer contains valid backups and also deassigns the media ID in the Media Manager catalog.

`-force`

Prior to running the specified operation, `bpexpdate` queries before starting the operation. This option forces `bpexpdate` to carry out the operation without querying the user.

`-host` *name*

Note For NetBackup Server this option is not required because there is only one server (the master), so if you do use the option specify the host name of that server.

Specifies the host name of the server where the media catalog resides. This option is required only if the master has remote media servers and the volume was not written on the server where you run the `bpexpdate`

command. In this case, the media ID is in the NetBackup media catalog on the server where the media was written and you must specify the name of that server on the `bpexpdate` command.

For example, assume you have a master server named whale and a media server named eel. You run the following `bpexpdate` command on whale in order to manually remove media ID BU0001 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*

Specifies the media ID that is affected by the expiration date change. The expiration dates of the backups on the media ID are also changed. The `-d` option must be included with this option.

This option can also be used when the `-deassignempty` option is specified to check if valid backups exist on this particular media ID. In this case, do not include the `-d` option.

The media ID must be six or less characters and must be in the NetBackup media catalog.

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

`-policy` *name*

Specifies the policy name and is valid with the `-recalculate` option. When specified, the expiration is recalculated based on the retention level for all backups created in this policy.

`-recalculate`
: Recalculates the expiration of backups based on the retention level or you can specify a new expiration date. Other options can be included in order to change the expiration for a single backup, or for all backups for a specific client name, policy name, or schedule type. Either the `-d` or `-ret` option must be specified with this option.

`-ret` *retention_level*
: Specifies the retention level to use when recalculating expiration dates and is valid with the `-recalculate` option. Levels range from 0 to 24. The new expiration date is determined by adding the configured retention level value to the backup's creation date. Either the `-backupid` or `-policy` option must be specified with this option.

`-sched` *type*
: Specifies the schedule type and is valid with the `-recalculate` option. When specified, the expiration is recalculated based on the retention level for all backups 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

The format that you must use for date and time values in NetBackup commands varies according to your locale setting.

If you are uncertain of the NetBackup command requirements for your locale, enter the command with the `-help` option and check the USAGE. For example, the following is the output for the `-d` option:

```
-d <mm/dd/yyyy HH:MM:SS | 0 | infinity>
```

Notice the month/day/year and hours:minutes:seconds requirements. These are for a locale setting of C and can be different for other locales. See the `locale`(1) man page for detailed information.

Some options in large environments can take a significant amount of time to complete. Changes that cause backups or media to expire are irrevocable; importing backups and (or) recovering previous versions of the catalogs can be required if mistakes are made using this command.

EXAMPLES

Example 1

The following command, run on the master server, removes media ID BU0002 from the media catalog, and 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

The following command changes the expiration of copy 2 of backupid eel_0904219764. The expiration of copy 1 of the backup is not affected.

```
bpexpdate -backupid eel_0904219764 -d 12/20/2003 08:00:00 -copy 2
```

Example 3

The following command removes 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

The following command checks for all media in host cat's media catalog that are still assigned but no longer contain valid backups. If any such media are found, the command removes them from the media catalog and deassigns them in the Media Manager catalog.

```
bpexpdate -deassignempty -host cat
```

FILES

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/media/*`

`/usr/openv/netbackup/db/images/*`

bpfis(1M)

NAME

bpfis - creates or deletes a snapshot, or returns information about existing snapshots.

SYNOPSIS

```
/usr/openv/netbackup/bin/bpfis create [-rhost host] [-id id]
         [-v] [-V] [-owner owner] [-help] -fim
         fim_name[:option=value,option=value, ...] file1 [file2
         ...]
```

```
/usr/openv/netbackup/bin/bpfis delete [-force] -id id
```

```
/usr/openv/netbackup/bin/bpfis query [-id id]
```

DESCRIPTION

The bpfis command can create, delete, or query snapshots of a client system (filesystem or volume).

Note To store the image on tape or other media requires running a separate backup job.

For more detailed examples and procedures for using bpfis, refer to the *NetBackup Advanced Client System Administrator's Guide*.

You must have root privileges to execute this command.

OPTION

`-rhost`

The remote host or alternate client on which the snapshot is made accessible. The default is the local host. -rhost can be used with the FlashSnap, VVR, TimeFinder, BusinessCopy, and ShadowImage methods only.

`-id`

For bpfis create, this is a user-defined snapshot identifier. The default id is a time stamp showing when the image was created.

For bpfis delete, this designates the ID of the snapshot to be deleted. For bpfis query, this is the ID of the snapshot for which to return information.

`-v -V`

Indicates verbosity levels in the log files. -V is a higher level of verbosity than -v. Default is non-verbose.

`-owner`

owner of this snapshot (default is GENERIC).

`-help`
: Displays bpfis usage statement.

`-fim` *`fim_name`*`[:option=`*`value`*`,option=`*`value`*`, ...]`
: This is a required parameter. It specifies the snapshot method to use when creating the image. Valid methods are: FlashSnap, NAS_Snapshot, VxFS_CheckPoint, VxFS_Snapshot, VVR, vxvm, nbu_snap, fsclone, TimeFinder, BusinessCopy, ShadowImage.

  Select the method based on the type of data and hardware used by the client. Refer to the *NetBackup Advanced Client System Administrator's Guide* for details on each of these snapshot methods.
  The available options depend on the snapshot method. For a list of the options, refer to the `<opt_params>` area of each snapshot method (FIM) listed in the `/usr/openv/vfm.conf` file. For example, under the BusinessCopy snapshot method, the first optional parameter is listed as follows:

  ```
  keep_fi=%b[0]#Keep frozen image after backup
  ```

  where `keep_fi=` is the option, and the value is boolean (0 for no, 1 for yes). For an example of the bpfis command using option=value, refer to bpfis in the *NetBackup Advanced Client System Administrator's Guide*.

`file1 file2`
: Specify the path of the filesystem or volume from which the snapshot is to be made.

`-force`
: Specifies force delete.

EXAMPLES

◆ Example 1

To create a snapshot of `/mnt/ufscon` on hostB using the FlashSnap method on a UNIX client:

```
/usr/openv/netbackup/bin/bpfis create -rhost hostB -fim FlashSnap
/mnt/ufscon
```

Sample output:

```
INF - BACKUP START 26808

INF - FIS_ID=1034037338

INF - REMAP FILE BACKUP /mnt/ufscon USING
/tmp/_vrts_frzn_img_26808/mnt/ufscon
OPTIONS:ALT_PATH_PREFIX=/tmp/_vrts_frzn_img_26808,FITYPE=MIRROR
,MNTPOINT=/mnt/ufscon,FSTYPE=ufs
```

```
INF - EXIT STATUS 0: the requested operation was successfully
completed
```

Example 2

To obtain information about a particular snapshot on the local host:

```
/usr/openv/netbackup/bin/bpfis query -id 1034037338
```

Sample output (on a UNIX client):

```
INF - BACKUP START 26838

INF - Frozen image host : ricochet

INF - Frozen image owner: GENERIC

INF - Time created      : Mon Oct  7 19:35:38 2002

INF - REMAP FILE BACKUP /mnt/ufscon USING
/tmp/_vrts_frzn_img_26808/mnt/ufscon
OPTIONS:ALT_PATH_PREFIX=/tmp/_vrts_frzn_img_26808,FITYPE=MIRROR
,MNTPOINT=/mnt/ufscon,FSTYPE=ufs

INF - EXIT STATUS 0: the requested operation was successfully
completed
```

Example 3

To delete a snapshot on the local host:

```
/usr/openv/netbackup/bin/bpfis delete -id 1034037338
```

Sample output:

```
INF - BACKUP START 26839

INF - EXIT STATUS 0: the requested operation was successfully
completed
```

bpgetconfig(1M)

NAME

bpgetconfig - A helper program for backuptrace and restoretrace to obtain configuration information.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpgetconfig -M master [-x|X]
        ["config_item" ...]

/usr/openv/netbackup/bin/admincmd/bpgetconfig [-u|h] [-x|X]
        ["config_item" ...]

/usr/openv/netbackup/bin/admincmd/bpgetconfig -g "server"
        [-L|U|l]

/usr/openv/netbackup/bin/admincmd/bpgetconfig -s "server"
        [-L|U|l]

/usr/openv/netbackup/bin/admincmd/bpgetconfig -H [config_item]
```

DESCRIPTION

The bpgetconfig command can be used as a standalone program or as a helper program for the backuptrace and restoretrace commands to obtain configuration information. This command is available for all NetBackup server platforms. This command is used to display the configuration information of a specified server in various formats.

You must have root privileges to execute this command.

OPTIONS

`-M` *`master`*
: Specifies the master server (*master*) whose host configuration will be displayed.

`-h`
: Displays the default, local host configuration.

`-u`
: Displays the current user configuration.

`-x`
: Excludes items not explicitly listed in the 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 onthe commend line.

"config_item"...

If the *config_item* is specified, it displays on the specified configuration items.

`-g` *server*

This option selects the host server (*server*) for which general Backup Exec and NetBackup information will be displayed. Currently:

Master or Client

NetBackup Client Platform

NetBackup Client Protocol Level

Product Type (for Backup Exec if installed, else NetBackup)

Version Name (for Backup Exec if installed, else NetBackup)

Version Number (for Backup Exec if installed, else NetBackup)

Installed Path for NetBackup Bin (null if Backup Exec installed)

Installed OS for host server

`-s` *server*

This option selects the host server (*server*) for which general NetBackup specific system information will be displayed. Currently:

Master or Client

NetBackup Client Platform

NetBackup Client Protocol Level

Product Type (NetBackup)

Version Name

Version Number

Installed Path for NetBackup Bin

Installed OS for host server

`-L`

Displays a long user readable listing.

`-U`

Displays a brief user readable listing (default).

`-l`

Displays a compact machine readable listing. The -L, -U, and -l options may be used with the -g or -s option.

`-H`
: Displays the help screen.

`-H config_item`
: Displays the vaild configuration items.

bpgetdebuglog(1M)

NAME

bpgetdebuglog - helper program for backuptrace and restoretrace. It can also be useful as a standalone program. It is available for all NetBackup server platforms.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpgetdebuglog remote_machine
        [remote_program mmddyy]
```

DESCRIPTION

If all three arguments are specified, bpgetdebuglog will print to standard output the contents of the specified debug log file. If only the *remote_machine* is specified, bpgetdebuglog will print to standard output the number of seconds of clock drift between the local machine and the remote machine. A positive number means that the local machine is ahead of the remote machine. A negative number means that the remote machine is ahead of the local machine.

bpgetdebuglog must be in the `<install_path>\NetBackup\bin\admincmd` directory in order to be used by backuptrace and restoretrace.

You must have root administrator privileges to execute this command.

OPTIONS

`remote_machine`
: name of the remote server

`remote_program`
: name of the debug log directory on the remote server

`mmddyy`
: The day stamp used to identify the log file (log.mmddyy for UNIX, mmddyy.log for Windows) to be read.

EXAMPLES

```
/usr/openv/netbackup/bin/admincmd/bpgetdebuglog peony bpcd 071202
```

bpimage(1M)

NAME

`bpimage` - Enables users to perform different functions to stored images in a database.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpimage -[de]compress
         [-allclients | -client client_name]

/usr/openv/netbackup/bin/admincmd/bpimage [-M
         master_server[,...,]]

/usr/openv/netbackup/bin/admincmd/bpimage -npc copy # -backupid
         backupid [-client client_name]

/usr/openv/netbackup/bin/admincmd/bpimage -newserver
         newserver_name [-oldserver oldserver_name] [-id id]

/usr/openv/netbackup/bin/admincmd/bpimage -deletecopy #
         -backupid backupid

/usr/openv/netbackup/bin/admincmd/bpimage -testlock # -backupid
         backupid

/usr/openv/netbackup/bin/admincmd/bpimage -prunetir
         [-allclients | -client client_name]

/usr/openv/netbackup/bin/admincmd/bpimage -create_image_list
         -client client_name

/usr/openv/netbackup/bin/admincmd/bpimage -index index_number
         -client client_name

/usr/openv/netbackup/bin/admincmd/bpimage -wff path_bytes
         -backupid backupid [-client client_name]

/usr/openv/netbackup/bin/admincmd/bpimage -cleanup

/usr/openv/netbackup/bin/admincmd/bpimage -update
```

DESCRIPTION

This command can be use to do many different functions to images stored in a database. Some of the functions that a user can use bpimage to perform are:

- Compress and de-compress stored images
- Remove existing images from the database
- Test the locking capability on an image

- Create an image list file that can be used to qualify an image
- Index a client.

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 this is a media report.

`-allclients`
: Specifies the selection of all NetBackup clients that have already been backed up on the system.

`-backupid` *backup_id*
: Specifies a backup ID to use for finding applicable images.

`-client` *name*
: Specifies a client name to use for finding backups or archives to list. This name must be as it appears in the NetBackup catalog.

`-cleanup`
: This command deletes expired images, compresses the images that are scheduled to be compressed, and prunes the TIR information from the images specified.

  Note: This command enables a user to manually accomplish the same tasks that are performed by the scheduler on a regular basis. It can be used when there is not enough time to wait for the scheduler to perform these tasks.

`-create_image_list`
: Creates an `image_list` file and an `image_info` file that can be used quickly to qualify an image.

`-d` *date*
: Specifies the start and end date range for the listing.

  `-d` specifies a start date and time for the listing. The resulting list shows only images in backups or archives that occurred at or after the specified date and time. The format of *date* depends on the user's locale setting. See the NOTES section for more information. For the C locale, the date syntax is as follows:

  mm/dd/yy [hh[:mm[:ss]]]

  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.

`-[de]compress`
: This command initiates an action to compress or de-compress a specified client, or all clients.

`-deletecopy #`
This command removes images that are specified by the copy number (#) and the *backup_id*.

`-filesysonly 0|1`
Depending on the setting, this option limits `bpimage` to querying only the local file system.

`-id id`
Specifies the backup ID when using the `update` command.

`-index n`
This command indexes the database. The *n* variable is the index level and has a range from 1 to 9. A value of 9 provides the most optimum index. This applies only to ASCII.

`-keyword "keyword_phrase"`
Specifies a keyword phrase for NetBackup to use when searching. The phrase must match the one that has been previously associated with the image.

`-objdesc string`
This command specifies the object description string of the Informix client type when using the `-update` command.

`-newserver name | -oldserver name`
Specifies the name (new or old) of a NetBackup server.

`-npc copy #`
This command sets the specified image as the primary image based on the copy number of the image.

`-numfiles number`
Specifies the number of files when using the `-update` command.

`-M master_server, . . .`
A list of alternative master servers. This is a comma-delimited list of hostnames. If this option is present, each master server in the list runs the `bpimage` command. If an error occurs for any master server, processing stops at that point.

The report is the composite of the information returned by all the master servers in this list. `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 issuing the `bpimage` command.

The default is the master server for the system running `bpimage`.

`-policy` *`name`*
: Searches for backups to import in the specified policy. The default is all policies.

`-prunetir`
: This command prunes the True Image Restore (TIR) information from the specified clients. The default is all clients.

`-rfile` *`0|1`*
: Specifies the use of the Restore file when using the `-update` command.

`-secinfo` *`0|1`*
: Specifies the use of Extended Security information on the NetWare client type.

`-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-NT`

  `NetWare`

  `Oracle`

  `OS/2`

  `Standard`

  `Sybase`

  `NDMP`

Note *The following policy types apply only to NetBackup Enterprise Server.*

  `AFS`

  `DataTools-SQL-BackTrack`

  `DB2`

  `FlashBackup`

  `SAP`

  `Split-Mirror`

`-update`
: This command updates an image based on the chosen parameter.

`-wff` *`path bytes`*
: This command writer the specified Files file.

NOTES

The format that you must use for date and time values in NetBackup commands varies according to the locale setting.

If you are uncertain of the NetBackup command requirements for your locale, enter the command with the `-help` option and check the USAGE. The following is part of the usage statement for `bpimage` that shows the `-d` option:

```
[-d mm/dd/yyyy hh:mm:ss]
```

Notice the month/day/year and hours:minutes:seconds requirements for the `-d` option. These are for a locale setting of C and can be different for other locales.

For more information on locale, see the locale(1) man page for your system.

bpimagelist(1M)

NAME

`bpimagelist` - Queries the NetBackup catalog and produces a report on the status of the NetBackup images.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpimagelist -l | -L | -U |
        -idonly [-d date | -hoursago hours] [-e date] [-keyword
        "keyword phrase"] [-client client_name] [-backupid
        backup_id] [-option option_name] [-policy policy_name]
        [-pt policy_type] [-rl retention_level] [-sl sched_label] [-st
        sched_type] [-M master_server[,...,]] [-v]

/usr/openv/netbackup/bin/admincmd/bpimagelist [-media] [-l | -L
        | -U | -idonly] [-d date | -hoursago hours] [-e date]
        [-server server_name] [-keyword "keyword phrase"]
        [-client client_name] [-option option_name] [-policy
        policy_name] [-pt policy_type] [-rl retention_level] [-sl
        sched_label] [-st sched_type] [-M master_server[,...,]] [-v]
```

DESCRIPTION

`bpimagelist` uses a specified format to report the images that match the attributes that are sent from the commands options. `bpimagelist` lists NetBackup catalog image information. The `bpimagelist` command writes its debug log information to the `/usr/openv/netbackup/logs/admin` directory. You can use the information in this directory for troubleshooting.

The output of `bpimagelist` goes to standard output.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to the *NetBackup System Administrator's Guide*.

OPTIONS

Report-type options

`-media`

Specifies that the listing reports on removable media satisfying a set of criteria. If `-media` is not present, the report is on images, not media, satisfying a set of criteria.

Report-format options:

`-U`

Report in User mode. The report is formatted, it includes a banner listing the column titles, and the status is a descriptive term instead of a number.

`-L`

Report in Long mode. For instance, for the Media List report, the report lists the information for each media ID as a series of *attribute* = *value* pairs, and the density value is provided as both a descriptive term and a number.

`-l`

Report in Short mode. This produces a terse listing. This option is useful for scripts or programs that rework the listing contents into a customized report format.

`-idonly`

Produce an abbreviated listing. For an image listing, the listing contains the creation time, backup ID, and schedule type of each image. For instance, if the listing criterion is a window of time image listing contains, for each image created in this window, only the creation time, backup ID, and schedule type of the image.

For a media listing, the listing contains only the applicable media IDs. For instance, if the listing criterion is a window of time, the listing contains only the media IDs 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 this is a media report.

`-hoursago` *hours*

Include images written up to this many hours ago. This is equivalent to specifying a start time (`-d`) of the current time minus *hours*. *hours* must be 1 or greater.

`-option` *option_name*

Specifies a criterion for finding images to list. *option_name* is one of the following character strings, in either upper-or lower-case:

`INCLUDE_PRE_IMPORT` - Include images that have completed phase one of an import. Refer to the `bpimport(1M)` command description or the *NetBackup System Administrator's Guide* for more information.

`ONLY_PRE_IMPORT` - Include only images that have completed phase one of an import.

`INCLUDE_TIR` - Include images that were created by true-image-recovery backups. Refer to the `bpcpinfo(1M)` command description or the *NetBackup System Administrator's Guide* for more information on this topic.

`ONLY_TIR` - Include only images that were created by true-image-recovery backups.

The default is that there are no restrictions on the images selected.

`-backupid` *backup_id*
Specifies a backup ID to use for finding applicable images (applies only to image listing).

`-client` *client_name*
Specifies a client name to use for finding backups or archives to list. This name must be as it appears in the NetBackup catalog. By default, `bpimagelist` searches for all clients.

`-server` *server_name*
Specifies the name of a NetBackup server or `ALL`. This option applies to the media report (`-media`). If `-server` specifies a server name, the media in the report are only the media which reside on that server and which also satisfy the other criteria specified by `bpimagelist`. For instance, if `-hoursago 2` is specified, the media must contain an image created in the past two hours.

The query goes to the image catalog residing 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. This is equivalent to specifying `-server ALL`.

`-M` *master_server*, . . .
A list of alternative master servers. This is a comma-delimited list of hostnames. If this option is present, each master server in the list runs the `bpimagelist` command. If an error occurs for any master server, processing stops at that point.

The report is the composite of the information returned by all the master servers in this list. `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 issuing the `bpimagelist` command.

The default is the master server for the system running `bpimagelist`.

`-pt` *policy_type*
Specifies a policy type. By default, `bpimagelist` searches for all policy types. *policy_type* is one of the following character strings:

`Informix-On-BAR`

`MS-Exchange-Server`

`MS-SQL-Server`

`MS-Windows-NT`

NetWare

Oracle

OS/2

Standard

Sybase

NDMP

Note *The following policy types apply only to NetBackup Enterprise Server.*

AFS

DataTools-SQL-BackTrack

DB2

FlashBackup

SAP

Split-Mirror

`-rl` *retention_level*

Specifies the *retention_level*. The *retention_level* is an integer between 0 and 24. By default, `bpimagelist` searches for all retention levels.

`-d` *date*

`-e` *date*

Specifies the start and end date range for the listing.

`-d` specifies a start date and time for the listing. The resulting list shows only images in backups or archives that occurred at or after the specified date and time. The format of *date* depends on the user's locale setting. See the NOTES section for more information. For the C locale, the date syntax is as follows:

mm/dd/yy [hh[:mm[:ss]]]

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.

`-e` specifies an end date and time for the listing.

The resulting list shows only files from backups or 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.

`-keyword` "*keyword_phrase*"

Specifies a keyword phrase for NetBackup to use when searching. The phrase must match the one that has been previously associated with the image. For instance, the `-k` option of the `bpbackup(1)` or `bparchive(1)` command associates a keyword with the image when the image is created.

`-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:

`FULL` (full backup)

`INCR` (differential-incremental backup)

`CINC` (cumulative-incremental backup)

`UBAK` (user backup)

`UARC` (user archive)

`NOT_ARCHIVE` (all backups except user archive)

`-policy` *name*

Searches for backups to import in the specified policy. The default is all policies.

Other options:

`-help`

Prints a command line usage message when it is the only option on the command line.

`-v`

Selects 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 NetBackup has debug logging enabled (`/usr/openv/netbackup/logs/admin` directory defined).

NOTES

The format that you must use for date and time values in NetBackup commands varies according to the locale setting.

If you are uncertain of the NetBackup command requirements for your locale, enter the command with the `-help` option and check the USAGE. The following is part of the usage statement for `bpimagelist` that shows the `-d` and `-e` options:

```
[-d mm/dd/yy hh:mm:ss] [-e mm/dd/yy hh:mm:ss]
```

Notice the month/day/year and hours:minutes:seconds requirements for the `-d` and `-e` options. These are for a locale setting of C and can be different for other locales.

For more information on locale, see the locale(1) man page for your system.

EXAMPLES

Example 1

The first example shows the last time each media ID available to a server had a backup image written today:

```
   bpimagelist -media -U

  Media ID   Last Written     Server
  --------   --------------   ----------
  IBM000     01/06/2003 01:06   hat
  AEK800     01/06/2003 03:01   hat
  C0015      01/06/2003 02:01   hat
```

Example 2

The following example shows the last time the media IDs available to the server had a backup image written during the specified time:

```
bpimagelist -media -d 01/05/2003 18:00:46 -e 01/06/2003 23:59:59
-U

  Media ID   Last Written     Server
  --------   --------------   ----------
  IBM000     01/06/2003 01:06   hat
  AEK800     01/06/2003 03:01   hat
  C0015      01/06/2003 02:01   hat
  143191     01/05/2003 23:00   hat
```

The following example lists all images written today:

```
bpimagelist -U
Backed Up       Expires     Files       KB  C  Sched Type Policy
--------------  -------- -------- --------  -  ------------
------------
01/27/2003 01:08  02/03/2003     1122   202624  N  Full Backup
3590Grau
01/27/2003 01:01  02/03/2003     1122   202624  N  Full Backup
IBM3590policy
01/27/2003 03:01  02/03/2003      531  1055104  N  Full Backup
DELLpolicy
01/27/2003 02:01  02/03/2003      961    31776  N  Full Backup
QUALpolicy
01/27/2003 01:08  02/03/2003     2063   603328  N  Full Backup
IBM3590policy
01/27/2003 01:01  02/03/2003     2063   603328  N  Full Backup
3590Grau
```

Example 3

The following example lists media written information for 01/05/2003:

```
bpimagelist -media -d 01/05/2003 -e 01/05/2003 -U
Media ID   Last Written     Server
--------   --------------   ----------
IBM000     01/05/2003 01:13   hat
143191     01/05/2003 23:00   hat
AEK800     01/05/2003 03:07   hat
C0015      01/05/2003 02:06   hat
```

FILES

`/usr/openv/netbackup/logs/admin/log.`*mmddyy*

`/usr/openv/netbackup/db/images`

SEE ALSO

`bp(1),bparchive(1),bpbackup(1),bprestore(1)`

bpimmedia(1M)

NAME

`bpimmedia` - Display information about the NetBackup images on media.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpimmedia [-l | -L] [-policy
        policy_name] [-client client_name] [-d date] [-e date]
        [-mediaid media_id | path_name] [-mtype image_type]
        [-option option_name] [-rl retlevel] [-sl sched_label] [-t
        sched_type] [-verbose] [-M master_server,...]

/usr/openv/netbackup/bin/admincmd/bpimmedia -spangroups
        [-mediaid media_id] [-U] [-cn copy_number]
```

DESCRIPTION

`bpimmedia` queries the NetBackup image catalog and reports on the NetBackup images. `bpimmedia` produces two reports:

- An Images-on-Media report
- A Spangroups report

The first form of `bpimmedia` in the SYNOPSIS displays a set of NetBackup images in the Images-on-Media report. The Images-on-Media report lists the contents of media as recorded in the NetBackup image catalog. You can generate this report for any medium (including disk), filtering the report contents according to client, media ID or path, and so on. Refer to the section on NetBackup Reports in the *NetBackup System Administrator's Guide* for more information, including details about the fields in the Images on Media report. The Images on Media report does not show information for media used in backups of the NetBackup catalogs.

The second form of `bpimmedia` in the SYNOPSIS uses the `-spangroups` option to list media id groups 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 spanning images. The `-spangroups` form of `bpimmedia` must be run on the NetBackup master server that administers the volumes. (See the Spanning Media topic in the *NetBackup System Administrator's Guide*.) 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.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-policy` *policy_name*
Policy name. By default, `bpimmedia` searches for images for all policies.

`-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 (1 or 2) of a backup ID. The default is copy 1. This option is used only in combination with `-spangroups`.

`-d` *date*

`-e` *date*
The start and end date. These specify the time range during which an image must have been created to be included in the report.

`-d` specifies a start date and time. The resulting list shows only images from backups or archives that occurred at or after the specified date and time. The format of *date* depends on the user's locale setting. See the NOTES section for more information. For the C locale, the date syntax is as follows:

mm/*dd*/*yyyy* [*hh*[: *mm*[: *ss*]]]

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.

`-e` specifies an end date and time. The resulting list shows only images from backups or 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.

`-help`
Prints a command line usage message when `-help` is the only option on the command line.

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

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

`-M` *master_server,...*
A list of alternative master servers. This 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 issuing the command. If an error occurs for any master server, processing 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 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 filesystem for a disk storage unit.

When `-mediaid` is specified, the Images-on-Media report displays only images stored on this VSN or pathname. By default, the report displays images stored on all media IDs and pathnames.

For the Spangroups report (`-spangroups`), `-mediaid` can only be followed by a VSN. If `-mediaid` is omitted when `-spangroups` is present, `bpimmedia` displays all media in all spanning groups.

`-mtype`

Image type. The defined values, and their interpretations, are

`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 upper-or lower-case:

`INCLUDE_PRE_IMPORT` - Include images that have completed phase one of an import. Refer to the `bpimport(1M)` command description or the *NetBackup System Administrator's Guide* for more information.

`ONLY_PRE_IMPORT` - Include only images that have completed phase one of an import.

The default is `INCLUDE_PRE_IMPORT`.

`-rl` *retention_level*

The retention_level. The retention_level is an integer between 0 and 24. By default, `bpimmedia` searches for all retention levels.

`-sl` *sched_label*

The schedule label. By default, `bpimmedia` searches for images for all schedule labels.

`-spangroups`

Specifies that `bpimmedia` should create a Spangroups report. The default is to create an Images-on-Media report.

`-t` *sched_type*

Specifies a schedule type for the image selection. The default is any schedule type. Valid values, in either upper- or lower-case, are:

FULL (full backup)

INCR (differential-incremental backup)

CINC (cumulative-incremental backup)

UBAK (user backup)

UARC (user archive)

-U

The list type is user. This option is used only in combination with -spangroups. See the section DISPLAY FORMATS for more detail.

-verbose

Select verbose mode for logging. This is only meaningful when running with debug logging turned on (the /usr/openv/netbackup/logs/admin directory is defined).

DISPLAY FORMATS

IMAGES-ON-MEDIA REPORT

For the Images-on-Media report, there are two formats, short (-l or default) and long (-L).

Note, if you want to process and use the output of bpimmedia, VERITAS recommends that you use the -l option. The output of bpimmedia using 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, for example, want to obtain a quick and more readable view of the NetBackup images on media.

- Long Display Format (-L)

  If the command line contains -L, the display format is long. The -L display format 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 in the table below. The first line of the entry contains the fields Backup_ID...Expires. Then, for each fragment in the image, there is a line containing 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 bpduplicate(1M) for more information on the terms *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..24)

Files - Number of files in the backup

C - Compression (Y or N)

E - Encryption (Y or N)

T - Image type

R is Regular (scheduled or user-directed backup)

P is Pre-imported backup (phase 1 completed)

I is Imported backup

PC - Primary copy, 1 or 2. Designates which copy of the backup NetBackup chooses when restoring.

Expires - Expiration date of the first copy to expire, which is indicated by the Expires field of the fragment which is described below

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 for removable media; Disk otherwise)

Density - Density of the device that produced the backup (applies only to removable media)

Fnum - File number; this is the n-th backup on this medium (applies only to removable media)

Off - The byte offset on the medium where the backup begins (applies only to optical disk; ignore this value for tapes and magnetic disk)

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 indicating whether this copy is multiplexed, Y or N (applies only when fragment number is 1)

Expires - 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 regr1_guava -t FULL
Backup-ID        Policy      Type  RL  Files   C  E  T  PC  Expires
Copy Frag  KB Type Density FNum Off Host DWO MPX Expires MediaID
----------------------------------------------------------------
guava_0949949902 regr1_guav FULL  3   25  N  N  R  1  12:58 03/09/2003
 1   1    256 RMed dlt     13   0   plum 0   Y   12:58 03/09/2002 A00002
```

- Short Display Format (`-l`)

  If the `bpconfig` command line contains `-l` or contains no list-format option, the display format is short. This produces a terse listing. This option can be useful for scripts or 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 for an entry is n+1, where n is the number of fragments for the image. The layout of an entry is a first line, containing information about the image, followed by a line containing information about each fragment of the image. The attributes appear in the following order, separated by blanks.

  Fields and Meanings for the `-l` format are as follows:

  Line 1

  IMAGE - Identifies the start of an image entry

  Client - Client for the backup that produced this image

  Version - Image-version level

  Backup-ID - Unique identifier for the backup that produced this image

  Policy - Policy name

  Policy type - 0 denotes Standard, etc. Run bpimmedia -L or refer to bpbackup(1M) to interpret the policy-type value as a policy-type name.

  Schedule - Schedule name

  Type - Schedule type (full, etc.)

  RL - Retention level (0..24)

  Files - Number of files

  Expires - Expiration date of the first copy to expire, which is indicated by the Expires field of the fragment which is described below (system time); 0 denotes an image “in progress” or failed.

  C - Compression; 1 (yes) or 0(no)

  E - Encryption; 1 (yes) or 0(no)

Line 2_n+1

FRAG - Identifies a fragment line in an image entry

Copy - Copy number of this fragment

Frag - Fragment number, or -1 for a TIR fragment

KB - Size of the fragment, in kilobytes

(Internal) Internal value, not documented

Type - Media type (2 for removable media; 0 for disk)

Density - Density value (applies only to removable media) Run `bpimmedia -L` or `bpmedialist -mlist -L -m` *mediaid* to interpret the density value as a density label.

Fnum - File number; this is the n-th backup on this medium (applies only to removable media)

MediaID - Media ID or absolute path where the image is stored

Host - Server whose catalog contains this image

Block size - Number of kilobytes per block for this medium

Off - Offset

Media dateTime this medium was allocated (system time)

DWO - Device Written On (applies only to removable media)

(Internal) - Internal value, not documented

(Internal) - Internal value, not documented

Expires - Expiration date of this copy in system time (applies only when fragment number is 1)

MPX - Flag indicating whether this copy is multiplexed, 1(yes) or 0(no) (applies only when fragment number is 1)

Example of the short display format:

```
bpimmedia -l -policy regr1_guava -t FULL
IMAGE guava 3 guava_0949949902 regr1_guava 0 full 0 3 25 952628302 0 0
FRAG 1 1 10256 512 2 13 13 A00002 plum 65536 0 949616279 0 0 *NULL* 952628302 1
```

SPANGROUPS REPORT

For the Spangroups report, there are two formats: user (-U option) and short (the default). Both formats list, for each server, the server name, and the group data for that server. For each group of media that share spanned backup images, the media Ids are listed. When -mediaid appears on the command line, only the server and media group related to that media ID are displayed.

Note, if you want to process and use the output of bpimmedia, VERITAS recommends that you use the -l option. The output of bpimmedia using 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, for example, want to obtain a quick and more readable view of the NetBackup images on media.

The user (-U) display format looks like this:

```
bpimmedia -spangroups -U
```

```
Related media groups containing spanned backup images, server plum:
Group:
  A00002  A00003
Group:
  400032
```

The short display format looks like this

```
bpimmedia -spangroups
```

```
SERVER plum
GROUP A00002 A00003
GROUP 400032
```

NOTES

The format that you must use for date and time values in NetBackup commands varies according to your locale setting.

If you are uncertain of the NetBackup command requirements for your locale, enter the command with the -help option and check the USAGE. The following is part of the usage statement for bpimmedia that shows the -d and -e options:

```
[-d mm/dd/yy hh:mm:ss] [-e mm/dd/yy hh:mm:ss]
```

Notice the month/day/year and hours:minutes:seconds requirements for the -d and -e options. These are for a locale setting of C and can be different for other locales.

For more information on locale, see the locale(1) man page for your system.

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

Backup-ID        Policy  Type  RL  Files   C  E  T  PC  Expires
Copy Frag    KB Type Density FNum      Off       Host       DWO MPX Expires MediaID
-----------------------------------------------------------------------------------------

t_0929653085    c_NDMP  FULL  3   5909    N  N  R  1   15:58 07/18/2003
 1 IDX      844 RMed dlt     2         0         almond     3                     CB7514
 1   1     9136 RMed dlt     1         0         almond     3   N   15:58 07/18/2003 CB7514
```

◆ Example 2

The following example displays the tapes required to restore a particular file. If the `bpimmedia` command line provides the criteria to identify an individual backup, the output shows which media were 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 plum contains the backup.

```
bpimmedia -L -client guava -d 2/7/2002 -t UBAK

Backup-ID            Policy      Type  RL  Files   C  E  T  PC  Expires
Copy Frag    KB Type Density FNum      Off       Host       DWO MPX Expires     MediaID
-----------------------------------------------------------------------------------------

guava_0949949686     regr1_guav UBAK  3   25      N  N  R  1   12:54 03/09/2002
 1   1    10256 RMed dlt     11        0         plum       0   Y   12:54 03/09/2002 A00002
```

Example 3

List, in long format, all the backups in the image catalog on the master server guava.

```
bpimmedia -L -M guava


Backup-ID            Policy      Type  RL  Files   C  E  T  PC  Expires
Copy Frag    KB Type Density FNum      Off       Host       DWO MPX Expires   MediaID
-----------------------------------------------------------------------------------------
guava_0949599942     test-policy FULL  1   15      N  N  R  1   11:45 02/17/2002
 1   1      224 Disk -       -         -         guava      -   N   11:45 02/17/20
/var/qatest/storage_unit//guava_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 07/18/2003
 1 IDX      839 RMed dlt     4         0         almond     6                 CB7514
```

```
 1   1    27154 RMed dlt     3         0         almond     6   N   23:14 07/18/2003 CB7514

toaster1_0929653085  NDMP_policy FULL  3   5909    N  N  R  1   15:58 07/18/2003
 1 IDX      844 RMed dlt     2         0         almond     3                  CB7514
 1   1     9136 RMed dlt     1         0         almond     3   N   15:58 07/18/2003 CB7514
```

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 administrative logging is enabled, the exit status is logged in the administrative daily log under the directory `/usr/openv/netbackup/logs/admin` in the form:

`bpimmedia: EXIT status =` *exit status*

If an error occurred, a diagnostic precedes this message.

FILES

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/images`

SEE ALSO

`bpbackup(1M),bpduplicate(1M),bpimport(1M)`

bpimport(1M)

NAME

`bpimport` - Import NetBackup and Backup Exec backups that are expired or are from another NetBackup or Backup Exec server.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpimport -create_db_info -id
        media_id [-server name] [-L output_file [-en]]
        [-passwd][-local]

/usr/openv/netbackup/bin/admincmd/bpimport [-l] [-p] [-pb]
        [-PD] [-PM] [-v] [-local] [-client name] [-Bidfile
        file_name] [-M master_server] [-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]
```

DESCRIPTION

The `bpimport` command allows backups to be imported. This command is useful for importing backups that have expired or are from another NetBackup server.

The import operation consists of two steps:

- Step 1 is performed with the first form of the command shown above (`-create_db_info` option) and recreates catalog entries for the backups that are on the specified media.
- Step 2 is performed with the second form of the command shown above and 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 2003 and its retention level is one week, its new expiration date is 21 November 2003.

You can import a backup only if all copies of it are expired. For more information on importing backups, see the *NetBackup System Administrator's Guide*.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

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 be imported. List one backup ID per line in the file. If this option is included, other selection criteria is ignored.

`-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 backups that are already in the catalog. This option only creates information about backups that are candidates for import, and does not perform the import operation. The `bpimport` command must be run with this option prior to importing any backups.

The `-id` parameter is required with this option.

`-e` *enddate*

`-s` *startdate*

Specifies the end (`-e`) or start (`-s`) of the range of dates and times that include all backups to import. The format of *enddate* or *startdate* depends on the user's locale setting. See NOTES. For the C locale, the date and time syntax is as follows:

mm/*dd*/*yy* [*hh*[: *mm*[: *ss*]]]

The default for the end date is the current date and time; the default for the start date is 24 hours prior to the current date and time.

`-hoursago` *hours*

Specifies number of hours to search prior to the current time for backups. Do not use with the `-s` option. The default is the previous midnight.

`-id` *media_id*

For step 1 (`-create_db_info`), this option specifies the media ID that has the backups you are going 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 by step 1 of the import operation.

A backup ID that begins on a media ID that was not processed by step 1 is not imported. A backup that ends on a media ID that was not processed by step 1 will be incomplete.

`-L` *output_file* `[-en]`

Specifies the name of a file in which to write progress information. The default is to not use a progress file.

Include the `-en` option to generate a log in English. The name of the log will contain the string `_en`. This option is useful to support personnel assisting in a distributed environment where differing locales may create logs of various languages.

`-l`

Produces output in the progress log that lists each file imported.

`-local`

When `bpimport` is initiated from a host other than master server and the `-local` option is *not* used (default), `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 the `-local` option to prevent the creation of a remote copy on the master server and 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 For NetBackup Server, this option is not required because there is 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 be imported according to the option settings, but does not perform the import. Displays the media IDs, server name, and information about the backups to be imported.

`-passwd`

Use with the Backup Exec tape reader option to catalog password protected Backup Exec media. When `-passwd` is specified, `bpimport` prompts the user for a password. The password given is then compared with the password on the media. If the password matches, the job proceeds. If the password does not match, the job fails.

Use `-passwd` only when Backup Exec media are being imported and the Backup Exec media are password-protected. Backup Exec media can only be imported on a Windows media server.

`-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 are sorted by date and time (newest to oldest).

`-PM`

Displays information on the backups to be imported according to the option settings, but does not perform the import. It displays the following information about the backup: date and time of the backup, policy, schedule, backup ID, host, and media ID.

`-policy` *name*

Search for backups to import in the specified policy. The default is all policies.

`-pt` *policy_type*

Search for backups created by the specified policy type. The default is any policy type.

Valid values are:

`Informix-On-BAR`

`MS-Exchange-Server`

`MS-SQL-Server`

`MS-Windows-NT`

`NDMP`

`NetWare`

`Oracle`

`OS/2`

`Standard`

`Sybase`

Note *The following policy types apply only to NetBackup Enterprise Server.*

AFS

DataTools-SQL-BackTrack

DB2

FlashBackup

SAP

Split-Mirror

`-server` *name*

Note For NetBackup Server there is only one server (the master). When using NetBackup Server, specify the name of that server.

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 be imported. The default is the media server where the command is run.

`-sl` *sched_label*

Search for backups to import which were created by the specified schedule. The default is all schedules.

`-st` *sched_type*

Search for backups to import which were created by the specified schedule type. 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 verbose mode. When specified, the debug and progress logs display more information.

NOTES

The format that you must use for date and time values in NetBackup commands varies according to your locale setting. The examples in this command description are for a locale setting of C.

For more information on locale, see the `locale`(1) man page for your system.

EXAMPLES

Example 1

The following command (all on one line) creates catalog information for backups on media ID A00000. The media host hostname is cat. The progress file is `/tmp/bpimport.ls`.

```
bpimport -create_db_info -id A00000 -server cat -L
/tmp/bpimport.ls
```

Example 2

The following command (all on one line) displays information about the backups that are candidates for import. The backups displayed would have been created between 11/01/2002 and 11/10/2002. The `bpimport` command with the `-create_db_info` option must be run prior to this command.

```
bpimport -PM -s 11/01/2002 -e 11/10/2002
```

Example 3

The following command imports the backups specified in the `/tmp/import/images` file. The progress is entered in the `/tmp/bpimport.ls` file.

```
bpimport -Bidfile /tmp/import/image -L /tmp/bpimport.ls
```

FILES

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/images/*`

bpinst(1M)

NAME

bpinst - installs and configures NetBackup Encryption to provide file-level encryption of backups and archives.

SYNOPSIS

```
/usr/openv/netbackup/bin/bpinst -ENCRYPTION [-force_install]
          [-verbose] [-policy_names] name1 [name2 ... nameN]

/usr/openv/netbackup/bin/bpinst -LEGACY_CRYPT
          [-update_libraries] [-crypt_option
          option][-crypt_strength strength] [-passphrase_prompt
          |-passphrase_stdin] [-verbose] [ [-policy_encrypt 0 |
          1] -policy_names] name1 [name2 ... nameN]
```

Note You must have NetBackup Encryption, a separately priced product, in order to use this command.

DESCRIPTION

NetBackup Encryption provides file-level encryption of backups and archives. There are two versions:

- `-ENCRYPTION` is the Standard Encryption method (recommended)

  Provides the ability to encrypt data using 128-bit or 256-bit OpenSSL ciphers.

- `-LEGACY_CRYPT` is the Legacy Encryption method

  Provides the user with the encryption strength choices previously available (40-bit DES and 56-bit DES).

The `bpinst` command, used with the `-LEGACY_CRYPT` or the `-ENCRYPTION` option, installs and configures the NetBackup Encryption product on NetBackup clients that can support encryption.

Before using this command, install the encryption software on the server as explained in the *NetBackup Encryption System Administrator's Guide*. Then, execute `bpinst -LEGACY_CRYPT` or `-ENCRYPTION` on the master server to install and configure NetBackup Encryption on the clients. A single execution copies the required files to the selected clients and also makes the necessary configuration changes on both the clients and the master server.

NOTE: If you are using bpinst -LEGACY_CRYPT to configure encryption on clients that were not previously configured for encryption, ensure that you push the encryption libraries to the clients first with one bpinst command and then configure the encryption pass phrase with a separate bpinst command. For example:

- bpinst -LEGACY_CRYPT -update_libraries
- bpinst -LEGACY_CRYPT -passphrase_prompt clientname1

If you try to specify both the -update_libraries and -passphrase_prompt arguments on the same command line, the pass phrase configuration can fail because the encryption libraries are not yet available on the client.

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 install and configure the software on the client.

See the OPTIONS section for an explanation of all options used with `bpinst -ENCRYPTION` or `-LEGACY_CRYPT`. (Pay special attention to the -passphrase_prompt option.)

Note You can also configure encryption for a client that is installed on the master server host.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

The following options apply to the `-ENCRYPTION` command.

`-ENCRYPTION`
: Required if using 128- or 256-bit OpenSSL ciphers. This option must be the first option specified to use the bpinst command to install or configure Cipher-based encryption. The order is important and do not omit this option.

`-force_install`
: Installs the client files on the client machine without checking the version of any existing files on the the client machine.

`-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` or `-ENCRYPTION` installs and configures all the clients in each policy specified.

If you omit the `-policy_names` option, the names are assumed to be NetBackup client names.

name1 [*name2* ... *nameN*]
: 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.

`-verbose`
: Prints the current encryption configuration of each client and what gets installed and reconfigured on each client.

The following options apply to the `-LEGACY_CRYPT` command.

`-LEGACY_CRYPT`
: Required if using 40- or 56-bit DES encryption. This option must be the first option specified to use the bpinst command to install or configure DES encryption. The order is important and do not omit this option.

`-update_libraries`
: Installs the encryption libraries on NetBackup clients. This option applies to the `-LEGACY_CRYPT` option only.

`-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 below).

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. This is the default.

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 40-bit DES encryption. This is the default value for a client that has not been configured for encryption.

`DES_56 | des_56 | 56`

Specifies 56-bit DES encryption.

`-passphrase_prompt | -passphrase_stdin`

Caution Do not forget the pass phrase. If the key file is damaged or lost, you may need the pass phrase in order to regenerate the key file. Without the proper key file, you cannot restore encrypted backups.

NetBackup uses a pass phrase to create 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 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 are using `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. Encryption keys generated from the pass phrase are used for subsequent backups. Old encryption keys are retained in the key file in order 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 is the default for 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` or `-ENCRYPTION` installs and configures all the clients in each policy specified.

If you omit the `-policy_names` option, the names are assumed to be NetBackup client names.

name1 [*name2* ... *nameN*]

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 list of notes applies to both the `-ENCRYPTION` and the `-LEGACY_CRYPT` option. For additional information about NetBackup encryption, refer to the *NetBackup Encryption System Administrator's Guide*.

- If you are running NetBackup in a clustered environment, pushing software to the client is only allowed from the active node.
- If you are pushing the encryption software to clients located in a cluster, specify the hostnames of the individual nodes (not virtual names) in the list of clients.
- In a clustered environment, after you have successfully installed the add-on, unfreeze the node.
- When you finish restoring encrypted files from a client, rename or delete the key file created, and 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/name, you may not be able to restore your own encrypted backups.
- Existing 40- or 56-bit encryption license keys are valid for upgrades.

The following list of notes applies to the –LEGACY_CRYPT option only.

- The pass phrase that `bpinst -LEGACY_CRYPT` sends over the network to a client is encrypted by a privately defined NetBackup 40-bit DES key.

- The key file on each NetBackup client is encrypted with a privately defined NetBackup DES key. The key can be 40 bit or 56 bit, depending on how the client is configured. Restrict access to the key file to the administrator of the client machine. 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.
- It is important to 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 named orca has been performing 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 in order to restore your backups.

  The following is the basic procedure for disaster recovery when using encryption (see the *NetBackup Troubleshooting Guide* for details on restoring the operating system and NetBackup). This example assumes a NetBackup client named `orca`.

1. Reinstall the operating system on `orca`.
2. Reinstall and configure the NetBackup client software on `orca`.
3. Reinstall and configure encryption on orca by executing the following command (one line):

```
bpinst -LEGACY_CRYPT -update_libraries -crypt_option allowed
```

4. Execute `bpinst -LEGACY_CRYPT` to create a pass phrase.

```
bpinst -LEGACY_CRYPT -passphrase_prompt orca
Enter new NetBackup pass phrase: *********************
Re-enter new NetBackup pass phrase: *********************
```

   The pass phrase that you enter here is the first one used on `orca`.

5. Execute `bpinst -LEGACY_CRYPT` for each subsequent pass phrase used on `orca`:

```
# bpinst -LEGACY_CRYPT -passphrase_prompt orca
Enter new NetBackup pass phrase: *********************
Re-enter new NetBackup pass phrase: *********************
```

6. Restore the backed up files to `orca`.

EXAMPLES

Example 1

The following command copies encryption software from a master server to NetBackup clients.

From a Master Server

Assume that you want to install the encryption software on `client1` and `client2`. You would enter a command like this (all on one line):

```
bpinst -ENCRYPTION client1 client2
```

Assume that you want to install the encryption software on all clients in the NetBackup policies `policy1` and `policy2`. You would enter a command like this (all on one line):

```
bpinst -ENCRYPTION -policy_names policy1 policy2
```

Example 2

The following command installs the libraries on a NetBackup client named mars (one line):

```
bpinst -LEGACY_CRYPT -update_libraries  mars
```

Example 3

The following command (all on one line) installs and configures 40-bit DES encryption on UNIX clients in a policy named policy40:

```
bpinst -LEGACY_CRYPT -update_libraries -crypt_option allowed
-crypt_strength des_40 -policy_encrypt 1

bpinst -LEGACY_CRYPT -passphrase_prompt -policy_names policy40
Enter new NetBackup pass phrase: *********************
Re-enter new NetBackup pass phrase: *********************
```

The above command uses 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 4

The following command (all on one line) specifies that the NetBackup client named strong must use 56-bit DES encryption:

```
bpinst -LEGACY_CRYPT -crypt_option required -crypt_strength des_56
strong
```

Example 5

The following command displays a verbose listing of the configuration for the client named strong:

```
bpinst -LEGACY_CRYPT -verbose strong
BPCD protocol version 4.5.0 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 sgi5 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
No update of NetBackup configuration required for client strong
No update of NetBackup pass phrase required for client strong
```

FILES

UNIX:

- UNIX server command

  /usr/openv/netbackup/bin/bpinst

- UNIX server directory with encryption software

  /usr/openv/netbackup/crypt

- UNIX client encryption libraries for 40- and 56-bit DES

  /usr/openv/lib/libvdes*.*

- UNIX client encryption key file for 40- and 56-bit DES

  /usr/openv/netbackup/keyfile

- UNIX client encryption key file utility for 40- and 56-bit DES

  /usr/openv/netbackup/bin/bpkeyfile

- UNIX client encryption key file utility for 128- and 256-bit OpenSSL cipher

  /usr/openv/netbackup/bin/bpkeyutil
  /usr/openv/share/ciphers.txt
  /usr/openv/share/version_crypt

bpkeyfile(1)

NAME

bpkeyfile - Encryption key file utility for NetBackup.

SYNOPSIS

```
bpkeyfile [-stdin] [-change_key_file_pass_phrase]
          [-change_netbackup_pass_phrase] [-display]
          key_file_path
```

AVAILABILITY

The `bpkeyfile` command is available only with the NetBackup Encryption option.

DESCRIPTION

`bpkeyfile` creates or updates a file that contains information used to generate DES encryption keys. The information is generated based on a NetBackup pass phrase that you supply. The key file is encrypted by a key-file pass phrase that you supply.

The NetBackup client software uses an encryption key calculated from information in the key file 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` can be run automatically. If you use your own key-file pass phrase, start `bpcd` with the -keyfile argument as explained under in the *NetBackup Encryption System Administrator's Guide*.

OPTIONS

`-stdin`
: Read pass phrases from standard input. By default, bpkeyfile reads pass phrases that you are prompted to input from your terminal window.

`-change_key_file_pass_phrase (or -ckfpp)`
: Change the pass phrase used to encrypt the key file.

`-change_netbackup_pass_phrase (or -cnpp)`
: Change the pass phrase used to encrypt NetBackup backups and archives on this client.

`-display`
: Display information about the key file.

key_file_path
The path of the key file to be created or updated by `bpkeyfile`.

NOTES

Pass phrases used by NetBackup 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. Space character (code 32) to tilde character (code 126).

The `bpkeyutil` command is used for standard encryption.

FILES

UNIX:

/usr/openv/netbackup/keyfile

(UNIX client encryption key file)

bpkeyutil(1M)

NAME

bpkeyutil - A key file utility used for NetBackup standard encryption.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpkeyutil [-stdin |
    -insert | -delete] [-display] [-client client_name]
    [-M server]
```

AVAILABILITY

The `bpkeyutil` command is available only with the NetBackup Encryption option.

DESCRIPTION

The `bpkeyutil` command updates a key file that contains keys used for encryption and decryption. The keys are generated based on private VERITAS *NetBackup pass phrases* that you supply. The key file is encrypted using a key. The NetBackup client software will use an encryption key from the key file, to encrypt files during a backup or decrypt files during a restore.

OPTIONS

`-stdin`
: Read pass phrases from standard input. By default, bpkeyutil reads pass phrases that you are prompted to input from your terminal window.

`-insert`
: Insert a new NetBackup pass phrase to the key file to encrypt NetBackup backups and archives on this client.

`-delete`
: Delete an existing pass phrase from the key file.

`-display`
: Display information about the key file.

`-client` *`client_name`*
: Name of the client where the key file resides. The default is the local client. 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

- The `bpkeyfile` command is used for legacy encryption.
- The key file must be the same on all nodes in a cluster.

FILES

`/usr/openv/var/keyfile.dat`

(UNIX client encryption key file)

bplabel(1M)

NAME

`bplabel` - Write a NetBackup label on tape media.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bplabel -m media_id -d density
          [-o] [-p volume_pool_name] [-n drive_name | -u
          device_number] [-host media_server] [-erase [-l]]
```

DESCRIPTION

The `bplabel` command writes a NetBackup label on the specified media. Labeling is required only for media that were last used for NetBackup catalog backups or by a non-NetBackup application. You can use this command to erase and label 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 (`ltid`) must be active for `bplabel` to succeed. You must also 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.

The following are some facts about using 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 already 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. For optical disk media, use the `tpformat` command on a UNIX server.
- You must have root privileges to run this command.

OPTIONS

`-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 is always converted to uppercase. The media ID must be six or fewer alphanumeric characters.

`-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 entering 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)

Note *The following densities are supported only by NetBackup Enterprise Servers.*

`8mm2` (8-mm Cartridge 2)

`8mm3` (8-mm Cartridge 3)

`dlt2` (DLT Cartridge 2)

`dlt3` (DLT Cartridge 3)

`dtf` (DTF Cartridge)

`hcart2` (1/2 Inch Cartridge 2)

`hcart3` (1/2 Inch Cartridge 3)

`odiskwm` (Optical Disk Write-Many)

`odiskwo` (Optical Disk Write-Once)

`-o`

Unconditionally overwrites the selected media ID. If this option is not specified, `bplabel` prompts for permission to overwrite media that meets any of the following conditions:

Contains a NetBackup media header.

Is 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 Media Manager volume database but is not in the NetBackup volume pool. *volume_pool_name* must specify the correct pool.

`-u` *device_number*
: Unconditionally assigns the standalone drive specified by *device_number*. 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.

`-n` *drive_name*
: Unconditionally assigns the standalone drive specified by *drive_name*. 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.

`-erase [-l]`
: This option is used to erase the media. Short erase is the default erase. If -l option is specified, the media will be long erased. A long erase operation can be very time consuming 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 will run on the local system.

NOTES

tpconfig -d, tpconfig -l, and vmoprcmd may truncate long drive names. Please use tpconfig -dl to obtain the full drive name.

SEE ALSO

`ltid(1M),vmadm(1M)`

bplist(1)

NAME

`bplist` - Lists backed up and archived files on the NetBackup server.

SYNOPSIS

```
/usr/openv/netbackup/bin/bplist [-A | -B] [-C client] [-S
          master_server] [-t policy_type] [-k policy] [-F] [-R [n]] [-b
          | -c | -u] [-l] [-r] [-flops file_options] [-Listseconds]
          [-T] [-unix_files] [-nt_files] [-s date] [-e date] [-I]
          [-PI] [-help] [-keyword "keyword_phrase"] [filename]
          [-Listpolicy]
```

DESCRIPTION

`bplist` 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.

The list shows only the files that you have read access to. You also must own or have read access to all directories in the file paths. You can list files that were backed up or archived by another client only if you are validated to do so by the NetBackup administrator.

If you create directory `/usr/openv/netbackup/logs/bplist/` with public-write access, `bplist` creates an debug log file in this directory that you can use for troubleshooting.

The output of `bplist` goes to standard output.

OPTIONS

`-A | -B`
: Specifies whether to produce the listing from archives (`-A`) or backups (`-B`). The default is `-B`.

`-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.

`-S` *master_server*
: Specifies the name of the NetBackup server. The default is the first `SERVER` entry found in the `/usr/openv/netbackup/bp.conf` file.

`-t` *policy_type*

Specifies one of the following numbers corresponding to the policy type. The default is 0 for all clients except Windows NT/2000, where the default is 13.

`0` = Standard

`4` = Oracle

`6` = Informix-On-BAR

`7` = Sybase

`10` = NetWare

`13` = MS-Windows-NT/2000

`14` = OS/2

`15` = MS-SQL-Server

`16` = MS-Exchange-Server

`19` = NDMP

Note *The following policy types apply only to NetBackup Enterprise Server.*

`11` = DataTools-SQL-BackTrack

`17` = SAP

`18` = DB2

`20` = FlashBackup

`21` = Split-Mirror

`22` = AFS

`-k` *policy*

Names the policy to search to produce the list. If not specified, all policies are searched.

`-F`

Specifies that in the list output, symbolic links (applies only to UNIX clients) will end with a trailing @ and executable files with a trailing *.

`-R [`*n*`]`

Recursively lists subdirectories encountered to a depth of *n*. The default for *n* is 999.

`-b | -c | -u`

Specifies an alternate date and 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 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.

`-l`

Lists in long format, giving mode, owner, group, size in bytes, and time of last modification for each file (see the EXAMPLES section of this man page). The list shows the mode of each file as 10 characters that represent the standard UNIX file permissions. The first character is one of the following:

d (specifies a directory)

l (specifies a link)

- (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 means the file is readable

w means the file is writable

x means the file is executable

- means the indicated permission is not granted

`-Listseconds`

Specifies that seconds granularity be used for the time stamp when the the `-l` option is used.

`-r`

Lists raw partitions that were backed up. The default is to list file systems.

`-flops` *file_options*

Allows either Backup Exec files to be listed, or both Backup Exec and NetBackup files to be listed. The default (`-flops` not specified) is to list only NetBackup files.

To list only Backup Exe files specify:

```
-flops 524288
```

To list Backup Exe and NetBackup files specify:

```
-flops 1048576
```

`-T`

Lists directories in true-image backups. The default is to list non-true-image backups.

Note: TIR information will not appear for synthetic full backups, even though TIR information is used for sythetic full backups.

`-unix_files`

Lists the files and directories in UNIX format. For example: `/C/users/test`.

`-nt_files`

Lists the files and directories in Windows format. For example: `C:\users\test`.

`-s` *date*

`-e` *date*

Specifies the start and end date range for the listing.

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

The format of *date* depends on the user's locale setting. See the NOTES section for more information. For the C locale, the date syntax is as follows:

mm/*dd*/*yy* [*hh*[:*mm*[:*ss*]]]

The valid range of dates are 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 backups or archives that occurred at or before the specified date and time. Use the same format as explained above for start date and time. The default is the current date and time.

`-I`

Specifies a case-insensitive search. This means that capitalization is not considered when comparing names (for example, Cat matches cat).

`-PI`

Specifies a path-independent search, which means that NetBackup searches for a specified file or directory without regard to the path. For example, if a file named `test` exists in the three directories shown below, a search for `test` finds all three instances of the file:

```
/tmp/junk/test
/abc/123/xxx/test
/abc/123/xxx/yyy/zzz/test
```

`-help`

Prints a command line usage message when `-help` is the only option on the command line.

`-keyword` "*keyword_phrase*"

Specifies a keyword phrase for NetBackup to use when searching 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 the `bpbackup` or `bparchive` command.

You can use this option in place of or in combination with the other restore options in order to make it easier to restore your backups and archives. The following meta characters can be used to simplify the task of matching keywords or parts of keywords in the phrase:

* matches any string of characters.

? matches any single character.

[ ] matches one of the sequence of characters specified within the brackets.

[-] matches one of the range of characters 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 ('...') to avoid conflict with the UNIX shell.

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

filename

Names the file or directory to list. If you do not specify a path, the default is the current working directory.

Any files or directories that you specify must be listed at the end, following all other options.

For directories, if you do not use the `-R` option, include the trailing path separator (/) as in the following:

```
bplist -l "/home/user1/*"
```

Note: If you are using the asterisk meta character "*", you should use quotation marks around the filename for the command to work properly.

`-Listpolicy`

Includes the schedule type and policy name in the command output.

NOTES

The format that you must use for date and time values in NetBackup commands varies according to the locale setting.

If you are uncertain of the NetBackup command requirements for your locale, enter the command with the -help option and check the usage. The following is part of the bplist usage output that shows the -s and -e options:

[-s mm/dd/yy hh:mm:ss] [-e mm/dd/yy hh:mm:ss]

These formats are for a locale setting of C and may be different for other locales. For more information on locale, see the locale(1) man page for your system.

EXAMPLES

Example 1

To list recursively, in long format, the files that were backed up in `/home/user1`.

```
bplist -l -R /home/user1
lrwxrwxrwx  user1    eng     0   Apr  5 12:25 /home/user1/dirlink
drwxr-xr-x  user1    eng     0   Apr  4 07:48 /home/user1/testdir
drwxr-x--- user1     eng     0   Apr  4 07:49 /home/user1/dir
-rwxr-----  user1    eng  1002   Apr  2 09:59 /home/user1/dir/file
lrwxrwxrwx  user1    eng     0   Apr  4 07:49 /home/user1/dir/link
```

Example 2

To list, with details, the files that were backed up and associated with all or part of the keyword phrase

`"My Home Directory"`

in directory `/home/kwc` , enter the following:

```
bplist -keyword "*My Home Directory*" -l /home/kwc/
```

Example 3

To list, with details, the files that were archived and associated with all or part of the keyword phrase

`"My Home Directory"`

in directory `/home/kwc` , enter the following:

```
bplist -A -keyword "*My Home Directory*" -l /home/kwc/
```

Example 4

To list, recursively and with details, the files that were backed up on drive D of Windows NT client slater and associated with all or part of the keyword phrase

`"Win NT"`

enter the following:

```
bplist -keyword "*Win NT*" -C slater -t 13 -R -l /D
```

FILES

`/usr/openv/netbackup/logs/bplist/log.`*mmddyy*

SEE ALSO

`bp(1),bparchive(1),bpbackup(1),bprestore(1)`

bpmedia(1M)

NAME

`bpmedia` - Freeze, unfreeze, suspend, or unsuspend NetBackup media.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpmedia -freeze | -unfreeze |
        -suspend | -unsuspend -m media_id [-h host] [-v]

/usr/openv/netbackup/bin/admincmd/bpmedia -movedb -m media_id
        -newserver hostname [-oldserver hostname] [-v]
```

DESCRIPTION

`bpmedia` allows an individual NetBackup media ID to be controlled in terms of allowing or disallowing future backups or archives to be directed to the media. Note that this command applies only to media managed by Media Manager.

Note Under certain media or hardware error conditions, NetBackup automatically suspends or freezes media. If this happens, the reason is logged in the NetBackup Problems report. If necessary, you can use the `bpmedia -unfreeze` or `-unsuspend` options to reverse this action.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-freeze`

Freezes the specified media ID. When an active NetBackup media ID is frozen, NetBackup stops directing 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`

Unfreeze the specified media ID. This 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 that when the media ID expires, it is immediately unassigned in the NetBackup volume pool.

`-unsuspend`

Unsuspend the specified media ID. This reverses the action of `suspend` and allows the media to be used for backups or archives again.

`-movedb -newserver` *hostname* `[-oldserver` *hostname*`]`

Note You cannot use the `-movedb` option with NetBackup Server.

Moves a media catalog entry from one server to another in a master and media server cluster. This command moves the media catalog entry for the specified media ID from *oldserver* to *newserver* and updates the NetBackup image catalog to reflect that the media ID was moved. It is assumed that after the move, *newserver* has access to the media.

`-newserver` *hostname* specifies the name of the host to which the entry is moved.

`-oldserver` *hostname* specifies the name of the host where the catalog entry to be moved currently resides. If you do not specify `-oldserver`, the system where the command is being run is considered to be the old server.

The `-movedb` option is most meaningful in configurations where a master and its media servers are sharing a robotic library and have access to all the media in the robot. If this is not the case, at a minimum, all NetBackup servers must use the same Media Manager volume database, so the media can be moved from one robotic library to another without losing their attributes and assignment status.

`-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 and you must specify the name of that server on the `bpmedia` command.

For example, assume you have a master server named whale and a media server named eel. You run the following `bpmedia` command on whale in order 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`

Select verbose mode. This is only meaningful when running with debug logging turned on (that is, when the `/usr/openv/netbackup/logs/admin` directory exists).

EXAMPLES

Note You cannot use the `-movedb` option with NetBackup Server.

Assume that the master server is HOSTM, with HOSTS1 and HOSTS2 being media servers. The following command, run on HOSTM, moves the media catalog entry for media ID DLT001 from HOSTS1 to HOSTS2 and updates the NetBackup image catalog:

```
bpmedia -movedb -m DLT001 -newserver HOSTS2 -oldserver HOSTS1
```

FILES

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/media/*`

bpmedialist(1M)

NAME

`bpmedialist` - Display NetBackup media status.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpmedialist  [-mlist] [-U |
        -l | -L] [-m media_id]  [-rl ret_level] [-d density] [-p
        pool_name] [-h host_name | -M master_server, ... ]  [-v]

/usr/openv/netbackup/bin/admincmd/bpmedialist  -summary [-U |
        -L] [-brief] [-p pool_name]  [-h host_name | -M
        master_server, ...] [-v]

/usr/openv/netbackup/bin/admincmd/bpmedialist  -mcontents -m
        media_id [-U | -l | -L] [-d density] [-h host_name | -M
        master_server, ...]  [-v]

/usr/openv/netbackup/bin/admincmd/bpmedialist  -count -rt
        robot_type -rn robot_number [-d density] [-U | -l] [-h
        host_name | -M master_server]  [-v]
```

DESCRIPTION

`bpmedialist` queries one or more NetBackup media catalogs and produces a report on the status of the NetBackup media. This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

`bpmedialist` produces one of four reports:

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. This is the default report type.

If `-U` is an option, the status field appears as English text. Otherwise, the status appears as a hexadecimal integer. This is a three-digit value. The interpretation of the two upper-order digits is given here. Any or all of these flags can be set. Settings other than those listed here correspond to unreported states.

>= 0x200 Multiplexing is TRUE.

>= 0x080 Imported is TRUE.

>= 0x040 Multiple retention levels is TRUE.

The interpretation for the low-order status digit is determined by comparing 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 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 below. The section on the Media List Report in your NetBackup system administrator's guide describes the fields in detail. Any fields listed below 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
- Kbytes
- nimages
- vimages (unexpired images)
- retention level
- volume pool
- number of restores
- status (described above)
- hsize
- ssize

- l_offset
- reserved
- psize
- reserved
- 4 reserved fields

MEDIA SUMMARY REPORT

The Media Summary report lists, by server, summary statistics for active and inactive media 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 if you attempt to abort the command by entering ctl-c and the media requested are still being mounted or positioned, the storage unit may stay in use for some time after the break. 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, containing the fields below. The section on the Media Contents Report in your NetBackup system administrator's guide contains more details. Any fields not described 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.

MEDIA COUNT REPORT

The Media Count report shows a count of the number of UP devices matching all the criteria specified. The robot type and the robot number are mandatory criteria for this report. The `-U` format provides a title, Number of UP devices for *rt*(*rn*) = *value*. The `-l` format provides only the value.

OPTIONS

Report-type Options

`bpmedialist` produces one of four types of reports. An option on the command line determines the type of report produced. The report-type options are as follows:

`-mlist`
: Produce a Media List report. This is the default report type.

`-summary`
: Produce a Media Summary report.

`-mcontents`
: Produce a Media Contents report.

`-count`
: Produce a Media Count report. This report also displays the media attribute `ALLOW_MULT_RET_PER_MEDIA` and its value, 0 (do not allow) or 1 (allow).

Report-format Options

The `bpmedialist` report can appear in one of several formats. The report-format options are as follows:

`-brief`

Produce 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, reporting on each media ID's status within these categories.

`-U`

Report in user mode. This is the default report mode. The report includes a banner listing the column titles, and the report style is descriptive, rather than terse.

`-L`

Report in long mode. This format produces the report with the most complete information. For instance, for the Media List report, the report lists the attributes of each media ID as a series of *keyword* = *value* pairs, one attribute per line. A value may be expressed as both a numeric value and a descriptive value.

`-l`

Report in short mode. This format produces a terse report. This option is useful for scripts or programs that rework the listing contents into a customized report format.

Other Options

The following are the remaining options used by `bpmedialist`:

`-d` *density*

Report 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

`odiskwm` - Optical Disk Write-Many

`odiskwo` - Optical Disk Write-Once

`-m` *media_id*

Report on this media ID only. This is a required option for the Media Contents report.

For the Media List report, this option is optional, and, by default, all media IDs are included in that report. The media ID can be provided in either upper- or lower-case. 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).

`-h` *host_name*

Note For NetBackup Server, there is 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 residing on the system host_name. For the `-mcontents` and `-count` options, 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 for a master server other than the local master, if a `bpmedialist` query is made using `-h` *the_media_server*, and an equivalent `bpmedialist` query uses `-M` *the_media_servers_master*, the `bpmedialist` using `-h` may complete faster. This difference in response time can be significant if the master server addressed by `-M` is located remotely, and the media server addressed by `-h` is local.

If host_name is `ALL`, the query goes to the local master server and its media servers.

`-help`

Prints a command line usage message when `-help` is the only option on the command line.

`-M` *master_server*, . . .

A list of alternative master servers. This 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, processing stops at that point.

The report is the composite of the information returned by all the master servers in this list. `bpmedialist` queries each of these master servers. Each master server in the list must allow access by the system issuing 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 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 issuing the `bpmedialist` command.

The default is the master server for the server running `bpmedialist`.

Note NetBackup Server supports only one server, the master; so the default, in this case, is always the NetBackup Server master where you run `bpmedialist`.

`-p` *pool_name*

Report on the media IDs that belong to this volume pool. The default is all pools.

`-rl` *retention_level*

Report on media that are using this retention level. The retention level determines how long to retain backups and archives. The *retention_level* is an integer between 0 and 24. The default retention level is 1.

Following are the retention levels with the installation values for the corresponding retention periods. Note that your site may have reconfigured the retention periods corresponding to the retention levels.

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 - 24 infinite

`-rn robot_number`

Report on the robot using this robot number. This is a required option when the `-count` option is used. The robot number can be obtained from the Media Manager device configuration. For rules concerning the use of this number, see your Media Manager system administrator's guide.

`-rt` *robot_type*

Report on a robot of this type. This is a required option when the `-count` option is used. For non-robotic (standalone) devices select NONE. Valid robot types include the following

`RSM` - Removable Storage Manager

`TL4` - Tape Library 4MM

`TL8` - Tape Library 8MM

`TLD` - Tape Library DLT

`TS8` - Tape Stacker 8MM

`TSD` - Tape Stacker DLT

`NONE` - Not robotic

Note *The following robot types apply only to NetBackup Enterprise Server.*

`ACS` - Automated Cartridge System

`LMF` - Library Management Facility

`ODL` - Optical Disk Library

`TLH` - Tape Library Half-Inch

`TLM` - Tape Library Multimedia

`TSH` - Tape Stacker Half-Inch

`-v`

Select 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 debug logging enabled (`/usr/openv/netbackup/logs/admin` directory defined).

EXAMPLES

Example 1

The following example produces a media report for all media IDs defined for the master server of the local system and any media servers.

Note For NetBackup Server, the report includes only media IDs for the master server because remote media servers are not supported.

```
hat 36# ./bpmedialist
Server Host = hat

id      rl  images   allocated      last updated   density   kbytes  restores
            vimages   expiration     last read        <------- STATUS ------->
-----------------------------------------------------------------------
143191  0    28   12/03/2002 23:02  12/22/2002 23:00    dlt     736288     1
              7   12/29/2002 23:00  12/09/2002 10:59

144280  0     9   11/25/2002 11:06  12/01/2002 23:03    dlt     290304     0
              0   12/08/2002 23:03      N/A         EXPIRED  FROZEN

AEK800  0    22   12/06/2002 03:05  12/23/2002 03:01    dlt    23213184    0
              7   12/30/2002 03:01  12/09/2002 10:48

C0015   0    28   11/26/2002 02:09  12/23/2002 02:01    dlt     896448     0
              7   12/30/2002 02:01      N/A

IBM001  0    16   12/16/2002  01:01  12/23/2002 01:07   dlt     6447360    0
             14   12/30/2002 01:07      N/A

L00103  0    20   12/07/2002 08:33   12/23/2002 01:07   dlt     7657728    0
              9   12/30/2002 01:07      N/A

L00104  0     9   12/11/2002  01:09  12/21/2002 01:04   dlt     5429504    0
              5   12/28/2002 01:04      N/A
```

Example 2

The following example produces a media count report for robot type TLD and robot number 0:

```
./bpmedialist -count -rt TLD -rn 0
ALLOW_MULT_RET_PER_MEDIA 0
Number of UP devices for TLD(0) = 2
```

Example 3

The following example produces a media contents report for media ID AEK802. The report is partially listed below.

```
./bpmedialist -mcontents -m AEK802
media id = AEK802, allocated 01/08/2003 03:10, retention level = 0


File number 1
 Backup id = hat_0915786605
 Creation date = 01/08/2003 03:10
 Expiration date = 01/15/2003 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 = 01/08/2003 09:23
            Expiration date = 01/15/2003 09:23
            Retention level = 0
            Copy number = 1
            Fragment number = 1
          Block size (in bytes) = 65536
```

Example 4

In this example, `bpmedialist` runs on the master server buffalo. `bpmedialist` produces a Media List report for master servers hat and duo.

```
 ./bpmedialist -M hat,duo
Server Host = hat

 id     rl  images   allocated      last updated    density  kbytes   restores
           vimages   expiration     last read        <------- STATUS ------->
-------------------------------------------------------------------------
143191   0     51   12/03/2002 23:02  01/11/2003 23:04    dlt    1436686      2
               9   01/18/2003 23:04  01/08/2003 10:26

144280   0      9   11/25/2002 11:06  12/01/2002 23:03    dlt     290304      0
               0   12/08/2002 23:03  01/12/2003 16:10  EXPIRED  FROZEN

AEK800   0     38   12/06/2002 03:05  01/08/2003 03:10     dlt  3922200024      0
               3   01/15/2003 03:10  12/09/2002 10:48  FULL

AEK802   0      6   01/08/2003 03:10  01/12/2003 03:05     dlt   6140544      0
               6   01/19/2003 03:05  01/12/2003 16:12

C0015    0     48   11/26/2002 02:09  01/12/2003 02:11     dlt   1531968      0
               7   01/19/2003 02:11      N/A

IBM000   0     19   01/01/2003 01:09  01/12/2003 02:05    dlt    8284224       0
              13   01/19/2003 02:05  01/09/2003 05:41

Server Host = duo

 id     rl  images   allocated      last updated    density    kbytes  restores
           vimages   expiration     last read        <------- STATUS ------->
-------------------------------------------------------------------------
A00004   0      0   11/16/2003 05:31      N/A            4mm         0       0
               0       N/A             N/A         FROZEN
```

```
DLT210   1      5   12/09/2002 06:10  01/08/2003 06:04     dlt      2560       0
                2   01/22/2003 06:04      N/A

DLT215   0    124   12/08/2002 14:57  01/12/2003 08:07     dlt   9788072       4
               28   01/19/2003 08:07  12/31/2002 15:42
```

Example 5

In this example, `bpmedialist` reports which of two hosts has a given media ID configured. Since the host hat does not have A00004 configured in its media catalog, it reports, the requested media ID was not found in the NetBackup media catalog or Media Manager volume 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 hat -h duo -m A00004
```

```
requested media id was not found in NB media database and/or
MM volume database

Server Host = duo

 id     rl  images   allocated      last updated    density    kbytes  restores
           vimages   expiration     last read        <------- STATUS ------->
-------------------------------------------------------------------------
A00004   0      0   11/16/2003 05:31      N/A            4mm       0       0
                0       N/A             N/A         FROZEN
```

FILES

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/media/mediaDB`

bpminlicense(1M)

NAME

`bpminlicense` - Manage NetBackup license file.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpminlicense [-path
        license_key_file | -M server] [-debug] [-verbose]
        [-list_keys] [-nb_features | -sm_features]
```

```
/usr/openv/netbackup/bin/admincmd/bpminlicense [-path
        license_key_file | -M server] [-debug] [-verbose]
        -find_keys | -delete_keys | -add_keys keystring1 ..
        keystringn
```

DESCRIPTION

The `bpminlicense` utility manages a NetBackup license file. 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`(1M) utility to manage the NetBackup licenses, which is preferred to this command.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-add_keys | -delete_keys | -find_keys` *keystring1 .. keystringn*
: Respectively, these options find and list, add, or delete one or more specified *keystrings* in the NetBackup license file.

`-debug`
: Display detailed information to standard error.

`-list_keys`
: List the keys in the NetBackup license file.

`-M` *server*
: Use the standard NetBackup license file from the specified NetBackup *server*.

`-nb_features`

`-sm_features`
: Respectively, list only active NetBackup or Storage Migrator feature IDs (and active keys when specified with the `-verbose` option).

`-path` *license_key_file*
: Use the specified *license_key_file* on the local system. The default is the standard NetBackup license file.

`-verbose`
: Display additional information to standard output.

bpmoverinfo(1M)

NAME

bpmoverinfo - discovers the third-party copy devices available on the SAN and creates a `mover.conf` file.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpmoverinfo [-u] [-h] [-o -]
          [- output_file_name]
```

DESCRIPTION

The `bpmoverinfo` command discovers the devices on the SAN that can operate as third-party copy devices (data movers), and by default writes the information to file `/usr/openv/volmgr/database/mover.conf`.

Note For backups using the Third-Party Copy Device backup method, a `mover.conf` file must exist at `/usr/openv/volmgr/database`.

See the *NetBackup Advanced Client System Administrator's Guide* for instructions on this command and for creating the `mover.conf` file.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-u`
: Discovers all third-party copy devices on the SAN, and updates the existing `mover.conf` file. If the `mover.conf` file does not exist, the -u option will fail.

`-h`
: Displays the `bpmoverinfo` usage statement.

`-o -`
: Sends output to the screen. Note the space before the second hyphen.

`-o output_file_name`
: Specifies an alternate path for the `bpmoverinfo` command output. If this option is not specified, the default is `/usr/openv/volmgr/database/mover.conf`.

FILES

`mover.conf`

bpnbat(1M)

NAME

`bpnbat` - enables a user to accomplish Authentication tasks from within NetBackup.

SYNOPSIS

```
/usr/openv/netbackup/bin/bpnbat [-Login] [-WhoAmI] [-AddDomain
         | -RemoveDomain] [-AddUser | -RemoveUser]
         [-AddMachine] [-LoginMachine] [-GetBrokerCert]
         [-ShowBrokerCerts] [-RemoveBrokerCert] [
```

DESCRIPTION

The bpnbat command is a tool that enables a user to use the VERITAS Security Subsystem (VxSS). VxSS has two distinct pieces to it.

- Authentication - the act of proving who you are
- Authorization - the act of checking what you can do

bpnbat enables a user to accomplish Authentication tasks from within NetBackup.

Note Any command that asks for a password will not echo the password or asterisks as they allow a *shoulder surfer* to significantly narrow the password search space.

Note The use of NetBackup Access Control requires the user's home directories to work correctly.

OPTIONS

`-Login`

Use this option to identify oneself to the system. When running this command, enter a Name, Password, Domain, Authentication type, and a server to authenticate. The combination of a name, password, domain, and domain type create 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.

`-WhoAmI`

Use this command to tell what identity you are currently using within VxSS. It lists your name, domain, the authenticating broker who issued the credential, the time at which a certificate will expire, and the domain type that was used when creating the credential.

`[-AddDomain | -RemoveDomain]`

These options enable an administrator, who is running 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, and only have meaning within VxSS. They are intended to be used in places where a centralized naming authority (such as a PDC/AD, or NIS domain) is not available.

You must have root privileges to use these command options.

`[-AddUser | -RemoveUser]`

These options enable an administrator, who is running locally on an Authentication server, to add or remove users from within domains in the private VERITAS Domain Database. These accounts only have meaning within VxSS. They are intended to be used in places where a centralized naming authority (such as, PDC/AD or NIS domain) is not available.

You must have root privileges to use these command options.

`-AddMachine`

Run this option on your authentication broker (root +ab). This option registers a machine in a private VERITAS Security Subsystem database. The identity is placed in the private domain NBU_Machines@<at.server.name>.

`-LoginMachine`

Run this option on your NetBackup Media, Master, and Clients. This option enables you to identify a machine using an account within the VERITAS Security Subsystem private domain NBU_Machines@<at.server.name>. This is analgus to logging in as a user to a specified authentication broker.

`-GetBrokerCert`

This command is used to obtain a broker certificate without authenticating to a broker.

`-ShowBrokerCerts`

This command lists all of the brokers that the user currently trusts. Any broker listed is trusted to handle authentication requests that are sent to it.

`-RemoveBrokerCert`

This command removes a trust of a specified authentication broker. 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.

EXAMPLES

Example 1

In the following example the user is using the -Login option to connect to the Authentication Broker (the server that handles the Authentication process) called test.domain.veritas.com, using the default port number. In the following example, an NIS account is being used, therefore a domain name 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, NIS+, NT, 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` command verifies the identity that you are currently using within VxSS. It lists your name, domain, the authenticating broker who issued the credential, the time at which your certificate will expire and what type of domain you used in creating the credential.

```
# bpnbat -WhoAmI

Name: user name

Domain: domain.veritas.com

Issued by: /CN=broker/OU=root@eek.min.veritas.com/O=vx

Expiry Date: Oct 27 20:57:43 2003 GMT

Authentication method: NIS

Operation completed successfully.
```

Example 3

Adding a machine to the machine identities list:

```
# bpnbat -AddMachine
```

```
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.
```

Logging in a machine 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.
```

Example 4

This command is used to 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

This command will list 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

Name: root
Domain: root@torpedo.domain.veritas.com
Issued by: /CN=root/OU=root@torpedo.domain.veritas.com/O=vx
Expiry Date: May 13 23:20:58 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.

```
# 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.

SEE ALSO

`bpnbaz` (1M)

bpnbaz(1M)

NAME

bpnbaz - enables a user to accomplish Authorization administration tasks from within NetBackup

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpnbaz -[AddUser | DelUser]
         Group_Name Domain_Type:Domain_Name:User_Name
         [-OSGroup|-AzGroup] -Server server1.domain.com
         [-CredFile Credential]

/usr/openv/netbackup/bin/admincmd/bpnbaz -[AddGroup | DelGroup]
         Group_Name -Server server1.domain.com [-CredFile
         Credential]

/usr/openv/netbackup/bin/admincmd/bpnbaz -[ListPerms |
         ListMainObjects | ListGroups | ShowAuthorizers]
         -Server server1.domain.com [-CredFile Credential]

/usr/openv/netbackup/bin/admincmd/bpnbaz -ListGroupMembers
         Group_Name -Server server1.domain.com [-CredFile
         Credential]

/usr/openv/netbackup/bin/admincmd/bpnbaz -AddPerms
         Permission_1[,Permission_2,...] -Group Group_Name
         -Object Object -Server server1.domain.com
         [-CredFileCredential]

/usr/openv/netbackup/bin/admincmd/bpnbaz -DelPerms -Group
         Group_Name -Object Object -Server server1.domain.com
         [-CredFileCredential]

/usr/openv/netbackup/bin/admincmd/bpnbaz
         -[AllowAuthorization|DisallowAuthorization] Machine
         Name -Server server1.domain.com

/usr/openv/netbackup/bin/admincmd/bpnbaz -SetupSecurity
         NBU.Master.Server.com -Server server1.domain.com
```

DESCRIPTION

Bpnbaz is a command line executable that is used within NetBackup to access the authorization portion of VxSS. Authorization is the process of checking rights on an object. This command enables you to do the following:

- Add users to Az groups

- Create Az groups
- Add and remove permissions from the main NetBackup resource objects
- Add and remove permissions on individual policies
- List current permissions on NetBackup resource and policies
- List Az groups
- Lists users within Az groups
- Permit machines to perform authorization actions
- Setup the initial security information

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 to this is with the SetupSecurity command. You must have local root privileges on the authorization server to use this command.

When using `bpnbaz`, it is assumed that the Master server and the Az server are the same machine.

Note The use of NetBackup Access Control requires the user's home directories to work correctly.

OPTIONS

`-AddGroup` *`Group_Name`*

This option enables you to create an authorization group defined with the variable *Group_Name*.

Note: An Az group is a collection within the Authorization engine into which OS groups and OS users can be placed. Adding a user to an Az group grants them the rights and privileges associated with that group.

`-AddPerms` *`Permission_1[,Permission_2,...]`*

This option adds the permissions specified for the given role to the object or policy in question. Refer to the *NetBackup System Administrator's Guide* for additional information. `-AddUser` *`Group_Name Domain_Type:Domain_Name:User_Name`*
You can add users by creating a unique enterprise account name, following this format: <Authentication type>:<Domain_Type>:<User_Name to which the user or group belongs>

The supported Authentication types for this variable are:

Nis ... Network Information Services

Nis+ ... Network Information Services Plus

Unixpwd ... Unix Password file on the Authentication server

NT ... Primary Domain Controller or Active Directory

Vx ... VERITAS Private database.

The *Domain_Type* variable is the domain that the user or group belongs, and the *User_Name* variable defines the applicable user or group name.

`-AllowAuthorization` *`Machine Name`*

This option specifies which machines 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.

`-CredFile` *`Credential`*

This option specifies a file name (*Credential*) from which to obtain an VxSS credential, rather than the default location.

`-DelGroup` *`Group_Name`*

Deleting an Az group from the authorization engine removes all the members of the group. This operation is not reversible; removing a group will revoke the rights granted to members of the group.

`-DelPerms`

This option deletes all permissions from an object for a given group. `-DelUser` *`Group_Name`* `Domain Type:Domain_Name:User_Name`

This option enables you to remove a user from an authorization group . This operation is not reversible. Refer to the AddUser option for definitions of the Domain_Type, User_Names, and Authentication types.

`-DisallowAuthorization` *`Machine Name`*

This option specifies which machines are not allowed to perform authorization checks. The security administrator must specify which servers (Master or Media) are not permitted to examine the Authorization database to perform authorization checks.

`-ListGroupMembers` *`Group_Name`*

This option lists the group member associated with a particular group defined by *Group_Name*.

`-ListGroups`

This option lists the defined groups.

`-ListMainObjects`

This option lists the current permissions for each group on each of the main NetBackup objects. This is an informative view that you can use to verify changes to permissions on an object. This options shows the permissions each group has within the authorization system.

`-ListPerms`

The option -ListPerms shows all applicable permissions for a given object or object type within the database. This will help the user to create meaningful customizations to their authorization. `-Group` *`Group_Name`*
This option enables you to define user groups that can be members of multiple user groups at the same time. NetBackup does not allow user groups to be nested.

`-Object` *`Object`*
This options enables you to control the access to specified objects or object collections.

`-OSGroup`
This option enables you to define a named collection of authentication principals, 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.

`-SetupSecurity`
This option must be run as root on the Az server.

`-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.

`-ShowAuthorizers`
This option lists the machines are allowed to perform authorization checks.

EXAMPLES

Example 1

An Az group is a collection within the Authorization engine where other OS groups and OS users are placed. This is the basic building block against which permissions are applied on the objects within the database. Adding a user to an Az group grants them all the rights and privileges associated with that group. When a user is placed in more than one group that user's effective permissions are 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.

```
/usr/openv/netbackup/bin/admincmd/bpnbaz -AddGroup "New Group 1"
-server test.domain.veritas.com
```

```
Operation completed successfully.
```

```
/usr/openv/netbackup/bin/admincmd/bpnbaz -ListGroups -server
test.domain.veritas.com
```

```
Administrators
```

```
Operators

Security Administrators

Resource Management Applications

Applications

New Group 1

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 2

Deleting an Az group:

Deleting an az group from the authorization engine will results in all the members being removed from the group. This operation is not reversible. Removing a group will revoke the rights granted to members of the group. As such you can do yourself a great disservice by deleting groups before careful thought goes into it.

```
/usr/openv/netbackup/bin/admincmd/bpnbaz -DelGroup "New Group 1"
-server test.domain.veritas.com

Operation completed successfully.

/usr/openv/netbackup/bin/admincmd/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

Adding and removing users from Az groups (and Listing group members):

Users are added by creating a unique enterprise name of the following format:
<Authentication type>:<Domain to which user/group belongs>:<user/group name>

Supported Authentication types are:

- Nis - Network Information Services
- NisPlus - Network Information Services Plus
- Unixpwd - UNIX Password file on the Authentication server
- NT - Primary Domain Controller or Active Directory
- Vx - VERITAS Private database

```
/usr/openv/netbackup/bin/admincmd/bpnbaz -AddUser  NBU_Operator
nis:domain.veritas.com:ssosa -server test.domain.veritas.com

Operation completed successfully.

/usr/openv/netbackup/bin/admincmd/bpnbaz -ListGroupMembers
NBU_Operator -server test.domain.veritas.com

==========

Type: User

Domain Type: nis

Domain:domain.veritas.com

Name: jdimaggio
```

```
==========

Type: User

Domain Type: nis

Domain:domain.veritas.com

Name: ssosa

Operation completed successfully.

/usr/openv/netbackup/bin/admincmd/bpnbaz -DelUser NBU_Operator
nis:domain.veritas.com:ssosa -server test.domain.veritas.com

Operation completed successfully.

/usr/openv/netbackup/bin/admincmd/bpnbaz -ListGroupMembers
NBU_Operator -server test.domain.veritas.com

==========

Type: User

Domain Type: nis

Domain:domain.veritas.com

Name: jdimaggio

Operation completed successfully.
```

Example 4

Listing Applicable Permissions:

Using -ListPerms will show all applicable permissions for a given object or object type within the database. This will help the user to create meaningful customizations to their authorization.

```
/usr/openv/netbackup/bin/admincmd/bpnbaz -ListPerms -server
test.domain.veritas.com

Object Type: Unknown

   Browse

Object Type: Media

   Browse

   Read

   New
```

```
   Delete
   Eject
. . .
   Restart
   Synchronize
Object Type: PolicyGroup
   Browse
   Read
   New
   Delete
   Activate
   Deactivate
   Backup
Operation completed successfully.
```

Example 5

ListMainObjects:

This option will list the current permissions for each group on each of the main NetBackup objects. This is an informative view that can be used to verify changes to permissions on an object. This show what permissions each group has within the authorization system.

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

Adding and deleting permissions from an object or policy:

Deletion deletes all permissions from an object for a given group. Add adds the permissions specified for the given role to the object or policy in question.

```
/usr/openv/netbackup/bin/admincmd/bpnbaz -AddPerms
Browse,Read,New,Delete -Group TestGroup1 -Object NBU_RES_Job
-server test.domain.veritas.com
```

```
Operation completed successfully.
```

```
/usr/openv/netbackup/bin/admincmd/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.
      /usr/openv/netbackup/bin/admincmd/bpnbaz -DelPerms -Group
      TestGroup1 -Object NBU_RES_Policy -server test.domain.veritas.com
      Operation completed successfully.
```

Example 7

Specifies what servers can perform Authorization checks as well as viewing what servers can perform Authorization checks. In addition, Disallows a server from performing Authorization checks:

This option is used to specify which machines 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 machine to perform authorization.

```
/usr/openv/netbackup/bin/admincmd/bpnbaz -AllowAuthorization
butterball.domain.veritas.com -server test.domain.veritas.com

Operation completed successfully.


/usr/openv/netbackup/bin/admincmd/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.

/usr/openv/netbackup/bin/admincmd/bpnbaz -DisallowAuthorization
butterball.domain.veritas.com -server test.domain.veritas.com

Operation completed successfully.

/usr/openv/netbackup/bin/admincmd/bpnbaz -ShowAuthorizers -server
test.domain.veritas.com

Operation completed successfully.
```

Example 8

Initial security boot strapping:

This option must be run as root on the Az server itself.

You are asked to provide login information for the first NetBackup Security administrator.

NOTE: Root on the system upon which the Az server is installed is always a security administrator.

```
/usr/openv/netbackup/bin/admincmd/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, NT, vx, unixpwd:

NIS

Operation completed successfully.
```

SEE ALSO

bpnbat (1M)

bppficorr (1M)

NAME

`bppficorr` - lists persistent snapshot information found in the NetBackup catalog for a specified client, and optionally deletes catalog entries for snapshots that no longer exist on the client.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bppficorr [-media] [-hoursago
         hours] [-policy policy_name] -client client_name
```

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, and removes any entries in the catalog that do not have corresponding snapshots on the client. This is useful if someone has renamed or removed a snapshot on the client.

Note Persistent snapshots are managed by NetBackup. 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 root privileges to execute this command.

OPTIONS

`-media`

Lists all persistent snapshot entries found in the NetBackup catalog for the client specified on the -client option. The list includes the backup IDs and the media descriptions for each backup ID. See the *NetBackup System Administrator's Guide* for details on the media description.

`-hoursago hours`

Includes images written up to this many hours ago (1 or greater). The default is all images.

`-policy policy_name`

NetBackup lists the persistent snapshot information found in the NetBackup catalog for this policy for the specified client. The default is all policies that include the client specified on the -client option.

`-client client_name`

This is a required option. NetBackup lists the persistent snapshot information found 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.

NOTES

bppficorr writes activity log information to the `/usr/openv/netbackup/logs/admin` directory. You can use the information in the directory for troubleshooting.

EXAMPLES

Example 1

To resynchronize the NetBackup catalog with a client's actual snapshots:

```
/usr/openv/netbackup/bin/admincmd/bppficorr -client lupine
```

Example 2

To display the snapshots that are currently in the catalog for client lupine:

```
/usr/openv/netbackup/bin/admincmd/bppficorr -media -client lupine
```

Sample output:

```
Listing frozen image info from NBU catalog
-----------------------------------------
backup_id            created      name
---------            -------      ----
1 lupine_1034167036   Wed Oct  9 07:37:16 2002
1 vxvm:32:vxfs:/V1fs:/dev/vx/dsk/oradg/PFI-V1_1034167036
2 lupine_1033995680   Mon Oct  7 08:01:20 2002
1 vxfs_pfi:34:vxfs:/ora8data:VX+NBU+PFI+ORA+2002.10.07.08h01m20s
3 lupine_1033880459   Sun Oct  6 00:00:59 2002
1 vxfs_pfi:34:vxfs:/V1fs:VX+NBU+PFI+FS+2002.10.06.00h00m59s
```

FILES

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

bpplclients(1M)

NAME

`bpplclients`, `bpclclients` - Administer the clients within NetBackup policies

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpplclients

/usr/openv/netbackup/bin/admincmd/bpplclients [policy_name |
        -allunique [-pt policy_type]] [-L | -l | -U | -noheader]
        [-M master_server,...] [-v]

/usr/openv/netbackup/bin/admincmd/bpplclients policy_name [-M
        master_server,...] [-v] -add host_name hardware os [priority]

/usr/openv/netbackup/bin/admincmd/bpplclients policy_name [-M
        master_server,...] [-v] -delete host_name ...

/usr/openv/netbackup/bin/admincmd/bpplclients policy_name [-M
        master_server,...] [-v] -modify host_name [-hardware
        hardware] [-os os] [-priority priority]

/usr/openv/netbackup/bin/admincmd/bpplclients policy_name
        -rename old_client_name new_client_name [-os os] [-hardware
        hardware]
```

DESCRIPTION

Note The command name `bpclclients` is being changed to `bpplclients`. The `bpclclients` command will be completely replaced by `bpplclients` in a future release.

`bpplclients` will do one of the following:

- Produce a listing of clients.
- Add a new client to a policy.
- Delete a list of clients from a policy.
- Modify an existing client in a policy.

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, and there is a single entry for each client.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

The options used with `bpplclients` depend on the form of `bpplclients` being used.

The first form of `bpplclients` has no options and produces a listing of information about the clients for all policies.

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:

policy_name | `-allunique [-pt` *policy_type*`]`

policy_name specifies the name of a policy and lists client information only for the policy with this name.

`-allunique` without [`-pt` *policy_type*] lists client information for all policies defined for NetBackup on the master server.

If you use `-allunique -pt` *policy_type*, where *policy_type* is a specific policy type (such as Sybase), the command lists the client information only for the clients that belong to that type of policy.

If the command line contains neither the *policy_name* nor `-allunique` option, the listing contains client information for all policies.

These options, if used, must be the first option on the command line.

`-L`

List in long format. There is no two-line header 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

There are also four additional fields which can be ignored. These fields are either unused or used for internal processing.

`-l`

List in short format; this produces a terse listing and is also called *raw output mode*. There is no two-line header 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 (the header)

Client name

Hardware type

Operating system

Priority

There are also four additional fields which can be ignored. These fields are either unused or used for internal processing.

This option is useful for scripts or programs that rework the listing contents into a customized report format.

`-U`

List in user format. The listing consists of one line for each client, containing the hardware type, operating system, and client name. A two-line header begins the listing. This is the default format for the listing.

`-noheader`

List without any header. The listing consists of one line for each client, containing the hardware type, operating system, and client name.

`-M` *master_server,. . .*

A list of alternative master servers. This is a comma-delimited list of host names. If this option is present, each master server in the list runs the `bpplclients` command. Each master server in the list must allow access by the system issuing the `bpplclients` command. If an error occurs for any master server, processing stops at that point.

If `bpplclients` is producing a listing, the listing is the composite of the information returned by all the master servers in this list.

If `bpplclients` is adding, deleting, or modifying a client (explained later), the change is made on all the master servers in this list.

`-v`

Selects 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 NetBackup has debug logging enabled (`/usr/openv/netbackup/logs/admin` directory defined).

The next three forms of `bpplclients` affect one or more clients in a single policy. The client will be added, deleted, or have its attributes modified within the policy. This form of `bpplclients` uses the following options:

policy_name

Change the client information for this policy. This option must be the first option on the command line.

`-M` *master_server,. . .*

Explained earlier. This option must precede the `-add`, `-delete`, or `-modify` option on the command line.

`-v`
: Explained earlier. This option must precede the `-add`, `-delete`, or `-modify` option on the command line.

Note The next three options, `-add`, `-delete`, and `-modify`, determine the change that `bpplclients` makes to the clients for the policy. Any of these options, with its accompanying client information, must be the final option on the command line. Only one of these options can be used at a time.

`-add` *host_name hardware os* [*priority*]
: Add a client to the policy. If the local system already has the maximum number of clients defined, an error is returned. The installation default for the maximum number of clients is unlimited for NetBackup Enterprise Server and 4 for NetBackup Server. Specify the host name, hardware type, and operating system (see the definitions below). (*priority* is not implemented at this time)

`-delete` *host_name ...*
: Delete one or more clients from the policy. Up to twenty clients can be deleted at a time. The clients are provided as a space-delimited list of host names.

`-modify` *host_name ...*
: Modify the attributes for a client within a policy. The client has been added to the policy previously. The attribute values that follow the client name replace the previous equivalent attribute values for this client. At least one of the client's attributes must be modified. `-priority` is not implemented at this time.

`-hardware` *hardware*
: The hardware type of this client. Use one of the hardware types as displayed in the dialog box used for adding clients to a policy with the Backup Policy Management utility.

`-os` *os*
: The operating system of this client. Use one of the hardware types as displayed in the dialog box used for adding clients to a policy with the Backup Policy Management utility.

  The values chosen for the hardware and os options must form a valid combination.

`-priority` *priority*
: Not implemented.

The following form of `bpplclients` changes the name of the client in a policy and can also change the operating system and hardware type that is specified for the client. This form of `bpplclients` uses the following options:

policy_name
The policy that has the client. This option must be the first option on the command line.

`-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.

`-hardware` *hardware*
Specifies a different operating system for the client. Use one of the hardware types as displayed in the dialog box used for adding clients to a policy with the Backup Policy Management utility.

`-os` *os*
Specifies a different operating system for the client. Use one of the hardware types as displayed in the dialog box used for adding clients to a policy with the Backup Policy Management utility.

The values chosen for the hardware and os options must form a valid combination.

EXAMPLES

Example 1

While running on the master server, list the clients known to the master server.

```
bpplclients
```

The output returned will look like the following:

```
Hardware          OS                Client
---------------   ---------------   --------------
Novell            Novell 5.1        marge
Windows           WindowsNT         marmot
HP9000            HP-UX 11.0        squash
PC                WindowsNT         tiger
```

This command could also be entered on a client of hat, with the same results.

Example 2

List the clients defined for the policy onepolicy:

```
bpplclients onepolicy
Hardware          OS                Client
---------------   ---------------   --------------
Sun               Solaris7          buffalo
Sun               Solaris8          jeckle
IBM               AIX               streaky
HP9000            HP-UX 11.0            chilly
SGI               IRIX6.5.15        yak
```

```
Tru64-Alpha      TRU 5.1          alpha
Sun              Solaris7         heckle
HP9000           HP-UX            shark
NCR              UNIX             cougar
```

Example 3

Add the client marmot to the policy twopolicy on the master servers serv1 and serv2. marmot's hardware type is HP9000, and marmot's operating system is HP-UX 11.0. The default priority is used. (the command is all on one line)

```
bpplclients twopolicy -M serv1,serv2 -add marmot HP9000 HP-UX 11.0
```

Example 4

Delete the clients marmot and vole from the policy twopolicy on the master servers serv1 and serv2. (the command is all on one line)

```
bpplclients twopolicy -M serv1,serv2 -delete marmot vole
```

Example 5

While running on the master server hat, list client information for policy BackTrack on the master server beaver:

```
bpplclients BackTrack -M beaver
Hardware         OS               Client
---------------  ---------------  --------------
Sun              Solaris7         saturn
```

Example 6

Assume you have a policy called my_policy that has 1 client defined. The client name is pear, the operating system is Solaris2.6, and the hardware type is Solaris.

```
    bpplclients my_policy -rename pear apple -os MacOS \
-hardware MACINTOSH
```

This command changes the client name pear in my_policy to apple. It also changes the os from Solaris to MacOS and hardware from Solaris to MACINTOSH.

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 administrative logging is enabled, the exit status is logged in the administrative daily log under the directory `/usr/openv/netbackup/logs/admin` in the form:

```
bpplclients: EXIT status = exit status
```

If an error occurred, a diagnostic precedes this message.

FILES

`/usr/openv/NetBackup/logs/admin/*`

`/usr/openv/NetBackup/db/policy/`*policy_name*`/clients`

SEE ALSO

`bpadm(1M),bpplinfo(1M)`

bppldelete(1M)

NAME

`bppldelete` - Delete policies from the NetBackup database.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bppldelete policyname
        [-verbose] [-M master_server,...master_server]
```

DESCRIPTION

`bppldelete` deletes policies from the NetBackup database.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

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

Delete policy information for a specific master server(s). For example, to delete policy MWF_PM from master server Saturn, enter:

```
bppldelete MWF_PM -M Saturn
```

`-verbose`

Select verbose mode for logging.

policyname

Specifies the policy to remove from the NetBackup database.

bpplinclude(1M)

NAME

`bpplinclude`, `bpclinclude` - Maintain the list of files automatically backed up by a NetBackup policy.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpplinclude policy_name [-v]
        [-M master_server,...] -add path_name

/usr/openv/netbackup/bin/admincmd/bpplinclude policy_name [-v]
        [-M master_server,...] -delete path_name

/usr/openv/netbackup/bin/admincmd/bpplinclude policy_name [-v]
        [-M master_server,...] -modify {old_path_name
        new_path_name}

/usr/openv/netbackup/bin/admincmd/bpplinclude policy_name [-v]
        [-M master_server,...] -L | -l
```

DESCRIPTION

Note The command name `bpclinclude` is being changed to `bpplinclude`. The `bpclinclude` command will be completely replaced by `bpplinclude` in a future release.

`bpplinclude` maintains the policy file list for a NetBackup policy. This is the list of files 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 pathnames to the policy file list
- Deletes pathnames from the policy file list
- Modifies pathnames in the policy file list
- Displays the policy file list for a policy

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 absolute pathname syntax for your client type, refer to the File-Path Rules topics in the *NetBackup System Administrator's Guide*. The last part of the path can be a filename, 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.

File-Path Rules for does 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.

See the *NetBackup System Administrator's Guide* for additional information on policy file lists.

For database extensions, the input entries are scripts. NetBackup runs these during the backup. See the NetBackup guide that comes with the extension product for additional information.

For certain policy attributes (such as Allow Multiple Data Streams) and extension products (such as NetBackup for NDMP), the entries added to the policy file list may be directives, rather than pathnames. Refer to the *NetBackup System Administrator's Guide* 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.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-add` *path_name*

Add these path_names to the policy file list. 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. This means that `bpplinclude` concatenates two or more comma-delimited pathnames into a single pathname with embedded commas. `bpplinclude` does not verify the syntax or the existence of the pathnames. This option must be the final entry on the command line.

`-delete` *path_name*

Delete these path_names from the policy file list. Refer to `-add` for the pathname-list syntax. Deleting a pathname from the policy file list does not prevent you from recovering any backups or archives for that pathname. This option must be the final entry on the command line.

`-help`

Prints a command line usage message when `-help` is the only option on the command line.

`-L`

Display the contents of the policy file list in long format.

`-l`
Display 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*}
Modify 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 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 issuing the command. If an error occurs for any master server, processing stops at that point in the list. The default is the master server for the system where the command is entered.

`-v`
Select verbose mode for logging. This is only meaningful when running with debug logging turned on (the `/usr/openv/netbackup/logs/admin directory` is defined).

OPERANDS

`policy_name`
Specifies the policy for which the policy file list is to be set.

EXAMPLES

Example 1

While running on another master server kiwi, display the policy file list for policy oprdoc_policy on the master server plum:

```
bpplinclude oprdoc_policy -L -M plum
 Include:           c:\oprdoc
```

Example 2

Illustrate `bpplinclude`'s interpretation of wildcards by adding and deleting pathnames that include one wildcard entry:

```
bpplinclude mkbpolicy -add /yap /y*
```

```
bpplinclude mkbpolicy -L
 Include: /yap
 Include: /y*
bpplinclude mkbpolicy -delete /y*
bpplinclude mkbpolicy -L
 Include: /yap
```

Note The wildcard entry `/y*` for `-delete` is not interpreted by `bpplinclude` 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 when NetBackup is selecting files to be backed up, during the actual backup.

Example 3

Add two entries to the policy file list for a policy, and then modify them:

```
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
```

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
```

(see the Adding Unix Raw Partitions to the File List section of the *NetBackup System Administrator's Guide*).

Example 5

Display the policy file list for the policy mkb_policy:

```
bpplinclude mkb_policy -l
 INCLUDE /etc/services
 INCLUDE /etc/aliases
 INCLUDE /usr/bin
```

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 administrative logging is enabled, the exit status is logged in the administrative daily log under the directory `/usr/openv/netbackup/logs/admin` in the form:

`bpplinclude: EXIT status =` *exit status*

If an error occurred, a diagnostic precedes this message.

FILES

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/policy/`*policy_name*`/includes`

SEE ALSO

`bpplclients(1M),bpplinfo(1M),bpplsched(1M),bppldelete(1M), bppllist(1M)`

bpplinfo(1M)

NAME

bpplinfo, bpclinfo - Manage or display policy attributes for NetBackup.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpplinfo policy_name -L | -l |
        -U [-v] [-M master_server,...]

/usr/openv/netbackup/bin/admincmd/bpplinfo policy_name -set |
        -modify [-v] [-active | -inactive] [-blkincr flag]
        [-collect_tir_info value] [-compress flag] [-crossmp
        flag] [-disaster flag] [-ef effective_time] [-encrypt flag]
        [-follownfs flag] [-keyword "keyword phrase"] [-M
        master_server,...] [-multiple_streams flag] [-policyjobs
        max_jobs] [-pool label] [-priority flag] [-pt policy_type]
        [-residence label] [-rfile flag] [-ut] [-chkpt [1|0]]
        [-chkpt_intrvl interval]

/usr/openv/netbackup/bin/admincmd/bpplinfo policy_name -help
```

DESCRIPTION

Note The command name bpclinfo is being changed to bpplinfo. The bpclinfo command will be completely replaced by bpplinfo in a future release.

bpplinfo initializes, modifies, or displays the attribute values for a NetBackup policy. This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

The options used with bpplinfo depend on the form of bpplinfo being used.

The first form of bpplinfo displays a policy. The following options apply to this form:

policy_name -L | -l | -U

List information for this policy. This is a required option.

-L specifies a long list type and produces a listing with one policy attribute per line, in the format *policy_attribute*: *value*. The value may be expressed both in numeric and name form. Fields in the list include:

Policy Type

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

Backup Copy

Disaster Recovery

Max Frag Size

Residence

Volume Pool

`-l` specifies a short list type and produces a terse listing. This option is useful for scripts or 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, effective_date, policy ID

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 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 has debug logging enabled (`/usr/openv/netbackup/logs/admin` directory defined).

`-M` *master_server,...*

A list of alternative master servers. This is a comma-delimited list of hostnames. 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 issuing the `bpplinfo` command. If an error occurs for any master server, processing terminates at that point.

For the display form of `bpplinfo`, the report is the composite of the information returned by 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 instance, if the policy type is *MS-Windows-NT*, `bpplinfo` accepts the options `-compress` and `-crossmp`. When `bpplinfo` completes, it returns a zero status. However, NetBackup's subsequent handling of the policy with the `MS-Windows-NT` policy type is as though the options had not been 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. This is 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 for temporarily inactivating a policy to prevent schedules from being used.

`-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`, do perform block-level-incremental backups.

If `0`, do not perform block-level-incremental backups.

`-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 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. Files deleted before the time of the selected backup are not restored. After enabling this attribute, NetBackup starts collecting additional information beginning 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.

`-compress` *flag*

`0` (disabled) or `1` (enabled). Specifies whether to compress files or not. If 1, the files selected are compressed by the client software onto the media. Compression may increase total backup time. If 0, the files are not compressed onto the media. This is the default.

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 that are on the same file system as the selected file path. This is the default.

This attribute can affect the **Follow NFS** policy attribute, which applies only to NetBackup Enterprise Server. Refer to the NetBackup system administrator's guide for more details.

`-disaster 0|1`

Collect information required 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

`-ef` *`effective time`*
This time specifies the time the policy will be active.

`-encrypt` *flag*
`0` (disabled) or `1` (enabled). Specifies whether files should be encrypted or not.

If `1`, encryption is enabled.

`-followfs 0|1`

Note *The* `followfs` *option applies only to NetBackup Enterprise Server*

`0` (disabled) or `1` (enabled). Specifies whether to follow NFS mount points or not. For policy types MS-Windows-NT and OS/2, 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. This is the default.

The behavior of this attribute varies somewhat depending on the setting of the **Cross Mount Points** attribute. Refer to the *NetBackup System Administrator's Guide* for more details.

`-keyword "`*keyword phrase*`"`
The value will be associated with all backups created using this policy. The keyword phrase can be used to link related policies. It can also be used during restores to search only for backups that have the keyword phrase associated with them.

`-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`, do not allow multiple data streams.

policy_name `-set | -modify`
Initialize or modify attributes for this policy. This is a required option.

`-set` initializes (or reinitializes) attributes for the policy to their default values, except for those attributes set by options on the current command line.

`-modify` modifies attributes for the policy. Attributes that are not explicitly set by options on the current command line do not change their values.

`-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 `/usr/openv/volmgr/bin/vmpool -listall`.

`-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). *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 effective maximum number of jobs in this instance is 8 for NetBackup and 2003 for NetBackup Enterprise Server.

`-priority` *flag*

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):

`Informix-On-BAR`

`MS-Exchange-Server`

`MS-SQL-Server`

`MS-Windows-NT`

`NDMP`

`NetWare`

`Oracle`

`OS/2`

`Standard`

`Sybase`

Note *The following policy types apply only to NetBackup Enterprise Server.*

AFS

DataTools-SQL-BackTrack

DB2

FlashBackup

SAP

Split-Mirror

`-residence` *label*

Specifies the label of the storage unit for storing the backups created according to this schedule. The default is Any_available. This allows the policy to use any storage unit which has the attribute On Demand Only? set to No. If the policy needs to use a specific storage unit or the storage unit desired has the attribute On Demand Only? set to Yes, then specify the storage unit. 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`, do not allow 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.

`-ut`

Any of the date/time arguments that follow `-ut` will be accepted as UNIX time, instead of the standard time format. The `-ut` option is used primarily for Java.

The third form of `bpplinfo` (not shown in the synopsis) shows usage information and has only one option as follows:

`-help`

Prints a command line usage message when `-help` is the only option on the command line.

EXAMPLES

Note *References to Follow NFS Mounts in these examples apply only to NetBackup Enterprise Server.*

Example 1

To set the storage unit of the policy tstpolicy to tstunit and view the results, perform the following:

```
bpplinfo tstpolicy -modify -residence tstunit
bpplinfo tstpolicy -L
Policy Type:         Standard (0)
  Active:             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
  Multiple Streams:   1
  Disaster Recovery:  0
  Max Frag Size:      0 MB  (1048576 MB)
  Residence:          tstunit
  Volume Pool:        NetBackup
```

Example 2

To set the attributes of policy tstpolicy back 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
  Max Frag Size:      0 MB  (1048576 MB)
```

```
   Residence:          -
   Volume Pool:        NetBackup
```

Example 3

The following is an example of a short listing for the policy 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*
POOL NetBackup *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL* *NULL*
FOE 0 0 0 0 0 0 0 0 0 0
```

FILES

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/policy/`*policy_name*`/info`

bppllist(1M)

NAME

`bppllist` - List policy information.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bppllist [policyname] [-L | -l
        | -U] [-allpolicies] [-M master_server,...master_server]
        [-hwos] [-byclient client] [-keyword "keyword
        phrase"][-verbose]
```

DESCRIPTION

`bppllist` lists policies within the NetBackup database.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-allpolicies`
: Lists all policies.

`-hwos`
: Lists possible hardware and the operating system.

`-L`
: Displays a full listing.

`-l`
: Displays information in raw output mode.

`-M` *master_server,...master_server*
: Lists policy information for a specific master server(s).

`-U`
: Displays information in the style used by `xbpadm`.

`-byclient` *client*
: Lists policy information for all policies containing the client indicated.

`-keyword` *"keyword phrase"*
: The value will be associated with all backups created using this policy. The keyword phrase can be used to link related policies. It can also be used during restores to search only for backups that have the keyword phrase associated with them.

policyname
: Specifies the policy in the NetBackup database.

-verbose
: Select verbose mode for logging.

bpplsched(1M)

NAME

bpplsched, bpclsched - Add, delete, or list NetBackup schedules.

SYNOPSIS

/usr/openv/netbackup/bin/admincmd/bpplsched *policy_name* [-v] [-M *master_server*, . . .] -add *sched_label* [-st *sched_type*] [-freq *frequency*] [-mpxmax *mpx_factor*] [-number_copies *number*] [-rl *retention_level*[, *rl-copy2*, . . . , *rl-copyn*]] [-residence *storage_unit_label*[, *stunit-copy2*, . . . *stunit-copyn*]] [-pool *volume_pool_label*[, *pool-copy2*, . . . *pool-copyn*]] [-fail_on_error 0|1[,0|1,...0|1][-window *start_duration*]] [-cal 0|1|2] [-ut] [-incl *mm/dd/yyyy*] [-excl *mm/dd/yyyy*] [-weekday *day_name_week*] [-dayomonth 1-31 or l]

/usr/openv/netbackup/bin/admincmd/bpplsched *policy_name* [-v] [-M *master_server*, . . .] -delete *sched_label*

/usr/openv/netbackup/bin/admincmd/bpplsched *policy_name* [-v] [-M *master_server*, . . .] -deleteall

/usr/openv/netbackup/bin/admincmd/bpplsched *policy_name* [-v] [-M *master_server*. . .] [-L | -l | -U] [-label *sched_label*]

DESCRIPTION

Note The command name bpclsched is being changed to bpplsched. The bpclsched command will be completely replaced by bpplsched in a future release.

bpplsched will do one of the following:

- Add a new schedule to a policy.
- Delete one or more schedules from a policy.
- Delete all the schedules from a policy.
- List one or all schedules in a policy.

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.

When the listing option is used there is 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, 2 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. This is also true for the `u_wind` entry in the `-L` display.

Line 2: SCHEDWIN, seven pairs of the form *start*,*duration*, expressing the start and duration of the window for each day of the week, starting 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, `bpplsched` performs the operation on each of the master servers listed. For instance, if `bpplsched` is adding a schedule, `bpplsched` adds the schedule to the policy on each of the master servers listed for `-M`. If the `-M` option is used on a listing request, the listing is the composite of the information returned by 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 `bpplschedrep`.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

These options are common to all forms of `bpplsched`:

policy_name
: The name of the policy that contains the schedules. The policy must exist before running this command. This option is required, and must be the first one on the command line.

`-help`
: Prints a command line usage message when `-help` is the only option on the command line.

`-M` *master_server*, . . .

A list of alternative master servers. This is a comma-separated list of host names. If this option is present, each master server in the list runs the `bpplsched` command. Each master server in the list must allow access by the system issuing the `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, processing terminates at that point.

If `bpplsched` is producing a listing, the listing is the composite of the information returned by all the master servers in this list.

If `bpplsched` adds or deletes a schedule, all master servers in this list receive the change.

`-v`

Selects verbose mode. This option causes `bpplsched` to log additional information for debugging purposes. The information goes into the NetBackup administration debug log. This option is meaningful only when NetBackup has debug logging enabled (`/usr/openv/netbackup/logs/admin` directory defined).

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 suboptions for the `-add` option explained below. These are attributes of the schedule being added. Refer to the *NetBackup System Administrator's Guide* for details on schedules and their attributes.

`-cal 0|1|2`

Indicates whether `bpplschred` is following 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 retires after run day

`-dayomonth 1-31 l`

Specifies the day 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 schedule the 15th day of every month, enter:

```
-dayomonth 15
```

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 backups initiated according to this schedule. Valid range for this option is 0 through 2419200 (number of seconds in four weeks). When 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.

`-mpxmax` *mpx_factor*
This is the maximum number of jobs for this schedule that NetBackup will multiplex 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 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 minimum value is 1. The maximum value is 4 or the Maximum Backup Copies global parameter, whichever is smaller. The default is 1.

`-pool` *volume_pool_label*`[,`*pool-copy2*`, . . .` *pool-copyn*`]`
This is the name of the volume pool. This choice overrides the policy-level volume pool. Entering "*NULL*" causes NetBackup to use the volume pool specified at the policy level. The default is to use the volume pool 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 specifying `-number_copies` greater than 1, specify a pool for each copy.

`-residence` *storage_unit_label*`[,`*stunit-copy2*`, . . .` *stunit-copyn*`]`
This is the name of the storage unit, which specifies the location of the backup images. The value "*NULL*" causes NetBackup to use the storage unit specified at the policy level. The default is for NetBackup to use the

storage unit 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 specifying `-number_copies` greater than 1, specify a residence for each copy.

`-rl` *retention_level*`[,`*rl-copy2*`,...,` *rl-copyn*`]`

The retention level determines how long to retain backups and archives. The retention_level is an integer between 0 and 24. The default retention level is 1. Valid retention levels and their corresponding default retention times are listed below.

When specifying `-number_copies` greater than 1, specify a retention level for each copy.

CAUTION: Because the retention period associated with each level can be changed by using the NetBackup administration interface, 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 making any changes with this command. Otherwise, backups could expire sooner than you expect, resulting in loss of data.

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 - 24 infinite

`-st` *sched_type*

This is the type of the schedule. The default schedule type is FULL. Here are the possible values, with their meanings, for this attribute:

`FULL` - full

`INCR` - differential incremental

`CINC` - cumulative incremental

`UBAK` - user backup

`UARC` - user archive

`-ut`

Any of the date/time arguments that follow `-ut` will be accepted as UNIX time, instead of the standard time format. The `-ut` option is used primarily for Java.

`-weekday` *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.

For example, to instruct the policy to run the second Monday of the month, enter:

```
-weekday Monday 2
```

`-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 is the number of seconds since midnight. This is an integer between 0 and 86399 (there are 86400 seconds in a day).

duration is the length of time that the window remains open. The time unit is seconds. This is a non-negative integer.

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. The elements of the sched_label list must be separated by 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. This is the default list type. This 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 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 listing, but it has fewer entries. Most attribute values are descriptive terms, rather than numbers.

EXAMPLES

Example 1

In this example, `bpplsched` lists 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 running on the system hat, 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:
 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
```

Example 3

The following example adds a new schedule, full_2, to the policy tstpolicy on beaver, and then lists the new schedule in Long mode. These commands run on the system hat:

```
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
 Monday      000:00:00  000:00:00
 Tuesday     000:00:00  000:00:00
 Wednesday   000:00:00  000:00:00
 Thursday    000:00:00  000:00:00
 Friday      000:00:00  000:00:00
 Saturday    000:00:00  000:00:00
```

Example 4

In this example, `bpplsched` deletes the schedules, full_3, user, user_2, and user_3 from policy tstpolicy:

```
bpplsched tstpolicy -delete full_3 user user_2 user_3
```

Example 5

In this example, `bpplsched` lists 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       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


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
```

Example 6

In this example, `bpplsched` adds a new schedule, full, with a window from 11 pm to midnight. The second `bpplsched` lists the information for schedule full:

```
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
 Fail on Error:0
 Residence:       (specific storage unit not required)
Volume Pool:     (same as policy volume pool)
Daily Windows:
      Sunday     23:00:00  -->  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   23:00:00  -->  Saturday   24:00:00
```

FILES

/usr/openv/netbackup/logs/admin/*

/usr/openv/netbackup/db/policy/*policy_name*/schedule

SEE ALSO

bpplschedrep(1M)

bpplschedrep(1M)

NAME

bpplschedrep, bpclschedrep - Modify the attributes of a NetBackup schedule.

SYNOPSIS

/usr/openv/netbackup/bin/admincmd/bpplschedrep *policy_name* *sched_label* [-M *master_server*, . . .] [-v] [-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*] [-dayomonth 1-31 l] [-delweekday *day_name week*] [-deldayomonth 1-31 l] [-ci] [-ce] [-cw] [-cd] [-number_copies *number*][-rl *retention_level*[, *rl-copy2*, . . . , *rl-copyn*]] [-fail_on_error 0|1[,0|1,...,0|1]] [-residence *storage_unit_label*[, *stunit-copy2*, . . . *stunit-copyn*]] [-pool *volume_pool_label*[, *pool-copy2*, . . . *pool-copyn*]] [-(0..6) start duration]

DESCRIPTION

Note The command name bpclschedrep is being changed to bpplschedrep. The bpclschedrep command will be completely replaced by bpplschedrep in a future release.

bpplschedrep changes the attributes of a NetBackup schedule. The schedule and policy named by bpplschedrep should already exist when this command is run. If the -M option is used, bpplschedrep changes the schedule on each of the master servers listed.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's 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 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 is a non-negative integer.

`-cal 0|1|2`

Indicates whether `bpplschedrep` is following 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 retires after run day

`-dayomonth 1-31 l`

Specifies the day 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 schedule the 15th day of every month, enter:

```
-dayomonth 15
```

To run the last day of every month, enter:

```
-dayomonth l
```

`-deldayomonth 1-31 l`

Specifies a day of every month to be excluded 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.

For example, to exclude the 20th day of every month from the schedule, enter:

```
-deldayomonth 20
```

`-delweekday` *day_name week*

Specifies a day of the week and the week of the month to be excluded as a run day from 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.

For example, to exclude the second Monday of the month, 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`
: 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, representing 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.

`-incl` *mm/dd/yyyy*
: Indicates to include this single date.

`-M` *master_server*, . . .
: A list of alternative master servers. This is a comma-separated list of hostnames. 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 issuing the `bpplschedrep` command. If an error occurs for any master server, processing terminates at that point.

  The schedule attributes will be modified on all the master servers in this list.

`-mpxmax` *mpx_factor*
: This is 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 NetBackup Server and 1 through 32 for NetBackup Enterprise Server. A value of 1 specifies no multiplexing and a value greater than 1 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 information on multiplexing refer to the multiplexing topic in the *NetBackup System Administrator's Guide*.

`-number_copies` *number*

Specify the number of simultaneous backup copies. The minimum value is 1. The maximum value is 4 or the Maximum Backup Copies global parameter, whichever is smaller. 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*`, . . .` *pool-copyn*`]`

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 which contains this schedule.

Specify a pool for each copy.

To display the configured volume pools, run `/usr/openv/volmgr/bin/vmpool -listall`.

`-residence` *storage_unit_label*`[,` *stunit-copy2*`, . . .` *stunit-copyn*`]`

Specifies the label(s) of the storage unit to be used for storing the backups created according to this schedule. If "*NULL*" is specified, the residence for the schedule defaults to the residence of the policy which contains this schedule. If the residence value is a storage unit label, the residence for the schedule becomes that storage unit, overriding 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*`[,` *rl-copy2*`, . . . ,` *rl-copyn*`]`

Specifies how long NetBackup retains the backups that it creates using this schedule. Valid retention levels and their corresponding default retention times are listed below.

Specify a retention level for each copy.

Caution Because the retention period associated with each level can be changed by using the NetBackup administration interface, 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 making any changes with this command. Otherwise, backups could expire sooner than you expect, resulting in loss of data.

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 - 24 infinite

NetBackup keeps the information about the backups for the specified time. Then it deletes information about them. Once deleted, the files in the backups are unavailable for restores. When all the backups on a volume have expired, the volume can be reassigned.

sched_label

The name of the schedule to be changed. This schedule has been previously created.

`-st` *sched_type*

Specifies the type of backup this schedule performs. Schedule types fall into two main categories: automatic and user. 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

`FULL` (full backup)

`INCR` (differential incremental backup)

`CINC` (cumulative incremental backup)

`UBAK` (user backup)

`UARC` (user archive)

`-weekday` *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.

For example, to instruct the policy to run the second Monday of the month, enter:

```
-weekday Monday 2
```

`-v`

Selects 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 has debug logging enabled (`/usr/openv/netbackup/logs/admin` directory defined).

EXAMPLES

Example 1

Set the frequency for a schedule.

```
bpplschedrep mkbpolicy incr -freq 604800
```

This sets to 1 week the frequency with which automatic backups will be performed for the schedule incr in policy mkbpolicy.

Example 2

For Saturday and Sunday of each week, have the window for schedule full in policy newpolicy open at 10 pm instead of 11 pm. Also, have the window duration be 2 hours instead of 1 hour. `bpplschedrep` resets the windows, and `bpplsched` lists the new schedule values.

```
bpplschedrep newpolicy full -0 79200 7200 -6 79200 7200
bpplsched 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
```

FILES

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/policy/`*policy_name*`/schedule`

SEE ALSO

`bpplsched(1M)`

bppolicynew(1M)

NAME

`bppolicynew`, `bpclassnew` - Create, copy, or rename a NetBackup policy.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bppolicynew policy_name
        [-verbose] [-M master_server, ...]

/usr/openv/netbackup/bin/admincmd/bppolicynew policy_name
        -sameas existing_policy_name [-verbose] [-M
        master_server,...]

/usr/openv/netbackup/bin/admincmd/bppolicynew existing_policy_name
        -renameto policy_name [-verbose] [-M master_server, ...]
```

DESCRIPTION

Note The command name `bpclassnew` is being changed to `bppolicynew`. The `bpclassnew` command will be completely replaced by `bppolicynew` in a future release.

`bppolicynew` performs one of the following operations on a NetBackup policy:

- Create a new NetBackup policy with default attribute values
- Create a new NetBackup policy with the same attributes as an existing policy r
- Rename an existing NetBackup policy

When `bppolicynew` runs without `-sameas` or `-renameto`, it creates a new NetBackup policy with default attribute values. If `-M` is present, the defaults 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 an image listing for the renamed policy does not include the images that were created before the policy was renamed. `bppolicynew` does not rename a policy to have the same name as an existing policy.

The NetBackup command `bpplinfo` replaces the policy-attribute defaults with new values. `bpplclients`, `bpplinclude`, and `bpplsched` 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.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

See the *NetBackup System Administrator's Guide* for additional information on policies.

OPTIONS

policy_name

The name of a NetBackup policy which `bppolicynew` creates or the name to which `bppolicynew` changes an existing policy. There is 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 any spaces between characters.

existing_policy_name

The name of a NetBackup policy which already exists when `bppolicynew` runs. There is no default value.

`-renameto`

Change the name of the existing policy to the new policy name.

`-sameas`

Create a new policy, copying its characteristics from the existing policy.

`-help`

Prints a command line usage message when `-help` is the only option on the command line.

`-M` *master_server,...*

A list of master servers. This 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 issuing the command. If an error occurs for any master server, processing 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 is only meaningful when running with debug logging turned on (that is, the directory `/usr/openv/netbackup/logs/admin` is defined).

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 plum:

```
bppolicynew ishkabibble -M plum
bppllist ishkabibble -U -M plum
------------------------------------------------------------
Policy Name:        ishkabibble
  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:           (specific storage unit not required)
  Volume Pool:         NetBackup
  Keyword:             (none specified)

  Clients:      (none defined)

  Include:      (none defined)

  Schedule:     (none defined)
```

Example 2

Create a new policy, mypolicy_copy from the existing policy mypolicy. `bppllist` shows that mypolicy_copy has the same attributes as mypolicy. For brevity, most of the schedule information is omitted here:

```
bppolicynew mypolicy_copy -sameas mypolicy
bppllist 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
                 SGI           IRIX6.5.15    mango

  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

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
               SGI           IRIX6.5.15    mango

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:

```
bppllist
 mypolicy
 policy_old
 test
bppolicynew policy_old -renameto policy_new
bppllist
 mypolicy
 policy_new
```

```
test
```

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 administrative logging is enabled, the exit status is logged in the administrative daily log under the directory `/usr/openv/netbackup/logs/admin` in the form:

`bppolicynew: EXIT status =` *exit status*

If an error occurred, a diagnostic precedes this message.

FILES

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/policy/`*policy_name*

SEE ALSO

`bpplclients(1M)`, `bpplinfo(1M)`, `bpplsched(1M)`, `bppldelete(1M)`, `bppllist(1M)`

FILES

bprd(1M)

NAME

bprd - Initiates the NetBackup request daemon.

SYNOPSIS

```
/usr/openv/netbackup/bin/bprd [-verbose]
```

DESCRIPTION

bprd is responsible for starting automatic client backups and 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 when bprd starts:

1. After disassociating itself from the terminal, the daemon
   - Logs a message indicating that it has 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.
2. 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.
3. 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
   ```

4. After binding to its port, the program starts scheduling automatic client backups, accepting requests from client machines for file restores or user backups or archives, and accepting administrative requests from the server.

You can use bprdreq -terminate to terminate bprd. Terminating bprd does not terminate bpdbm.

OPTIONS

-verbose
: Specifies that bprd will write 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

bpadm(1M),bpdbm(1M)

bprecover(1M)

NAME

`bprecover` - Recover selected NetBackup related catalogs.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bprecover [-v]
-l -m media_id -d density [-v]
-l -dpath disk_path [-v]
-l -tpath tape_device_path [-v]
-l -opath optical_device_path [-v]
-r [all | ALL | image_number] -m media_id -d density [-stdout]
          [-dhost destination_host] [-v]
-r [all | ALL | image_number] -dpath disk_device_path [-stdout]
          [-dhost destination_host] [-v]
-r [all | ALL | image_number] -tpath raw_tape_device_path [-stdout]
          [-dhost destination_host] [-v]
-r [all | ALL | image_number] -opath optical_device_path [-stdout]
          [-dhost destination_host] [-v]
```

Note Stop `bpdbm` and `bprd` before using this command. Also, ensure that `bpcd` is running on any system that is being recovered.

DESCRIPTION

`bprecover` initiates the NetBackup utility for restoring the NetBackup internal databases called catalogs and recovers catalogs that were backed up by using the procedures described in the NetBackup system administrator's guide. Use `bprecover` only if catalogs were destroyed on disk.

The command has two main modes: list and recover. List shows the contents of a backup media or disk path. Recover recovers the catalog files.

You must have root privileges to execute this command.

OPTIONS

`-l`

Lists the header information from the specified media or disk path.

`-m` *media_id* `-d` *density*

Specifies the media ID and the density of the media from which to recover files. `ltid` and vmd must be running when you use the `-m` option.

media_id must be six or less characters and must be defined in the Media Manager volume database.

density must be one of the following:

`4mm` (4-mm cartridge)

`8mm` (8-mm cartridge)

`dlt` (dlt cartridge)

`dlt2` (dlt cartridge alternate)

`qscsi` (1/4-in 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)

`odiskwm` (Optical disk-write many)

`odiskwo` (Optical disk-write once)

`-dpath` *disk_path*

`-tpath` *tape_path*

`-opath` *optical_path*

Specifies a raw device path. If `-m` and `-d` are not specified. Use `-dpath`, `-opath`, or `-tpath` to specify a raw device path. Stop the Media Manager device and volume daemons (`ltid` and `vmd`) when using one of these options.

Note Some platforms require a Berkeley-style close device for the `tpath` option. This is the path with b in the device name (for example on a Solaris system, it could be `/dev/rmt/0cbn`). You will get an I/O error if you do not specify a Berkeley style close device on platforms that require it.

`-r [all | ALL |` *image_number*`]`

Recovers images from the specified media or disk path. There are three modes of recovery available with `-r`:

If `-r all` (or `ALL`) is specified, recover all the images contained in the specified media or disk path.

If `-r` *image_number* is specified, recover only the selected image number from the specified media or disk path.

If `-r` is specified by itself, `bprecover` interactively prompts and asks if you want to recover the images contained in the specified media or disk path.

`-stdout`

Specifies that the selected backup image be written to stdout instead of automatically being restored. This option is useful, for example, if only one individual file was lost and you want to restore it without restoring the rest of the catalog files in the image.

Note You cannot specify `-r ALL` with `-stdout` because the `-stdout` option permits only one file image to be read at a time.

`-dhost` *destination_host*

Specifies the host to which the selected catalog is restored. Normally, catalogs are restored to the host where the data originated (as displayed with the `-l` option). The `-d` option makes it possible to restore the catalog to another host.

Caution Use the `dhost` option with EXTREME caution, since it can overwrite existing catalogs on the destination host. To permit recovery in case you unintentionally overwrite the wrong catalogs, you can move existing catalogs to a temporary directory on the destination host.

The following NetBackup client software must be installed on the destination host:

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

and

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

Note Do not specify `-r all` (or `ALL`) with `-dhost` when using this command. Either explicitly specify an image (for example, `-r 2`) or use the interactive mode (`-r`).

`-v`

Selects verbose mode. This is meaningful only when running with debug logging turned on (that is, when the `/usr/openv/netbackup/logs/admin` directory exists).

EXAMPLES

Example 1

List the backup header information for catalog backup that was done to disk path `/disk/bpbackup`.

```
# bprecover -l -dpath /disk1/bpbackup
```

```
Database Backup Information from /disk1/bpbackup

Created:      02/20/2002 12:13:47
Server:       bphost

            Path
            ----
IMAGE1      /usr/openv/netbackup/db
IMAGE2      /usr/openv/volmgr/database
```

Example 2

List the backup header information from media ID JBL29, which is density 8mm.

```
# bprecover -l -m JBL29 -d 8mm
 Database Backup Information from JBL29

 Created:      01/22/02 07:50:51
 Server:       bphost
 Block size:   32768

           Path
           ----
 IMAGE1      /usr/openv/netbackup/db
 IMAGE2      /usr/openv/volmgr/database
```

Example 3

Recover the `/usr/openv/netbackup/db` files from disk path `/disk1/bpbackup`.

```
# bprecover -r 1 -dpath /disk1/bpbackup
Recovering bphost:/usr/openv/netbackup/db
```

◆ Example 4

Recover all the backed up catalogs from media ID JBL29.

```
# bprecover -r ALL -m JBL29 -d 8mm
 Recovering bphost:/usr/openv/netbackup/db
 Recovering bphost:/usr/openv/volmgr/database
```

Example 5

Interactively restore selected images. Use raw tape path `/dev/rmt/1cbn`. Assume the media that is loaded into the drive is the same one as in Example 4.

```
# bprecover -r -tpath /dev/rmt/1cbn
 Recover bphost:/usr/openv/netbackup/db y/n (n)? n
 Recover bphost:/usr/openv/volmgr/database y/n (n)? y
 Recovering bphost:/usr/openv/volmgr/database
```

Example 6

Recover a single file from image 1 on JBL29.

```
# bprecover -r 1 -m JBL29 -d 8mm -stdout | /bin/tar -xvf
 - /usr/openv/netbackup/file_to_recover
 Writing bphost:/usr/openv/netbackup/db to stdout
```

Example 7

Restore an image to another host by using the `-dhost` *destination_host* option.

```
# bprecover -r -m ODL08B -d odiskwm -dhost giskard
Recover bphost:/usr/openv/netbackup/db to host giskard y/n (n)? n
Recover bphost:/usr/openv/volmgr/database to host giskard y/n (n)? y
Recovering bphost:/usr/openv/volmgr/database to host giskard
```

ERRORS

If any errors occur during the recover operation, error messages are written to stderr.

FILES

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/*`

`/usr/openv/volmgr/database/*`

SEE ALSO

`tpreq(1)` (Media Manager command)

NetBackup Troubleshooting Guide for information on disaster recovery.

bprestore(1)

NAME

bprestore - Restores files from the NetBackup server.

SYNOPSIS

```
/usr/openv/netbackup/bin/bprestore [-A | -B] [-drs] [-F
        file_options] [-K] [-l | -H | -y] [-r] [-T] [-L progress_log
        [-en]] [-R rename_file] [-C client] [-D client] [-S
        master_server] [-t policy_type] [-p policy] [-s date] [-e date]
        [-w [hh:mm:ss]] [-k "keyword_phrase"] -f listfile | filenames
```

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 directory path that was previously included in the restore by placing an exclamation mark (!) in front of the file or directory path (does not apply to NDMP restores). The exclude capability is useful, for example, if you want to exclude part of a directory from the restore.

> Note: If a policy, schedule type, or date range is not specified then bprestore will start with the most recent full backup image and include all subsequent ncremental and differential backup images. From these images the most recent copy of a file will be restored.

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 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. It is also possible to restore files that were backed up or archived on another client (-C option). You must be validated by the NetBackup administrator to restore from other clients.

bprestore writes informative and error messages to a progress-log file if you create the file prior to running 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 named /usr/openv/netbackup/logs/bprestore with public-write access. bprestore then creates an debug log file in this directory.

In addition, if a nonroot user specifies `USEMAIL` = *mail_address* in their `$HOME/bp.conf` file, 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 files and 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 is a problem, use the `-f` option to restore the files.

Use the `bplist` command to display information on the files and directories that were backed up or archived.

OPTIONS

`-A | -B`

Specifies whether to restore from archives (`-A`) or backups (`-B`). The default is `-B`.

`-drs`

Allows files to be restored 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.

`-F` *file_options*

Allows either Backup Exec files to be restored, or both Backup Exec and NetBackup files to be restored. The default (`-F` is not specified), is to restore only NetBackup files.

To restore only Backup Exe files specify:

```
-F 524288
```

To restore Backup Exe and NetBackup files specify:

```
-F 1048576
```

`-K`

Specifying this option causes `bprestore` to keep existing files rather than writing over them when restoring files with the same name. The default is to overwrite existing files.

Note The `-l | -H | -y` options apply only when restoring UNIX files to a UNIX system.

`-l | -H | -y`

Specifying `-l` renames the targets of UNIX links by using the `-R` *rename_file* option in the same way as when renaming files.

Specifying `-H` renames UNIX hard links by using the `-R` *rename_file* option in the same way as when renaming files. Soft links are unchanged.

Specifying `-y` renames UNIX soft links by using the `-R` *rename_file* option in the same way as when renaming files. Hard links are unchanged.

See Example 5 in the EXAMPLES section.

`-r`

Specifying this option restores raw partitions instead of file systems.

`-L` *progress_log* `[-en]`

Specifies the name of an existing file in which to write progress information.

For example: `/home/tlc/proglog`

The default is to not use a progress log.

Include the `-en` option to generate a log in English. The name of the log will contain the string `_en`. This option is useful to support personnel assisting in a distributed environment where differing locales may create logs of various languages.

`-R` *rename_file*

Specifies the name of a file with name changes for alternate-path restores.

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 using the original path.

For example, the following entry renames `/usr/fred` to `/usr/fred2`:

```
change /usr/fred to /usr/fred2
```

`-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.

`-D` *client*

Specifies a destination client. This can be done by a root user on the master server in order to direct the restored files to a machine other than the client specified with the `-C` option. The default is the current client name.

`-S` *master_server*

Specifies the name of the NetBackup server. The default is the first server found in the `/usr/openv/netbackup/bp.conf` file.

`-t` *policy_type*

Specifies one of the following numbers corresponding to the policy type. The default is 0 for all clients except Windows NT/2000, where the default is 13.

`0` = Standard

`4` = Oracle

`6` = Informix-On-BAR

`7` = Sybase

`10` = NetWare

`13` = MS-Windows-NT/2000

`14` = OS/2

`15` = MS-SQL-Server

`16` = MS-Exchange-Server

`19` = NDMP

Note *The following policy types apply only to NetBackup Enterprise Server.*

`11` = DataTools-SQL-BackTrack

`17` = SAP

`18` = DB2

`20` = FlashBackup

`21` = Split-Mirror

`22` = AFS

`-p` *policy*

Specifies the policy for which the backups or archives were performed.

`-s` *date*

`-e` *date*

Specifies the start and end date range for the listing. The `bprestore` command restores only files from backups or archives that occurred within the specified start and end date range.

The format of *`date`* depends on the user's locale setting. See the NOTES section for more information. For the C locale, the date syntax is as follows:

mm/dd/yy [*hh*[*:mm*[*:ss*]]]

`-s` specifies a start date and time for the restore window. `bprestore` restores files only from backups or archives that occurred at or after the specified date and time.

The valid range of dates are 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 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 will be restored.

`-e` specifies an end date and time for the restore window. `bprestore` restores only files in backups or 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). The bprestore command restores the file that has the specified backup date and time or the file that is the most recent backup preceding the end date and time. The default is the current date and time."

`-T`

Specifies a true-image restore, where only files and 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 meeting the specified criteria are restored, even if they were deleted.

When the `-T` option is specified, the image 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.

`-w [`*hh:mm:ss*`]`

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

The date and time format are dependent on the user's locale. See NOTES.

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.

Specifying 0 or not specifying a time, means wait indefinitely for the completion status.

`-k "`*keyword_phrase*`"`

Specifies a keyword phrase for NetBackup to use when searching 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 `bparchive` command.

You can use this option in place of or in combination with the other restore options in order to make it easier to restore your backups and archives. The following meta characters can simplify the task of matching keywords or parts of keywords in the phrase:

* matches any string of characters.

? matches any single character.

[ ] matches one of the sequence of characters specified within the brackets.

[-] matches one of the range of characters 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 ('...') to avoid conflict with the UNIX shell.

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

`-f` *listfile*

Specifies a file (*listfile*) containing a list of files to be restored and can be used instead of the *filenames* option. In *listfile,* list each file path on a separate line.

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

To restore 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 are restoring. For example:

```
/home
/etc
/var
```

To restore 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 are restoring.

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 start and end date and time specified on the command line is used unless a line in *listfile* overrides it. The dates may change from line to line.

The user's locale affects how dates and time are specified. See NOTES.

You can exclude a file or directory path that was previously included in the restore by placing an exclamation mark (!) in front of the file or directory path (except when performing NDMP restores).

The following is an example that uses *filepathlen filepath*:

```
5 /home
4 /etc
4 /var
19 /home/abc/test file
12 !/etc/passwd
```

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, following all other options. You must also specify absolute file paths. You can exclude a file or directory path that was previously included in the restore by placing an exclamation mark (!) in front of the file or directory path (except when performing NDMP restores).

NOTES

The format that you must use for date and time values in NetBackup commands varies according to the locale setting.

If you are uncertain of the NetBackup command requirements for your locale, enter the command with the `-help` option and check the usage. The following is part of the `bpbprestore` usage statement output that shows the `-s`, -e, and `-w` options:

```
[-s mm/dd/yyyy  [HH:MM:SS]] [-e mm/dd/yyyy  [HH:MM:SS]]
      [-w [hh:mm:ss]]
```

Note formats for the month, day, year and hours, minutes, seconds. These are for a locale setting of C, and may be different for other locales. For more information on locale, see the `locale(1)` man page for your system.

EXAMPLES

Example 1

To restore files from backups of `/usr/user1/file1` that were performed between 04/01/2003 06:00:00 and 04/10/2003 18:00:00, enter the following (all on one line):

```
bprestore -s 04/01/2003 06:00:00 -e 04/10/2003 18:00:00
/usr/user1/file1
```

Example 2

To restore files listed in a file named `restore_list` by using the most recent backups, enter the following:

```
bprestore -f restore_list
```

Example 3

To restore the directory `/home/kwc` from the backups that are associated with a keyword phrase that contains "My Home Directory" and use a progress log named `/home/kwc/bkup.log`, enter the following (all on one line):

```
bprestore -k "*My Home Directory*" -L /home/kwc/bkup.log  /home/kwc
```

Example 4

To restore the `D` drive on the Windows NT client slater from the backups that are associated with a keyword phrase that contains "My Home Dir" and use a progress log named `/home/kwc/bkup.log`, enter the following (all on one line, or using the backslash continuation character):

```
bprestore -k "*My Home Dir*" -C slater \
-D slater -t 13 -L /home/kwc/bkup.log  /D
```

Example 5

Assume you have a rename file named `/home/kwc/rename` on a UNIX client and it contains the following:

```
change /home/kwc/linkback to /home/kwc/linkback_alt
```

To restore the hard link named `/home/kwc/linkback` to alternate path `/home/kwc/linkback_alt` on that client, run the following command:

```
bprestore -H -R /home/kwc/rename /home/kwc/linkback
```

Example 6

Assume you want to restore files from backups of `/home/user1` that were performed between 04/01/01 06:00:00 and 04/10/01 18:00:00. You also want to exclude all files with a `.pdf` extension, except for the one named `final_doc.pdf`. To do this, run the following (all on one line, or using the backslash continuation character):

```
bprestore -s 04/01/01 06:00:00 -e 04/10/01 18:00:00 /home/user1 \
!/home/user1/*.pdf /home/user1/final_doc.pdf
```

FILES

`$HOME/bp.conf`

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

SEE ALSO

`bp(1),bparchive(1),bpbackup(1),bplist(1)`

bpSALinfo(1M)

NAME

bpSALinfo - verifies and adds world-wide name and lun values to device entries in the `/usr/openv/volmgr/database/3pc.conf` file on the media server.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpSALinfo [-h] [-p] [-v]
          [-d domain_name] [-o output_file] [-o -]
          [-U SAL_username] [-P SAL_password]
          [-S SPC_server | -S SPC_server:port]
```

DESCRIPTION

The `bpSALinfo` command uses the SAL server component of VERITAS SANPoint Control to verify and update world-wide port names (wwpn) and logical unit numbers (lun) in the NetBackup 3pc.conf file. For 3pc.conf device entries that have no wwpn or lun entries, `bpSALinfo` obtains those values from the SAL component of SANPoint Control and adds them to the 3pc.conf file.

After `bpSALinfo` has updated the 3pc.conf file, no further editing of the 3pc.conf file is needed. Use of the bpSALinfo command is required only for backups that use the Third-Party Copy Device backup method.

OPTIONS

`-h` Displays the bpSALinfo usage statement.

`-p` Prints a debug listing of all records accessed from SAL. The listing is sent to the screen, not to the `3pc.conf` file.

`-v` Specifies verbose mode, causing `bpSALinfo` to list information on its SAL lookup progress. The information is written to the screen, not to the `3pc.conf` file.

`-d` *`domain_name`*
Identifies the domain of the NetBackup clients. This is required only if `bpSALinfo` cannot resolve individual host names into fully qualified domain names.

`-o` *`output_file`*
Specifies an alternate (usually temporary) path for the `SAL` device information. The default is /usr/openv/volmgr/database/3pc.conf.

`-o -` Sends the `SAL` device information to the screen. Note the space before the second hyphen.

`-U` *`SAL_username`*
: The username for accessing the SAL component of SANPoint Control. The default is the default SANPoint Control username.

`-P` *`SAL_password`*
: The password for accessing the SAL component of SANPoint Control. The default is the default SANPoint Control password.

`-S` *`SPC_server`*
: The host name of the SANPoint Control server. The default is the local host.

  NOTE: the default port number for SAL is 2802. You can specify a different port number to connect to SAL by entering -S *SPC_server:port*. This port number must match the port as entered in SAL.conf file.

NOTES

- Before running `bpSALinfo`, you should run the `bptpcinfo` command with the -x option to discover any Fibre Channel or SCSI devices not visible to the media server. The -x option of `bptpcinfo` adds entries for those devices to the `3pc.conf` file on the media server.
- A `3pc.conf` file must exist at `/usr/openv/volmgr/database` on the NetBackup media server, otherwise `bpSALinfo` will fail.
- Use of the `bpSALinfo` command is required only for backups that use the Third-Party Copy Device backup method.

FILES

`/usr/openv/volmgr/database/3pc.conf`

bpschedule(1M)

NAME

`bpschedule` - Add, delete, or list disk staging storage unit (DSSU) schedules.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpplsched [-v] [-M
          master_server, ...] -add sched_label [-freq frequency]
          [-number_copies number] [-residence
          storage_unit_label[,stunit-copy2, ...stunit-copyn]] [-pool
          volume_pool_label[,pool-copy2, ...pool-copyn]] [-fail_on_error
          0|1[,0|1,...0|1][-window start_duration]] [-cal 0|1|2]
          [-ut] [-incl mm/dd/yyyy] [-excl mm/dd/yyyy] [-weekday
          day_name_week] [-dayomonth 1-31 or l]

/usr/openv/netbackup/bin/admincmd/bpplsched [-v] [-M
          master_server, ...] -delete sched_label

/usr/openv/netbackup/bin/admincmd/bpplsched [-v] [-M
          master_server, ...] -deleteall

/usr/openv/netbackup/bin/admincmd/bpplsched [-v] [-M
          master_server...] [-L | -l | -U]  [-label sched_label]
```

DESCRIPTION

The `bpschedule` command will do one of the following:

- Add a new disk staging storage unit (DSSU) schedule.
- Delete one or more DSSU schedules.
- Delete all the DSSU schedules.
- List one or all DSSU schedules.
- The default is to 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.

When the listing option is used there is 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, 2 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. This is also true for the `u_wind` entry in the `-L` display.

Line 2: SCHEDWIN, seven pairs of the form *start*,*duration*, expressing the start and duration of the window for each day of the week, starting 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 master servers listed. For instance, if `bpschedule` is adding a schedule, `bpschedule` adds the schedule to the policy on each of the master servers listed for `-M`. If the `-M` option is used on a listing request, the listing is the composite of the information returned by 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 `bpschedulerep`.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

These options are common to all forms of `bpschedule`:

`-help`

Prints a command line usage message when `-help` is the only option on the command line.

`-M` *master_server*, . . .

A list of alternative master servers. This 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 issuing 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, processing terminates at that point.

If `bpplsched` is producing a listing, the listing is the composite of the information returned by 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 verbose mode. This option causes `bpschedule` to log additional information for debugging purposes. The information goes into the NetBackup administration debug log. This option is meaningful only when NetBackup has debug logging enabled (`/usr/openv/netbackup/logs/admin` directory defined).

The remaining options depend on the form of `bpschedule`. The first form of `bpschedule` adds a schedule to the named policy. The following options apply to this form of `bpschedule`:

`-add` *sched_label* `[`*suboptions*`]`

Add a single schedule to the named policy.

The suboptions for the `-add` option explained below. These are attributes of the schedule being added. Refer to the *NetBackup System Administrator's Guide* for details on schedules and their attributes.

`-cal 0|1|2`

Indicates whether `bpschedule` is following 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 retires after run day

`-dayomonth 1-31 l`

Specifies the day 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 schedule the 15th day of every month, enter:

```
-dayomonth 15
```

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 backups initiated according to this schedule. Valid range for this option is 0 through 2419200 (number of seconds in four weeks). When 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 minimum value is 1. The maximum value is 4 or the Maximum Backup Copies global parameter, whichever is smaller. The default is 1.

`-pool` *volume_pool_label*`[,` *pool-copy2*`, . . .` *pool-copyn*`]`

This is the name of the volume pool. This choice overrides the policy-level volume pool. Entering "*NULL*" causes NetBackup to use the volume pool specified at the policy level. The default is to use the volume pool 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 specifying `-number_copies` greater than 1, specify a pool for each copy.

`-residence` *storage_unit_label*`[,` *stunit-copy2*`, . . .` *stunit-copyn*`]`

This is the name of the storage unit, which specifies the location of the backup images. The value "*NULL*" causes NetBackup to use the storage unit specified at the policy level. The default is for NetBackup to use the storage unit 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 specifying `-number_copies` greater than 1, specify a residence for each copy.

`-ut`

Any of the date/time arguments that follow `-ut` will be accepted as UNIX time, instead of the standard time format. The `-ut` option is used primarily for Java.

`-weekday` *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.

For example, to instruct the policy to run the second Monday of the month, enter:

```
-weekday Monday 2
```

`-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 is the number of seconds since midnight. This is an integer between 0 and 86399 (there are 86400 seconds in a day).

duration is the length of time that the window remains open. The time unit is seconds. This is a non-negative integer.

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*
: Delete the listed schedules from the named policy. The elements of the sched_label list must be separated by 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 `bpplsched`:

`-deleteall`
: Delete 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 is the default list type. This 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 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 listing, but it has fewer entries. Most attribute values are descriptive terms, rather than numbers.

EXAMPLES

In this example, `bpschedule` lists the information for schedule test in Long mode.

```
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:
  Day         Open       Close       W-Open     W-Close
 Sunday      000:00:00  000:00:00
 Monday      000:00:00  000:00:00
 Tuesday     000:00:00  000:00:00
 Wednesday   000:00:00  000:00:00
 Thursday    000:00:00  000:00:00
 Friday      000:00:00  000:00:00
 Saturday    000:00:00  000:00:00
```

FILES

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/sched/`*`schedule name`*

SEE ALSO

`bpschedulerep(1M)`

bpschedulerep(1M)

NAME

`bpschedulerep` - Modify the attributes of a disk staging storage unit (DSSU) schedule.

SYNOPSIS

`/usr/openv/netbackup/bin/admincmd/bpplschedrep` *sched_label* `[ -M` *master_server*`, . . .]` `[-v] [-freq` *backup_frequency*`] [-cal 0|1|2] [-incl` *mm/dd/yyyy*`] [-excl` *mm/dd/yyyy*`] [-delincl` *mm/dd/yyyy*`] [-delexcl` *mm/dd/yyyy*`] [-weekday` *day_name week*`] [-dayomonth 1-31 l] [-delweekday` *day_name week*`] [-deldayomonth 1-31 l] [-ci] [-ce] [-cw] [-cd] [-number_copies` *number*`] [-fail_on_error 0|1[,0|1,...,0|1]] [-residence` *storage_unit_label*`[,` *stunit-copy2*`, . . .` *stunit-copyn*`]] [-pool` *volume_pool_label*`[,` *pool-copy2*`, . . .` *pool-copyn*`]] [-(0..6) start duration]`

DESCRIPTION

`bpschedulerep` changes the attributes of a NetBackup disk staging storage unit (DSSU) schedule. The schedule named by `bpschedulerep` should already exist when this command is run. If the `-M` option is used, `bpschedulerep` changes the schedule on each of the master servers listed.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's 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 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 is a non-negative integer.

`-cal 0|1|2`

Indicates whether `bpschedulerep` is following 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 retires after run day

`-dayomonth 1-31 l`

Specifies the day 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 schedule the 15th day of every month, enter:

```
-dayomonth 15
```

To run the last day of every month, enter:

```
-dayomonth l
```

`-deldayomonth 1-31 l`

Specifies a day of every month to be excluded 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.

For example, to exclude the 20th day of every month from the schedule, enter:

```
-deldayomonth 20
```

`-delweekday` *day_name week*

Specifies a day of the week and the week of the month to be excluded as a run day from 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.

For example, to exclude the second Monday of the month, 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`

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, representing 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.

`-incl` *mm/dd/yyyy*
Indicates to include this single date.

`-M` *master_server*, . . .
A list of alternative master servers. This is a comma-separated list of hostnames. 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 issuing the `bpschedulerep` command. If an error occurs for any master server, processing terminates at that point.

The schedule attributes will be modified on all the master servers in this list.

`-number_copies` *number*
Specify the number of simultaneous backup copies. The minimum value is 1. The maximum value is 4 or the Maximum Backup Copies global parameter, whichever is smaller. The default is 1.

`-pool` *volume_pool_label*`[`, *pool-copy2*, . . . *pool-copyn*`]`
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 which contains this schedule.

Specify a pool for each copy.

To display the configured volume pools, run `/usr/openv/volmgr/bin/vmpool -listall`.

`-residence` *storage_unit_label*`[,` *stunit-copy2*`, . . .` *stunit-copyn*`]`

Specifies the label(s) of the storage unit to be used for storing the backups created according to this schedule. If "*NULL*" is specified, the residence for the schedule defaults to the residence of the policy which contains this schedule. If the residence value is a storage unit label, the residence for the schedule becomes that storage unit, overriding the residence for the policy.

Specify a storage unit for each copy.

Run `bpstulist` to display the set of defined storage units.

sched_label

The name of the schedule to be changed. This schedule has been previously created.

`-weekday` *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.

For example, to instruct the policy to run the second Monday of the month, enter:

```
-weekday Monday 2
```

`-v`

Selects 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 has debug logging enabled (`/usr/openv/netbackup/logs/admin` directory defined).

EXAMPLES

Changing and schedule named test.

```
bpschedulerep test -cal 2
```

The following output 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 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 1
SCHEDFOE 0 0 0 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 pm instead of 11 pm. Also, have the window duration be 2 hours instead of 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

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/sched/`*`schedule name`*

SEE ALSO

`bpschedule(1M)`

bpsetconfig(1M)

NAME

bpsetconfig - A program used to update a NetBackup configuration.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpsetconfig [-h host] [-u
        "user"] ["file" ...]

/usr/openv/netbackup/bin/admincmd/bpsetconfig -H
```

DESCRIPTION

The bpsetconfig command is used as a standalone program, or as a helper program with the backuptrace and restoretrace commands, to update a configuration. This command is available for all NetBackup server platforms.

You must have root privileges to execute this command.

OPTIONS

`-h "host"`
: Specifies the host name (*"host"*) of the server or client whose configuration will be updated.

`-u "user"`
: Specifies the user (*"user"*) whose configuration will be updated.

`"file"...`
: Specifies the file or files where the updates are listed. If not specified, standard input is read.

`-H`
: Displays the help screen.

EXAMPLE

The following example demonstrates how to set a NetBackup configuration on a different system.

```
bpsetconfig -h orange.colors.org

SERVER = yellow.colors.org

SERVER = orange.colors.org

<ctl-D>
```

The result of running the this command is to set the NetBackup configuration on the system `orange.colors.org` to the designated server that follows. This means that `yellow.colors.org` is the master server for the client `orange.colors.org`:

```
SERVER = yellow.colors.org
```

```
SERVER = orange.colors.org
```

bpstuadd(1M)

NAME

`bpstuadd` - Create a NetBackup storage unit group or a storage unit.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpstuadd -group group_name
        stunit_name, ...

/usr/openv/netbackup/bin/admincmd/bpstuadd -label
        storage_unit_label -path path_name | -dspath path_name |
        {-density density [-rt robot_type -rn robot_number]} [-host
        host_name] [-cj max_jobs] [-odo on_demand_only] [-mfs
        max_fragment_size] [-maxmpx mpx_factor] [-nh
        NDMP_attach_host] [-verbose] [-M master_server, ...]
```

DESCRIPTION

The `bpstuadd` command creates a NetBackup storage unit or storage unit group. When creating a single storage unit, ensure you include a label for the new storage unit and either the `-density`, the `-path`, or the `-dspath` option. The `bpstuadd` command will not create the storage unit if the master server has already created the maximum number of storage units allowed by its NetBackup configuration. The command will 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.

There are several types of storage units. The storage-unit type affects how NetBackup stores the data. The options on the `bpstuadd` command line determine the storage-unit type, which is one of the following:

- Disk. The storage destination is a disk file system directory.
- 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 medium (a tape or optical device) managed by the Media Manager.
- NDMP. An NDMP storage unit is controlled by Media Manager. The NetBackup for NDMP option must be installed. Where the Media Manager storage-unit type is discussed in this command description, the discussion also applies to the NDMP storage-unit type, unless it is specifically excepted. 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. When defining an NDMP storage unit, t `bpstuadd` command must be run on the master server. Refer to the NetBackup for NDMP System Administrator's Guide for more information on adding NDMP storage units.

Errors go to stderr. A log of the command's activity goes to the NetBackup admin log file for the current day. See the NetBackup system administrator's guide for additional information on storage units.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-cj` *max_jobs*

The maximum number of concurrent jobs permitted for this storage unit. *max_jobs* is a non-negative integer. The appropriate value depends on your server's ability to comfortably run multiple backup processes and the available space on the storage media. Also, refer to Maximum Jobs per Policy in the *NetBackup System Administrator's Guide*.

0 means that this storage unit will never be selected when a job is being scheduled. The default is 1.

`-density` *density*

If this option is present, the storage unit type is Media Manager. There is no default for this option. Either `-density`, `-path`, or `-dspath` must be on the command line. Do not use `-path` or `-dspath` when `-density` is being used. If the robot type is specified on the command line, the value for *density* should be consistent with the robot type.

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 are supported only on NetBackup Enterprise Servers.*

`hcart` - 1/2 Inch Cartridge

`hcart2` - 1/2 Inch Cartridge alternate

`dtf` - DTF Cartridge

`odiskwm` - Optical Disk Write-Many

`odiskwo` - Optical Disk Write-Once

`-dspath` *path_name*

The path to a disk staging file system, expressed as an absolute pathname. This is the data storage area for this disk staging storage unit. When this option is present, The DSSU is defined as a type 6 storage unit. There is no default for this option. Either `-dspath`, or `-density` must be on the command line. Do not use `-density` when `-dspath` is being used.

Disk Staging addresses the automatic (or scheduled sweeping) of images from the DSSU to the final staging unit (FSU). This can be done on a schedule basis, or may need to be done based on a DSSU's finite capacity.

`-group` *group_name stunit_name stunit_name*

Add a storage unit group, specifiying 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.

`-help`

Prints a command line usage message when `-help` is the only option on the command line.

`-host` *host_name*

Note *NetBackup Server does not support remote media servers.*

The NetBackup host that is associated with the destination media. The default is the hostname of the local system.

The host you select must be either your NetBackup master server or a remote media server (if you are configuring 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 it has not been configured in NetBackup previously, *host_name* will be added to NetBackup's configuration as a media server. On UNIX, this shows up as a `SERVER` entry in the `bp.conf` file; on Windows, this shows up on the Servers tab in the server properties dialog box in the NetBackup configuration window. If *host_name* is not a valid network name, you must configure it manually.

`-label` *storage_unit_label*

The name of the storage unit. This is a required option unless you are using `-group`. The maximum length of a storage-unit label is 128 characters.

`-mfs` *max_fragment_size*

The maximum fragment size specifies, in megabytes, how large a fragment for a NetBackup image can be. NetBackup supports a maximum fragment size of 1,000,000 megabytes (1 terabyte).

For a Media Manager storage unit, this value is either zero or any integer greater than or equal to 50 megabytes (MB) and less than or equal to 1,000,000 megabytes (MB). The default value is 0, meaning the maximum of 1,000,000 megabytes.

For a Disk storage unit, this value ranges from 20 megabytes to 2000 megabytes (2 gigabytes). The default value is 2000 (2 gigabytes).

`-maxmpx` *mpx_factor*

The maximum multiplexing factor. Multiplexing sends concurrent, multiple backups from one or several clients to a single drive. Refer to the topic "Multiplexing (MPX)" in the NetBackup system administrator's guide.

The multiplexing factor can range from 1 to 32. 1 means no multiplexing. A value greater than 1 means that NetBackup can create multiplexed images on the destination medium. Licensing determines the effective subset of the 1,_,32 range for the local NetBackup installation.
The default is 1.

`-M` *master_server*

A list of master servers. This 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 issuing the command. If an error occurs for any master server, processing stops at that point. The default is the master server for the system where the command is entered.

`-nh` *NDMP_attach_host*

Specifies the hostname of the NDMP server. If this option is present, the storage unit type is set to NDMP. The default is no NDMP server.

`-odo` *on_demand_only*

The On-Demand-Only flag controls the condition under which NetBackup uses the storage unit:

To make the storage unit available only to policies or 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.

DSSU's are on-demand-only. They have to be explicitly chosen as a back-up target.

`-path` *path_name*

The path to a disk filesystem, expressed as an absolute pathname. This is the data storage area for this storage unit. When this option is present, the storage unit type is Disk. There is no default for this option. Either `-path` or `-density` must be on the command line. Do not use `-density` when `-path` is being used.

In general when this option is used, it is recommended that the On-Demand-Only flag be enabled (see `-odo`). Otherwise, any NetBackup policy that does not require a specific storage unit has the opportunity to fill the disk filesystem *path_name*. This can cause serious system problems. For instance, if the system swap area happens to be on the same filesystem, new processes may fail.

`-rn` *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 Manager device configuration. The Media Manager system administrator's guide discusses the rules concerning the use of this number. This option is ignored unless the `-rt` option is present. There is no default for this option.

`-rt` *robot_type*

The robot type for this storage unit. For non-robotic (standalone) 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

`TSD` - Tape Stacker DLT

`ACS` - Automated Cartridge System

`TS8` - Tape Stacker 8MM

`TL8` - Tape Library 8MM

`TL4` - Tape Library 4MM

`ODL` - Optical Disk Library

`TSH` - Tape Stacker Half-inch

`TLH` - Tape Library Half-inch

`TLM` - Tape Library Multimedia

`LMF` - Library Management Facility

`RSM` - Removable Storage Manager

`-verbose`
: Select verbose mode for logging. This is only meaningful when running with debug logging turned on (that is, the directory `/usr/openv/netbackup/logs/admin` is defined).

EXAMPLES

Example 1

Create a new storage unit, named hatunit. Its storage unit type is Disk. The path for the storage unit is `/tmp/hatdisk`:

```
bpstuadd -label hatunit -path /tmp/hatdisk -verbose
  <2>bpstuadd: INITIATING: NetBackup 3.2Beta created: 98121513
  <2>bpstuadd: EXIT status = 0.
```

Example 2

Create a new disk-staging storage unit, named hatunit. Its storage unit type is Disk. The path for the storage unit is `/tmp/hatdisk`:

```
bpstuadd -label hatunit -dspath /tmp/hatdisk -verbose
  <2>bpstuadd: INITIATING: NetBackup 3.2Beta created: 98121513
  <2>bpstuadd: EXIT status = 0.
```

Example 3

Note The following example refers to remote media servers and applies only to NetBackup Enterprise Server. NetBackup Server supports only a master server, not remote media servers.

Create a storage unit using a UNIX server, which has not been configured previously in NetBackup:

```
% bpstuadd -label parrot_stu -host parrot -density dlt -rt TLD -rn 2
```

The 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_slave_on_clients` shell script on mango.

```
% grep parrot /usr/openv/netbackup/bp.conf
SERVER = parrot
SERVER = parrot
```

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 administrative logging is enabled, the exit status is logged in the administrative daily log under the directory `/usr/openv/netbackup/logs/admin` in the form:

`bpstuaddnew: EXIT status =` *exit status*

If an error occurred, a diagnostic precedes this message.

FILES

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/config/storage_units`

SEE ALSO

`bpstudel(1M),bpstulist(1M),bpsturep(1M)`

bpstudel(1M)

NAME

`bpstudel` - Delete a NetBackup storage unit or storage unit group.

SYNOPSIS

`/usr/openv/netbackup/bin/admincmd/bpstudel -label` *storage_unit_label* `[-verbose] [-M` *master_server*, . . . *master_server*`]`

`/usr/openv/netbackup/bin/admincmd/bpstudel -group` *group_name* `[-verbose] [-M` *master_server*, . . . *master_server*`]`

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 (if for instance, if the storage unit label is mistyped on the command line), 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. See your NetBackup system administrator's guide for additional information on storage units.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-label` *storage_unit_label*
: The name of the storage unit. This is a required option. The maximum length for a storage-unit label is 128 characters.

`-group` *group_name*
: The name of a storage unit group. If this option is present, the named storage unit group is deleted.

`-M` *master_server*
: A list of master servers. This 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 issuing

the command. If an error occurs for any master server, processing stops at that point. The default is the master server for the system where the command is entered.

`-verbose`

Select verbose mode for logging. This is only meaningful when running with debug logging turned on (that is, the directory `/usr/openv/netbackup/logs/admin` is defined).

EXAMPLES

Delete the storage unit named tst.dsk, listing the existing storage units before and after the deletion:

```
bpstulist
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*

bpstudel -label tst.dsk

bpstulist
stuunit 0 mango 0 -1 -1 1 0 /tmp/stuunit 1 1 2000 *NULL*
```

FILES

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/config/storage_units`

SEE ALSO

`bpstuadd(1M),bpstulist(1M),bpsturep(1M)`

bpstulist(1M)

NAME

`bpstulist` - Display one or all of the NetBackup storage units or storage unit groups.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpstulist [-label
        storage_unit_label] [-L|-l|-U] [-g] [-verbose] [-M
        master_server, . . . master_server]

/usr/openv/netbackup/bin/admincmd/bpstulist [-group group_name]
        [-verbose] [-M master_server, . . . master_server]
```

DESCRIPTION

The `bpstulist` command displays the attributes for a NetBackup storage unit or storage unit group. If no storage unit label or storage unit group name is specified, the command displays the attributes for all NetBackup storage units or storage unit groups.

Errors are sent to stderr. A log of the command's activity is sent to the NetBackup admin log file for the current day. See your NetBackup system administrator's guide for additional information on storage units.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

List-type options:

`-L`

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 and raw form. For instance, a robot-type entry might be `TL4 (7)` (7 is NetBackup's internal value for a TL4 robot).

For a disk storage unit, a long listing has these attributes for each storage unit:

- Label
- Media Type (this is the storage-unit type)
- Host Connection
- Concurrent Jobs
- On Demand Only

- Path
- Robot Type (not robotic)
- Max Fragment Size
- Max MPX

For a Media Manager storage unit, a long listing has these attributes for each storage unit:

- Label
- Media Type (this is the storage-unit type, for example Disk Staging (6))
- Host Connection
- Concurrent Jobs
- On Demand Only
- Path
- Robot Type
- Max Fragment Size
- Max MPX/drive

`-l`

The list type is short. This produces a terse listing. This option is useful for scripts or programs that rework the listing contents into a customized report format. This 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
- robot_type
- robot_number
- density
- concurrent_jobs
- initial_mpx
- path
- on_demand_only
- max_mpx
- maxfrag_size
- ndmp_attach_host

`-U`

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 instance, a robot-type value might be `TL4`, instead of `7`.

For a disk storage unit, a user-type listing has these attributes for each storage unit:

- Label
- Media Type (this is the storage-unit type)
- Host Connection
- Concurrent Jobs
- On Demand Only
- Max MPX
- Path
- Max Fragment Size

For a Media Manager storage unit, a user-type listing has these attributes for each storage unit:

- Label
- Media Type (this is the storage-unit type)
- Host Connection
- Number of Drives
- On Demand Only
- Max MPX/drive
- Density
- Robot Type/Number
- Max Fragment Size

`-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*.

Here are the remaining options for `bpstulist`:

`-label` *storage_unit_label*

The name of the storage unit. 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` *group_name*
: A list that includes all defined storage units and storage unit groups. The list type for the list of storage units is short. This produces a terse listing. The list of storage unit groups is in the format *group_name*: *group_members*.

`-M` *master_server*, . . . *master_server*
: A list of master servers. This 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 issuing the command. If an error occurs for any master server, processing 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 is only meaningful when running with debug logging turned on (that is, the directory `/admin/usr/openv/netbackup/logs/admin` is defined).

EXAMPLES

Example 1

List the storage units defined on the master server apricot, 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
Path:               /usr/redtest
Max Fragment Size:  2000 MB

Label:              bluetest
Storage Unit Type:  Media Manager
Host Connection:    apricot
Number of Drives:   6
On Demand Only:     yes
Max MPX/drive:      1
Density:            4mm - 4mm Cartridge
Robot Type/Number:  TL4 / 0
Max Fragment Size:  1048576 MB
```

Example 2

The following output is realized using the following two `bpstuadd` commands to create a DSSU and a regular disk storage unit:

```
bpstuadd -label bean -dspath /tmp/bean  - creates a DSSU
bpstuadd -label apple -path /tmp/apple  - creates a regular Disk STU
```

Short output:

```
apple 0 felix.min.veritas.com 0 -1 -1 1 0 "/tmp/apple" 1 1 2000 *NULL*
bean 6 felix.min.veritas.com 0 -1 -1 1 0 "/tmp/bean" 1 1 2000 *NULL*
```

Long output:

```
Label:              apple
Media Type:         Disk (0)
Host Connection:    felix.min.veritas.com
Concurrent Jobs:    1
On Demand Only:     yes
Path:               "/tmp/apple"
Robot Type:         (not robotic)
Max Fragment Size:  2000
Max MPX:            1

Label:              bean
Media Type:         Disk Staging (6)
Host Connection:    felix.min.veritas.com
Concurrent Jobs:    1
On Demand Only:     yes
Path:               "/tmp/bean"
Robot Type:         (not robotic)
Max Fragment Size:  2000
Max MPX:            1
```

FILES

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/config/storage_units`

SEE ALSO

`bpstuadd(1M),bpstudel(1M),bpsturep(1M)`

bpsturep(1M)

NAME

`bpsturep` - Replace selected NetBackup storage unit attributes.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpsturep -label
          storage_unit_label [-host host_name] [-cj max_jobs] [-odo
          on_demand_only] [-mfs max_fragment_size] [-maxmpx
          mpx_factor] [{-path path_name} | {-density density_type
          [-rt robot_type -rn robot_number]}] [-nh NDMP_attach_host]
          [-verbose] [-M master_server, . . .]

/usr/openv/netbackup/bin/admincmd/bpstrep -group
          storage_unit_group [-addstu | -delstu] <storage_unit>
```

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 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 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` once for each attribute to be replaced.

`bpsturep` makes the changes by deleting the old storage unit and adding a new storage unit with the specified attribute changes. Therefore, if `bpsturep` specifies invalid options or an invalid combination of options, the storage unit may be deleted without being re-added. It is best to run `bpstulist` after `bpsturep` to determine whether the intended changes were actually applied.

Errors go to stderr. A log of the command's activity goes to the NetBackup administrative log file for the current day. See your NetBackup system administrator's guide for additional information on storage units.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-cj` *max_jobs*

The maximum number of concurrent jobs permitted for this storage unit. max_jobs is a non-negative integer. The appropriate value depends on your server's ability to comfortably run multiple backup processes and the available space on the storage media. Also, refer to the Maximum Jobs per Policy topic in your NetBackup system administrator's guide.

0 means that this storage unit will never be selected when a job is being scheduled. The default is 1.

`-density` *density_type*

If this option is present, the storage unit type is Media Manager. There is no default for this option. One of `-density` or `-path` must be on the command line, but not both. If the command line includes a robot type, the value for density should be consistent with the robot type.

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

`odiskwm` - Optical Disk Write-Many

`odiskwo` - Optical Disk Write-Once

`-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 hostname of the local system.

The host you select must be either your NetBackup master server or a media server (if you are configuring 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 in NetBackup, the value *host_name* will be added to NetBackup's configuration as a media server. On UNIX, this shows up in `bp.conf`; on Windows, this shows up in the Configuration window for Servers. If *host_name* is not a valid network name, you must configure it manually.

`-label` *storage_unit_label*

The name of a storage unit. This is the storage unit whose attributes `bpsturep` replaces. This is a required option. The maximum length of a storage-unit label is 128 characters.

`-mfs` *max_fragment_size*

The maximum fragment size specifies, in megabytes, how large a fragment for a NetBackup image can be. NetBackup supports a maximum fragment size of 1,000,000 megabytes (1 terabyte).

For a Media Manager storage unit, this value is either zero or any integer greater than or equal to 50 megabytes (MB) and less than or equal to 1,000,000 megabytes (MB). The default value is 0, meaning the maximum of 1,000,000 megabytes.

For a Disk storage unit, this value ranges from 20 megabytes to 2000 megabytes (2 gigabytes). The default value is 2000 (2 gigabytes).

`-maxmpx` *mpx_factor*

The maximum multiplexing factor. Multiplexing sends concurrent, multiple backups from one or several clients to a single drive. Refer to the topic "Multiplexing (MPX)" in your NetBackup system administrator's guide.

The multiplexing factor can range from 1 to 32, where 1 means no multiplexing. A value greater than 1 means that NetBackup can create multiplexed images on the destination medium. Depending on the licensing of the local NetBackup installation, it may not be possible to assign multiplexing factors in the entire range 1..32.

The default is 1.

`-M` *master_server_*

A list of master servers. This 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 issuing the command. If an error occurs for any master server, processing 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 hostname of the NDMP server. If this option is present, the storage unit type is set to NDMP. The default is no NDMP server.

`-odo` *on_demand_only*

The *on-demand-only* flag controls whether the storage unit is used only for backups that explicitly request (demand) the storage unit:

To make the storage unit available only to policies or 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.

`-path` *path_name*

The path to a disk filesystem, expressed as an absolute pathname. This is the data storage area for this storage unit. When this option is present, the storage unit type is `Disk`. There is no default for this option. One of `-density` or `-path` must be on the command line, but not both.

In general when this option is used, it is recommended that the *on-demand-only* flag be enabled (see `-odo`). Otherwise, any NetBackup policy that does not require a specific storage unit has the opportunity to fill the disk filesystem *path_name*. This can cause serious system problems. For instance, if the system swap area happens to be on the same filesystem, new processes may fail.

If the path name is defined as a disk staging storage unit (DSSU), then this option can be used to change the path name a different DSSU. It cannot be used to change a DSSU to a different type of storage unit.

`-rn` *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 Manager device configuration. The Media Manager system administrator's guide discusses the rules concerning the use of this number. This option is ignored unless the `-rt` option is present. There is no default for this option.

`-rt` *robot_type*

The robot type for this storage unit. For non-robotic (standalone) 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

`TSD` - Tape Stacker DLT

`ACS` - Automated Cartridge System

`TS8` - Tape Stacker 8MM

`TL8` - Tape Library 8MM

`ODL` - Optical Disk Library

`TSH` - Tape Stacker Half-inch

`TLH` - Tape Library Half-inch

`TLM` - Tape Library Multimedia

`LMF` - Library Management Facility

`RSM` - Removable Storage Manager

`-verbose`

Select `verbose` mode for logging. This is only meaningful when running with debug logging turned on (that is, the directory `/usr/openv/netbackup/logs/admin` is defined).

`-group` *storage_unit_group*

The name of a storage unit group. This 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.

EXAMPLES

Change the path for a disk storage unit, mkbunit. The path is changed from `/tmp/mkbunit` to `/tmp/mkbunit2`:

```
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*
```

FILES

/usr/openv/netbackup/logs/admin/*

/usr/openv/netbackup/db/config/storage_units

SEE ALSO

bpstuadd(1M),bpstudel(1M),bpstulist(1M)

bpsynth(1M)

NAME

bpsynth - Used to create a synthetic backup.

SYNOPSIS

```
/usr/openv/netbackup/bin/bpsynth -pl policy_name -sched
         schedule [-C client] [-S storage_unit] [-k "key_word"]
         [-sn stream number] [-jobid jobid]
```

DESCRIPTION

The `bpsynth` command will cause a new synthetic full or synthetic cumulative incremental backup to be created. The new backup image will be built using previously made full and incremental images from the same policy and client. This command must be executed on the master server.

OPTIONS

`-pl` *`policy_name`*

Specifies the policy for which the backup will be created. Required option. This policy must have True Image Restore with Move Detection selected. The most recent incremental backup for the client must have been created with True Image Restore with Move Detection.

The policy must be standard or a Windows NT policy type.

`-sched` *`schedule`*

The schedule name used to create the new backup. This schedule type must be a full or cumulative increments, and have the synthetic backup attribute set. This is a required option.

`-jobid` *`jobid`*

The command specifies the *jobid* number to be used when bpsynth updates the Activity Monitor.

`-C` *`client`*

The client for which the synthetic backup will be made. If omitted, the current hostname will be used.

`-S` *`storage_unit`*

Specifies the storage unit which will be used for the backup image. The default is the default for the schedule or policy.

`-sn` *`stream number`*

If the backup policy specifies multiple streams, each stream must be independently synthesized. The variable *stream number* is 1 through the number of streams.

`-k "`*`key_word`*`"`

If specified, a keyword for the new image.

bptpcinfo(1M)

NAME

bptpcinfo - discovers SAN devices and creates a `3pc.conf` file.

SYNOPSIS

```
/usr/openv/netbackup/bin/bptpcinfo [-a] [-c] [-h] [-u] [-r]
          [-v] [-d disk_device_directory] [-t tape_device_directory] [-p
          physical_device] [-x client_name] [-o output_file_name] [-o -]
```

DESCRIPTION

The `bptpcinfo` command discovers all disk and tape devices on fibre channel and SCSI connections, and 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 offhost 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. The 3pc.conf file created by bptpcinfo is complete and you do not need to rerun this command if any of the following is true:

- The backup is using the NetBackup Media Server backup method.
- You are using 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, you should run the bptpcinfo command manually to create the 3pc.conf file, and then edit the file as explained in the SAN Configuration chapter of the NetBackup Advanced Client System Administrator's Guide.

OPTIONS

`-a`

Discovers all disk and tape devices on the Fibre Channel and SCSI connections, and adds entries in the `3pc.conf` file (or alternate output file specified with the `-o` option). The `-a` option lists all devices in `/dev/rdsk` and `/dev/rmt`.

`-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 "cannot open file." In that case, use other options on this command to create the file. Note that if -c is specified, any other options are ignored.

The -c option checks for syntax errors such as missing spaces between entries, missing keywords (such as a world-wide name without its "w="), or a world-wide 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 disk and tape devices on the Fibre Channel and SCSI connections, and adds entries in the 3pc.conf file (or alternate output file specified with the -o option) for any new devices that are found. If the 3pc.conf file does not exist, the -u option will fail (use -a instead).

Note: -u does not remove obsolete entries. To remove obsolete entries, use -r. (The -u and -r options cannot be used together.)

`-r`

Removes any obsolete entries in the 3pc.conf file (or alternate output file 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 verbose mode, causing 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 HP, and `/dev` on AIX) and creates new entries in the `3pc.conf` file (or alternate output file 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/rdsk on Solaris or HP, and /dev on AIX) and creates new entries in the `3pc.conf` file (or alternate output file 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*

If the specified device is discoverd, creates an entry for that device in the `3pc.conf` file (or alternate output file 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.

`-x` *client_name*

Discovers Fibre Channel and SCSI devices visible to this client but not visible to the media server, and adds entries for those devices to the 3pc.conf file on the media server. If -x is specified, any other options are ignored.

Note that you must edit the new entries in the 3pc.conf file by adding the world-wide name (wwn=) of each device. For assistance, refer to the SAN Configuration chapter of the NetBackup Advanced Client System Administrator's Guide.

`-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 output to the screen. Note the space before the second hyphen.

EXAMPLES

Example 1

Discover all source and destination devices on the SAN and create the required `3pc.conf` file in `/usr/openv/volmgr/database`.

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

Example 2

Discover all source and destination devices on the SAN, and send the output to the screen.

```
/usr/openv/netbackup/bin/bptpcinfo -a -o -
```

Sample output:

```
devid [p=devpath]     [s=sn]  [n=npid]        [l=lun] [w=wwpn] [i=iddesc]
 0     p=/dev/rdsk/c1t4d1s2    s=SEAGATE:ST39175LW:3AL02EV300001936JL7R
l=1i=1031000005013E000D3313933364A4C3752
 1     p=/dev/rdsk/c1t11d2s2   s=IBM:DDYS-T18350N:VEY06933
l=2i=1035005076706C01B15
 2     p=/dev/rdsk/c1t11d3s2   s=SEAGATE:ST19171N:LAE82305                    l=3
 3     p=/dev/rdsk/c1t13d4s2   s=SEAGATE:ST19101W:NH022724                    l=4
 4     p=/dev/rdsk/c1t18d0s2   s=SEAGATE:ST336605FC:3FP001Z000008122HWSD
l=0i=103200000203742595A
 5     p=/dev/rdsk/c1t19d0s2   s=SEAGATE:ST336605FC:3FP003KC00008122HWD1
l=0i=10320000020374259B5
 6     p=/dev/rdsk/c1t20d0s2   s=HITACHI:OPEN-9:60159003900                   l=0
 7     p=/dev/rdsk/c1t20d1s2   s=HITACHI:OPEN-9:60159000000                   l=1
 8     p=/dev/rdsk/c1t20d2s2   s=HITACHI:OPEN-9:60159000100                   l=2
 9     p=/dev/rdsk/c1t20d3s2   s=HITACHI:OPEN-9-CM:60159001C00                l=3
 10    p=/dev/rdsk/c1t20d4s2   s=HITACHI:OPEN-9:60159002B00                   l=4
 11    p=/dev/rdsk/c1t20d5s2   s=HITACHI:OPEN-9:60159002C00                   l=5
 12    p=/dev/rmt/0cbn s=QUANTUM:DLT8000:CX949P0164                    l=1
i=10200E09E6000000868
 13    p=/dev/rmt/1cbn s=QUANTUM:DLT8000:CX949P1208                    l=2
i=10200E09E6000001381
```

Example 3

Discover the devices in the `/dev/rmt` directory (`/dev` on AIX) and send the output to the screen:

On Solaris or HP:

```
/usr/openv/netbackup/bin/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=10200E09E6000000868
 1     p=/dev/rmt/1cbn s=QUANTUM:DLT8000:CX949P1208                    l=2
i=10200E09E6000001381
 2     p=/dev/rmt/4cbn s=QUANTUM:DLT8000:CX940P2790                    l=2
i=1031000005013E000D33934305032373930
 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:

```
  /usr/openv/netbackup/bin/bptpcinfo -t /dev -o -
Sample output:
        devid [p=devpath]     [s=sn]  [n=npid]        [l=lun] [w=wwpn] [i=iddesc]
        0 p=/dev/rmt0.1 s=STK:L20:LLC02203684                    l=1
```

```
 1 p=/dev/rmt5.1 s=QUANTUM:DLT8000:CXA49P1113             l=1 i=10200E09E6000034A57
 2 p=/dev/rmt6.1 s=QUANTUM:DLT8000:PXB13P4180             l=2 i=10200E09E600004B70B
 3 p=/dev/rmt7.1 s=STK:9840:331002059900                  l=4 i=103500104F0004817E5
 4 p=/dev/rmt9.1 s=QUANTUM:DLT8000:PXB33P0850             l=9
i=1036005013000B05269423333503038353 0
 5 p=/dev/rmt10.1 s=QUANTUM:DLT8000:CX949P1208             l=10
i=1036005013000B05269393439503132303 8
```

Example 4

Create a `3pc.conf` file that describes all devices on the SAN, and send the output to an alternate file:

```
/usr/openv/netbackup/bin/bptpcinfo -a -o /usr/openv/volmgr/database/3pc_alt1.conf
```

NOTES

- The `bptpcinfo` command should be run when no backups are in progress. If a device is being used (or is reserved) by a backup, the `bptpcinfo` command may not be able to obtain information on the device, thus omitting the device from the output.
- If you do not want to overwrite the existing `3pc.conf` file, include the -o option and specify the desired location.
- If you have a host running VERITAS SANPoint Control, you can use the `bpSALinfo` command to add world-wide 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 by manually adding the world-wide name (wwpn=) and luns of each device. For assistance, refer to the SAN Configuration chapter of the *NetBackup Advanced Client System Administrator's Guide*.

FILES

`/usr/openv/volmgr/database/3pc.conf`

bpverify(1M)

NAME

`bpverify` - Verify the backups created by NetBackup.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpverify [-l] [-p] [-pb] [-v]
          [-local] [-client name] [-st sched_type] [-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 | path]
```

DESCRIPTION

`bpverify` verifies the contents of one or more backups by reading the backup volume and 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, thus verifying that the volume is readable. NetBackup verifies only one backup at a time and tries to minimize media mounts and positioning time.

If either `-Bidfile` or `-backupid` is specified, `bpverify` uses this option as the sole criterion for selecting the set of backups it will verify. If the command line does not contain `-Bidfile` or `-backupid`, then `bpverify` selects the backups that satisfy all the selection options. For instance, if the command line looks like

```
bpverify -pt Standard -hoursago 10
```

then `bpverify` verifies the set of backups with policy type `Standard` that have been run in the past 10 hours.

If `-p` or `-pb` is specified, `bpverify` previews the set of backups that meet the selection criteria. In this case, `bpverify` displays the backup IDs, but does not perform the verification.

`bpverify` sends its error messages to `stderr`. `bpverify` sends a log of its activity to the NetBackup admin log file for the current day (found in `/usr/openv/netbackup/logs/admin)`.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-Bidfile` *file_name*

file_name specifies a file that contains a list of backup IDs to be verified. 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, meaning any backup can be verified.

`-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.

`-policy` *name*

Search for backups to verify in the specified policy. The default is any policy.

`-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 indicated by the `bpconfig -max_copies` setting, up to 10. The default is 1.

`-primary` indicates that the primary copy should be verified rather than the copy.

`-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:

```
AFS
DataStore
DataTools-SQL-BackTrack
DB2
FlashBackup
Informix-On-BAR
Lotus-Notes
MS-Exchange-Server
MS-SQL-Server
MS-Windows-NT
NCR-Teradata
NDMP
```

NetWare

Oracle

OS/2

SAP

Split-Mirror

Standard

Sybase

`-e` *date*

Specifies the end of the time range for selecting backups to verify. The `-s` option or the `-hoursago` option specifies the start of the range.

The format of *date* depends on the user's locale setting. See the NOTES section for more information. For the C locale, the date syntax is as follows:

mm/*dd*/*yyyy* [*hh*[: *mm*[: *ss*]]]

The default ending time is the current date and time.

`-help`

Prints a command line usage message when `-help` is the only option on the command line.

`-hoursago` *hours*

Specifies the number of hours before the current time to search for backups. This is equivalent to specifying a start time (`-s`) of the current time minus hours. Do not use both this option and the `-s` option.

Hours 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 are on this media ID or pathname. If a backup has some fragments on this media ID and some fragments on another media ID, NetBackup skips verifying that backup. For images stored on disk rather than removable media, specify an absolute pathname instead of *media_id*. The default is any media ID or pathname.

`-L` *output_file* `[-en]`

Specifies the name of a file in which to write progress information. The default is to not use a progress file, in which case the progress information is written to `stderr`. For additional information, see DISPLAY FORMATS later in this command description.

Include the `-en` option to generate a log in English. The name of the log will contain the string `_en`. This option is useful to support personnel assisting in a distributed environment where differing locales may create logs of various languages.

`-l`

Specifies that the list type is long, causing `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`

When `bpverify` is initiated from a host other than master server and the `-local` option is *not* used (default), `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 the `-local` option to prevent the creation of a remote copy on the master server and to run the `bpverify` only from the host where it was 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 issuing 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 is similar to the `-p` option, but `-pb` does not display information about the individual backups. For additional information, see DISPLAY FORMATS later in this command description.

`-s` *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 format of *date* depends on the user's locale setting. See the NOTES section for more information. For the C locale, the date syntax is as follows:

mm/*dd*/*yyyy* [*hh*[: *mm*[: *ss*]]]
The default is 24 hours ago.

`-sl` *sched_label*

Search for backups to verify that were created by the specified schedule. The default is all schedules.

`-st` *sched_type*

Search for backups to verify that were created by the specified schedule type. 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 verbose mode. When `-v` is specified, the debug and progress logs include more information. The default is not verbose.

DISPLAY FORMATS

PREVIEW DISPLAYS:

`bpverify` runs a preview by searching for backups and displaying them. `bpverify` does not actually verify the backups.

- The `-p` display lists backup IDs that meet the criteria set by the bpverify command-line options. The `-p` display is ordered by volume. For each volume containing a selected backup, the media ID and server are displayed, followed by the selected backup Ids that reside on that volume
- The `-pb` display is a brief version of the `-p` display. It lists the media ID and server for each volume that contains backups that meet the selection criteria.

VERIFICATION DISPLAYS:

`bpverify` creates these displays as it verifies images. If the `bpverify` command line 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 containing the progress log.

The verification display is ordered by volume.

- 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 backed up

  Any problems that `bpverify` detects while verifying the image

  Whether the image verification is successful or not

- In short format, `bpverify` omits listing the files backed up.

NOTES

The format that you must use for date and time option values varies according to the locale setting. The examples in this command description are for a locale setting of C.

For more information on locale, see the `locale(1)` man page for your system.

EXAMPLES

Example 1

The following example verifies the backups run in the past 36 hours:

```
  bpverify -hoursago 36
  Verify started Thu Feb  3 11:30:29 2003
  INF - Verifying policy mkb_policy, schedule Full
(plum_0949536546), path /tmp/mkbunit, created 02/02/01 18:09:06.
INF - Verify of policy mkb_policy, schedule Full
(plum_0949536546) was successful.
INF - Status = successfully verified 1 of 1 images.
```

Example 2

The following example compares the two preview displays, `-p` and `-pb`:

```
bpverify -p -hoursago 2002
Media id = A00002  Server = plum
Bid = plum_0949616279  Kbytes = 32800  Filenum = 1  Fragment = 1
Bid = guava_0949681647  Kbytes = 12191  Filenum = 2  Fragment = 1
Bid = guava_0949683298  Kbytes = 161  Filenum = 3  Fragment = 1
Bid = guava_0949683671  Kbytes = 11417  Filenum = 4  Fragment = 1
Bid = guava_0949684009  Kbytes = 11611  Filenum = 5  Fragment = 1
Bid = guava_0949684276  Kbytes = 806  Filenum = 6  Fragment = 1
```

```
Bid = guava_0949688704  Kbytes = 9869  Filenum = 7  Fragment = 1
Bid = guava_0949688813  Kbytes = 9869  Filenum = 8  Fragment = 1
Bid = guava_0949949336  Kbytes = 10256  Filenum = 9  Fragment = 1
Bid = plum_0949949337  Kbytes = 6080  Filenum = 9  Fragment = 1
Bid = plum_0949949337  Kbytes = 4176  Filenum = 10  Fragment = 2
Bid = guava_0949949686  Kbytes = 10256  Filenum = 11  Fragment = 1
Bid = plum_0949949687  Kbytes = 5440  Filenum = 11  Fragment = 1
Bid = plum_0949949687  Kbytes = 4816  Filenum = 12  Fragment = 2
Bid = guava_0949949902  Kbytes = 10256  Filenum = 13  Fragment = 1
Bid = plum_0949949901  Kbytes = 8832  Filenum = 13  Fragment = 1
Bid = plum_0949949901  Kbytes = 1424  Filenum = 14  Fragment = 2
Bid = plum_0950053561  Kbytes = 10256  Filenum = 15  Fragment = 1

Media id = 400032  Server = plum
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 = plum
Media id = 400032  Server = plum
```

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 administrative logging is enabled, the exit status is logged in the administrative daily log under the directory `/usr/openv/netbackup/logs/admin` in the form:

`bpverify: EXIT status =` *exit status*

If an error occurred, a diagnostic precedes this message.

FILES

`/usr/openv/netbackup/logs/admin/*`

`/usr/openv/netbackup/db/error/*`

`/usr/openv/netbackup/db/images/*`

SEE ALSO

NetBackup System Administrator's Guide

cat_convert(1M)

NAME

`cat_convert` - NetBackup catalog format conversion utility.

SYNOPSIS

```
/usr/openv/netbackup/bin/cat_convert [ -o [ -a2b | -b2a ] -s
        -v] source_file_directory [target_file_directory]
```

DESCRIPTION

`cat_convert` converts NetBackup catalog `.f` files between version 3.4, 4.0v or 4.5 ASCII format and 4.5 binary format. `cat_convert` automatically detects the source catalog file format and converts it to the other format.

You must have root privileges to execute this command.

OPTIONS

`-o`	Overwrite original catalog file content with the new, converting format. `-o` cannot be used with *target_file_directory*.
`-a2b`	Convert NetBackup 3.4, 4.0V, 4.5 ASCII format catalog `.f` file(s) to NetBackup 4.5 binary format `.f` file(s). Do not use `-a2b` with `-b2a`.
`-b2a`	Convert the NetBackup 4.5 binary format catalog `.f` file(s) to NetBackup 4.5 ASCII format `.f` file(s). Do not use `-b2a` with `-a2b`.
`-s`	Show statistic information to the console window.
`-v`	Show current progress information.

Specify either a single source file or an entire directory to convert:

- In order to specify a target file, the source must be a file.
- In order to specify a target directory, the source must be a directory.

  If the source is a directory, you must use `-a2b` or `-b2a`.

  The new files created by the conversion are converted to the specified format and the original file names are used in the target directory.

If the target file or directory is not specified when converting source files, the new files created by the conversion process will have a suffix appended (`_bin.f` or `_ascii.f`).

If the `catalog .f` file size is more than 4 megabytes, the binary catalog leaves output files separate and puts them in the `catstore` directory.

EXAMPLES

Example 1

Consider the following command:

```
cat_convert abc.f
```

If *abc.f* is in ASCII format, the *target_file_path* will be `abc_bin.f`.

If *abc.f* is in binary format, the *target_file_path* will be `abc_ascii.f`.

Example 2

Consider the following command:

```
cat_convert abc.f  /usr/tmp/abc1.f
```

`abc.f` will be converted to the other format and copied to `/usr/tmp/abc1.f`.

Example 3

Consider the following command:

```
cat_convert -a2b /home/john/catalog
```

Every ASCII `.f` file in `/home/john/catalog` will be converted to the NetBackup 4.5 binary format with new file name `*_bin.f`.

Example 4

Consider the following command:

```
cat_convert -b2a /home/john/catalog /home/john/catalog_ascii
```

Every NetBackup 4.5 binary `.f` file in `/home/john/catalog` will be converted to NetBackup 4.5 ASCII format and copied to `/home/john/catalog_ascii`.

Example 5

Consider the following command:

```
cat_convert -o abc.f
```

The content of `abc.f` will be converted to the other file format.

Example 6

Consider the following command:

```
cat_convert -o -b2a /home/john/catalog
```

The content of every NetBackup 4.5 binary `.f` file under `/home/john/catalog` will be converted to NetBackup 4.5 ASCII format.

duplicatetrace(1M)

NAME

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]
         [-install_path path] mmddyy [mmddyy …]

duplicatetrace [-master_server name] -backup_id id [-start_time
         hh:mm:ss] [-end_time hh:mm:ss] [-install_path path]
         mmddyy [mmddyy …]

duplicatetrace [-master_server name] [-policy_name name]
         [-client_name name] [-start_time hh:mm:ss] [-end_time
         hh:mm:ss] [-install_path path] mmddyy [mmddyy …]
```

DESCRIPTION

duplicatetrace consolidates the debug logs for the specified duplicate job[s] and writes them to standard output. The messages will be sorted by time. *duplicatetrace* will attempt to compensate for time zone changes and clock drift between remote servers and clients.

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

If either -job_id or -backup_id is specified, *duplicatetrace* uses this option as the sole criteria for selecting the duplicate job[s] it will trace. The options –policy_name or –client_name cannot be used in conjunction with –job_id or –backup_id. If –job_id or –backup_id are not specified then all duplicate jobs that match the specified selection criteria will be selected. If none of the options namely, -job_id, -backup_id, -policy_name or -client_name is specified, then all the duplicate jobs executed on the days specified by day stamps (*mmddyy*) will be traced. If –start_time/-end_time options are used then the debug logs in the specified time interval are examined.

If duplicatetrace is started with the –backup_id <bid>option then duplicatetrace will look for duplicate jobs started via bpduplicate with –backup_id <bid> option where the backup ids (<bid>) match.

If duplicatetrace is started with the –policy_name <policy> option then duplicatetrace will look for duplicate jobs started via bpduplicate with –policy <policy> option where the policy names (<policy>) match.

If duplicatetrace is started with the –client_name <client> option then duplicatetrace will look for duplicate jobs started via bpduplicate with –client <client> option where the client names (<client>) match.

duplicatetrace writes error messages to standard error.

You must have root privileges to execute 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 duplicated by the duplicate job to analyze. 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`
: Earliest time stamp to start analyzing the logs. Default is 00:00:00.

`-end_time`
: Latest time stamp to finish analyzing the logs. Default is 23:59:59.

`-install_path`
: The NetBackup install path on the Windows NT/2000 server. Default is c:\Program Files\VERITAS.

  Note that the install path must be enclosed in quotes if the path includes a space.

`mmddyy`
: One or more “day stamps”. This identifies the log file names (log.mmddyy for UNIX, mmddyy.log for Windows NT/2000) that will be analyzed.

OUTPUT FORMAT

The format of an output line is:

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

`daystamp`
: The day of the log in yyyymmdd format.

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

`program`
: The name of program (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 actually appears in the debug log file.

EXAMPLES

Example 1

The following example analyzes the log of duplicate job with job ID 3 executed on August 6, 2002.

```
duplicatetrace -job_id 3 080602
```

Example 2

The following example analyzes the log of duplicate jobs that duplicate backup image with backup ID pride_1028666945 executed on August 20, 2002. This command would analyze only those duplicate jobs, which were executed with option -backupid pride_1028666945.

```
duplicatetrace -backup_id pride_1028666945 082002
```

Example 3

The following example analyzes the log of duplicate jobs executed on policy *Pride-Standard* and client *pride* on August 16, 2002 and August 23, 2002. This command would analyze only those duplicate jobs, which were executed with options -policy *Pride-Standard* and -client *pride*.

```
duplicatetrace -policy_name Pride-Standard -client_name pride
         081602 082302
```

Example 4

The following example analyzes the log of all duplicate jobs that are executed on August 5, 2002 and August 23, 2002.

```
duplicatetrace 080502 081702
```

importtrace(1M)

NAME

`importtrace` – Trace debug logs for import job(s).

SYNOPSIS

```
importtrace [-master_server name] -job_id number [-start_time
         hh:mm:ss] [-end_time hh:mm:ss] [-install_path path]
         mmddyy [mmddyy]

importtrace [-master_server name] -backup_id id [-start_time
         hh:mm:ss] [-end_time hh:mm:ss] [-install_path path]
         mmddyy [mmddyy]

importtrace [-master_server name] [-policy_name name]
         [-client_name name] [-start_time hh:mm:ss] [-end_time
         hh:mm:ss] [-install_path path] mmddyy [mmddyy]
```

DESCRIPTION

importtrace consolidates the debug log messages for the specified import job[s] and writes them to standard output. The messages will be sorted by time. *importtrace* will attempt to compensate for time zone changes and clock drift between remote servers and clients.

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

If either -job_id or -backup_id is specified, *importtrace* uses this option as the sole criteria for selecting the import job[s] to trace. The options –policy_name or –client_name cannot be used in conjunction with –job_id or –backup_id. If –job_id or –backup_id are not specified then all import jobs that match the specified selection criteria will be selected. If none of the options namely, -job_id, -backup_id, -policy_name or -client_name is specified, then all the import jobs executed on the days specified by day stamps (*mmddyy*) will be traced. If –start_time/-end_time options are used then the debug logs in the specified time interval are examined.

If importtrace is started with the –backup_id <bid>option then importtrace will look for import jobs started via bpimport with –backup_id <bid> option where the backup ids (<bid>) match.

If importtrace is started with the –policy_name <policy> option then importtrace will look for import jobs started via bpimport with –policy <policy> option where the policy names (<policy>) match.

If importtrace is started with the –client_name <client> option then importtrace will look for import jobs started via bpimport with –client <client> option where the client names (<client>) match.

importtrace writes error messages to standard error.

You must have root privileges to execute 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 imported by the import job 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 time stamp to start analyzing the logs. Default is 00:00:00.

`-end_time`
: Latest time stamp to finish analyzing the logs. Default is 23:59:59.

`-install_path`
: The NetBackup install path on the Windows NT/2000 server. Default is c:\Program Files\VERITAS.

  Note that the install path must be enclosed in quotes if the path includes a space.

`mmddyy`
: One or more day stamps. This identifies the log file names (log.mmddyy for UNIX, mmddyy.log for Windows NT/2000) that will be analyzed.

OUTPUT FORMAT

The format of an output line is:

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

`daystamp`
: The day of the log in yyyymmdd format.

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

`program`
: The name of program (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 actually appears in the debug log file.

EXAMPLES

Example 1

The following example analyzes the log of import job with job ID 4 executed on August 6, 2002.

```
importtrace -job_id 4 080602
```

Example 2

The following example analyzes the log of import jobs that import backup image with backup id *pride_1028666945* executed on August 20, 2002. This command would analyze only those import jobs, which were executed with option -backupid *pride_1028666945*.

```
importtrace -backup_id pride_1028666945 082002
```

Example 3

The following example analyzes the log of import jobs executed on policy *Pride-Standard* and client *pride* on August 16, 2002 and August 23, 2002. This command would analyze only those import jobs, which were executed with options -policy *Pride-Standard* and -client *pride*.

```
importtrace -policy_name Pride-Standard -client_name pride 081602
082302
```

Example 4

The following example analyzes the log of all import jobs that are executed on August 5, 2002 and August 17, 2002.

```
importtrace 080502 081702
```

jbpSA(1)

NAME

`jbpSA` - Starts the Backup, Archive, and Restore client interface on Java-capable UNIX machines.

SYNOPSIS

```
/usr/openv/java/jbpSA [ -d | -display] [-D prop_filename] [-h |
          -help] [-l debug_filename] [-ms nnn] [-mx xxx]
```

DESCRIPTION

The `jbpSA` command starts the Backup, Archive, and Restore client interface 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 `jbpSA` command.

`-l` *debug_filename*
: Indicate the debug log file name. The default name is unique to this startup of `jbpSA` and written in `/usr/openv/java/logs`.

`-lc`
: This option prints the cmdlines used by the application to its log file.

  Note: The application does not always use the cmdlines 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, fewer cmdlines will be used.

`-ms` *nnn*
: The `-ms` option allows memory usage configuration for the Java Virtual Machine (JVM) where *nnn* is the megabytes of memory available to the application. Default: 36M (megabytes)

  The recommendation is to run `jnbSA` on a machine 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. It is unlikely that this value will require changing as the default is sufficient for quickest initialization of `jnbSA` on a machine with the recommended amount of memory.

Example:

```
jbpSA -ms 36M
```

The memory allocated can be specified 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) where ***xxx*** specifies the maximum heap size (in megabytes) the JVM uses for dynamically allocated objects and arrays. Default: 512M (megabytes).

This 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 using the `jbpSA` command or by setting the `MAX_MEMORY` option in `/usr/openv/java/nbj.conf`.

jnbSA(1M)

NAME

`jnbSA` - Starts the NetBackup Administration Console on Java-capable UNIX machines.

SYNOPSIS

`/usr/openv/netbackup/bin/jnbSA [ -d | -display] [-D` *prop_filename*`] [-h | -help] [-l` *debug_filename*`] [-lc] [-ms` *nnn*`] [-mx` *xxx*`]`

DESCRIPTION

`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*

Indicate the debug log file name. The default name is unique to this startup of `jnbSA` and written in `/usr/openv/java/logs`.

`-lc`

This option prints the cmdlines used by the application to its log file.

Note: The application does not always use the cmdlines 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, fewer cmdlines will be used.

`-ms` *nnn*

The `-ms` option allows memory usage configuration for the Java Virtual Machine (JVM) where *nnn* is the megabytes of memory available to the application. Default: 36M (megabytes)

The recommendation is to run `jnbSA` on a machine 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. It is unlikely that this value will require changing as the default is sufficient for quickest initialization of `jnbSA` on a machine with the recommended amount of memory.

Example:

```
jbpSA -ms 36M
```

The memory allocated can be specified using the `jnbSA` 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) where ***xxx*** specifies the maximum heap size (in megabytes) the JVM uses for dynamically allocated objects and arrays. Default: 512M (megabytes).

This 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 using the `jnbSA` command or by setting the `MAX_MEMORY` option in `/usr/openv/java/nbj.conf`.

lmfd(1M)

NAME

lmfd, lmfcd - Library Management Facility (LMF) daemon and control daemon.

SYNOPSIS

```
/usr/openv/volmgr/bin/lmfd [-v]
/usr/openv/volmgr/bin/lmfcd [-v] [-t]
```

DESCRIPTION

`lmfd` and `lmfcd` interface with Media Manager to mount and unmount tape volumes in an LMF robot.

Note `lmfd` and `lmfcd` only run on Solaris platforms.

`lmfd` directly interfaces with `ltid` (the Media Manager device daemon). `lmfd` runs on each host with a drive connection and sends mount and unmount requests to the control daemon, `lmfcd`.

`lmfcd` communicates with the Fujitsu LMF Server, which processes all requests and control functions for the robotic library. `lmfcd` can be running on a different host than `lmfd`, depending on where the Fujitsu library control is configured (see EXAMPLES). When communication with the library is established, `lmfd` puts the LMF robot in the UP state and can request volume mounts and unmounts. If the library or control daemon is inaccessible, `lmfd` changes the robot to the DOWN state. In this state, `lmfd` is still running and returns the robot to the UP state if `lmfcd` is able to make a connection.

Note If drives are on different hosts, the robotic information must be entered in the Media Manager device configuration on all hosts and the robot number must be the same on all hosts.

`lmfd` and `lmfcd` are automatically started when `ltid` is started and stopped when `ltid` is stopped. You can stop and start `lmfd` independently of `ltid` using `/usr/openv/volmgr/bin/vmps` or your server's `ps` command to identify the `lmfd` process id and then entering the following commands:

`kill` *lmfd_pid*

```
/usr/openv/volmgr/bin/lmfd [-v] &
```

`lmfcd` is on the host that has the robotic control and is automatically started by `lmfd` on that host. `lmfcd` is terminated when you stop `ltid`. The media ID for any volumes to be used in the library must be defined in the volume database before any volumes can be accessed using `ltid`, `lmfd`, and `lmfcd`. Both the initial volume database population and future updates can be accomplished using the Media Manager robotic inventory options.

Drives are numbered 1 through *n*, based on information obtained from the Fujitsu library. To map Fujitsu library drive names to the appropriate Media Manager robot drive numbers, you can use the robotic test utility, `lmftest` (or `robtest` if the robot is configured). You can also use this utility along with the Fujitsu `lmdisplay` command-line interface to verify library communications, status, and functionality.

Drive cleaning for LMF robotic drives must be configured through a Fujitsu administrative interface, since these operations are not made available to applications that are using the Fujitsu library. For this reason, cleaning volumes cannot be defined using Media Manager. In addition, you cannot use the `tpclean(1M)` command for cleaning operations on drives under LMF robotic control.

The Internet service port number for `lmfcd` must be in `/etc/services`. If you are using NIS (Network Information Service), the entry found in this host's `/etc/services` file should be placed in the master NIS server database for services. To override the services file, create the file `/usr/openv/volmgr/database/ports/lmfcd` with a single line containing the service port number for `lmfcd`. The default service port number is 13718.

You must have root privileges to execute this command.

OPTIONS

`-v`

Logs debug information using `syslogd`. If you start `ltid` with `-v`, `lmfd` and `lmfcd` are also started with `-v`.

`-t`

Terminates `lmfcd`.

NOTES

This command applies only to NetBackup Enterprise Server.

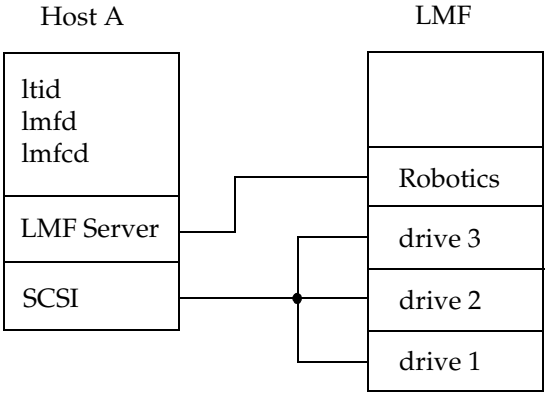
ERRORS

`lmfd` and `lmfcd` log an error message if there is a copy of the daemon running.

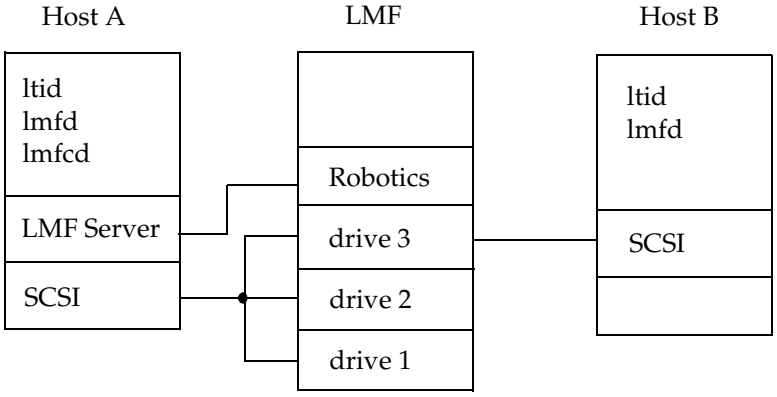
Media Manager logs any LMF robotic errors to `syslogd`. Log entries are also made when the state changes between UP and DOWN.

EXAMPLES

In the following diagram, the drives are attached to and the robotics are controlled from a single host. `ltid` initiates `lmfd`, which initiates `lmfcd`. The Fujitsu LMF Server daemon must be running on Host A.



In the following diagram, drives are attached to Host A and Host B. The robotics are controlled from Host A. `ltid` on each machine initiates `lmfd`. The `lmfd` on Host A also initiates `lmfcd`, since that is where the robotic control is defined. Requests to mount tapes from Host B go to `lmfd` on Host B, which sends the robotic command to `lmfcd` on Host A.



SEE ALSO

`ltid(1M), syslog(8), tpclean(1M), tpconfig(1M), vmadm(1M)`

ltid(1M)

NAME

ltid, stopltid - start and stop the Media Manager device daemon.

SYNOPSIS

```
/usr/openv/volmgr/bin/ltid [-v] [-nsu] [-logmounts [minutes]]
          [-noverify]

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

DESCRIPTION

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`, is also started by 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 root privileges to execute this command.

OPTIONS

`-v`

Logs debug information using `syslogd`. This is most informative when robotic devices are in use. This option starts robotic daemons and `vmd` in verbose mode.

`-nsu`

If this option is specified, tapes in standalone drives are not ejected when `tpunmount` is issued (though they are ejected if end of media is reached during a NetBackup backup or archive). You can override this option by specifying the `-force` option on `tpunmount`.

This option can be used in a NetBackup environment where it is desirable to keep the standalone drives ready after successful backups are performed.

Specifying this option is equivalent to specifying `DO_NOT_EJECT_STANDALONE` in the `vm.conf` file.

`-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, `ltid` does not verify drive names. Normally, `ltid` verifies that the no rewind on close drive name has the correct minor number bits relating to no rewind, variable, berkeley-style, and so on. This option is normally not required, but may be helpful if using non-standard platform device files. If this option is specified, caution should be taken in making sure the device files are correct.

ERRORS

`stopltid` does not stop the daemons if any drives are assigned to users. Ensure that all users have unmounted assigned tapes before attempting to stop the daemons.

Error messages are logged using `syslogd`.

SEE ALSO

`rc(8), syslogd(8), tpconfig(1M), vmadm(1M), tpunmount(1)`

nbdbsetport(1M)

NAME

`nbdbsetport` - Set TCP/IP port used by the nbdbd database service

SYNOPSIS

```
/usr/openv/bin/admincmd/ nbdbsetport -get
/usr/openv/bin/admincmd/ nbdbsetport -set port_number
```

DESCRIPTION

When the nbdbd database service is initially installed, the port number for the nbdbd database service is set to 13784. The default port is adequate in most cases.

If this port number is already being used by another service on your machine, the nbdbd database service will not run until the port is changed using `nbdbsetport -set` *port_number*.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-get`
: Returns the TCP/IP port numbercurrent being used by the nbdbd service.

`-set` *port_number*
: Set the nbdbd service TCP/IP port number to *port_number*. The new port number will take effect the next time NetBackup is restarted.

nbdbsetpw(1M)

NAME

`nbdbsetpw` - Modify passwords used by the nbdbd database service

SYNOPSIS

```
/usr/openv/bin/admincmd\ nbdbsetpw [-reset]
```

DESCRIPTION

When the nbdbd database service is initially installed, it has two passwords: one for the `root` user and one for `nbu` user. If you wish, you can use `nbdbsetpw` to modify these passwords.

When invoked, `nbdbsetpw` prompts for new passwords for the `root` user and `nbu` user.

NetBackup stores encrypted nbdbd passwords if private data files. NetBackup must know the passwords in order to change them. If for some reason these encrypted passwords are not in sync with the passwords in the nbdbd database authorization tables, you must reset the passwords to the default by running `nbdbsetpw -reset`. Resetting the passwords should not be necessary during normal operations. The `nbdbsetpw` command will inform you if reset is necessary.

If the reset fails, you should contact VERITAS Technical Support.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-reset`

Sets passwords to default. `nbdbsetpw` logs the fact that the nbdbd passwords have been changed.

ndmpmoveragent(1M)

NAME

ndmpmoveragent.start - starts the NDMP mover agent daemon (`ndmpmoveragent`) on the NetBackup media server (UNIX).

ndmpmoveragent.stop - stops the NDMP mover agent daemon (`ndmpmoveragent`) on the NetBackup media server (UNIX).

SYNOPSIS

```
/usr/openv/volmgr/bin/ndmpmoveragent.start [-h | -buffers N |
        -install | -noinstall] [-noprint]
```

```
/usr/openv/volmgr/bin/ndmpmoveragent.stop [-h | -remove |
        -noremove] [-noprint]
```

DESCRIPTION

The `ndmpmoveragent` daemon is a separate process that acts as an NDMP server in a type of three-way backup called Remote NDMP. This daemon only runs with NDMP version V2, but can back up NDMP hosts that are running with NDMP version V2, V3, and V4. This daemon must be launched by means of the `ndmpmoveragent.start` script, and stopped by the `ndmpmoveragent.stop` script. These scripts automatically install an initialization script that restarts/stops the daemon when the system is rebooted.

The `ndmpmoveragent` command is for UNIX systems only. See `InstallNdmpMoverAgent` for the Windows equivalent.

OPTIONS

`-h`

Print these instructions.

`-buffers` *N*

Create the specified number of 63k buffers to be used during remote NDMP backup or restore. N can be 4 to 64 (default is 64).

For optimal peformance when using networks and tape drives that exceed 10 MB/sec, such as Gigabit Ethernet (GbE) or Fibre Channel and LTO drives, it is advised that you use the default setting of 64 buffers and change your shared memory settings to 4 MB.

16 buffers require 1 MB of shared memory. Therefore, 64 buffers require 4MB of shared memory. You can increase max shared memory by changing the shmsys values in the /etc/system file. For example, to allow for a maximum of 4 MB, add the following line to /etc/system:

```
set shmsys:shminfo_shmmax=4194304
```

Then reboot.

Note If the -buffers option is set to a value greater than that allowed by max shared memory, the number of buffers is adjusted to the number allowed by max shared memory when the backup is run.

`-install`
: Install the initialization script.

`-noinstall`
: Do not install the initialization script.

`-noprint`
: Do not print status messages.

`-remove`
: Remove initialization script.

`-noremove`
: Do not remove initialization script.

NOTES

For `ndmpmoveragent.start`: if neither `-install` nor `-noinstall` is specified (and the initialization script is not already installed), the user will be prompted to install the initialization script.

If you answer yes when prompted, a sample initialization script located in `/usr/openv/volmgr/bin/goodies/ndmpmover` is installed in `/etc/init.d/ndmpmover`, with links from `/etc/rc0.d/K78ndmpmover` and `/etc/rc2.d/S76ndmpmover`.

For `ndmpmoveragent.stop`: if neither `-remove` nor `-noremove` is specified (and the initialization script is installed), the user will be prompted to remove the script. Removing the script will prevent the `ndmpmoveragent` daemon from being restarted when the system is rebooted.

odld(1M)

NAME

odld - Optical Disk Library (ODL) daemon

SYNOPSIS

```
/usr/openv/volmgr/bin/odld [-v]
```

DESCRIPTION

`odld` interfaces with Media Manager to mount and unmount optical platters in an Optical Disk Library. It is initiated by `ltid` (the Media Manager device daemon), if drives have been defined to be in an Optical Disk Library.

`odld` performs its tasks by communicating directly with the robotics using a SCSI interface. When the connection is established (that is, the path for robotics can be opened), `odld` puts the robot in the UP state and can mount and unmount platters. If the robotics are inaccessible, `odld` changes the robot to the DOWN state. In this state, `odld` is still running and it returns the robot to the UP state when it is able to make a connection.

You can stop or start `odld` independently of `ltid` using `/usr/openv/volmgr/bin/vmps` or the `ps` command to identify the `odld` process id and then entering the following commands:

`kill` *odld_pid*

```
/usr/openv/volmgr/bin/odld [-v] &
```

The Media Manager administrator must enter the media ID and slot number information for the platters in the Optical Disk Library into the volume database before users can access any platters using `ltid` and `odld`. Note that each optical platter contains two volumes (external media IDs), one per side. This information can be entered using `vmadm`.

The Internet service port number for `odld` must be in `/etc/services`. If you are using NIS (Network Information Service), you should place the entry in this host's `/etc/services` file in the master NIS server database for services. To override the services file, create the file `/usr/openv/volmgr/database/ports/odld` with a single line containing the service port number for `odld`. The default service port number is 13706.

You must have root privileges to execute this command.

OPTIONS

`-v`

Logs debug information using `syslogd`. If you start `ltid` with `-v`, `odld` also starts with `-v`.

NOTES

This command applies only to NetBackup Enterprise Server.

ERRORS

`odld` returns an error message if there is a copy of `odld` running.

Any ODL and robotic errors are logged using `syslogd`. Log entries are also made when the state changes between UP and DOWN.

SEE ALSO

`ltid(1M), syslogd(8), tpconfig(1M), tpformat(1M), vmadm(1M)`

restoretrace(1M)

NAME

`restoretrace` – consolidate debug logs for a restore job

SYNOPSIS

```
<install_path>\NetBackup\bin\admincmd\restoretrace
          [-master_server name] [-job_id number] [-client_name
          name] [-start_time hh:mm:ss] [-end_time hh:mm:ss]
          mmddyy [mmddyy ...]
```

DESCRIPTION

The restoretrace utility can be used to consolidate the debug logs for the specified restore job[s]. It will copy to standard output the debug log lines relevant to the specified restore job[s]. The messages will be sorted by time. The utility will attempt to compensate for time zone changes and clock drift between remote servers and clients. The output is formatted so that it should be relatively easy to sort or grep by time stamp, program name, and/or server/client name.

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

You must have root privileges to execute 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 time stamp to start analyzing the logs.

`-end_time hh:mm:ss`
: Latest time stamp to finish analyzing the logs.

`mmddyy [mmddyy]`
: One or more day stamps. This identifies the log file names (log.mmddyy for UNIX, mmddyy.log for Windows NT/2000) that will be analyzed.

NOTES

Media Manager logs are not analyzed.

Windows 95/98 and Mac OS 8/9 client logs may not be analyzed.

EXAMPLES

```
/usr/openv/netbackup/bin/admincmd/restoretrace -job_id 234 081302
log.234
```

set_ndmp_attr (1M)

NAME

set_ndmp_attr - authorizes access and sets configuration values for NDMP attached robots.

On Windows server systems: *install_path*`\Volmgr\bin\set_ndmp_attr`

On UNIX systems: `/usr/openv/volmgr/bin/set_ndmp_attr`

SYNOPSIS

The `set_ndmp_attr` command can take any of the following sets of parameters as a single line. Two or more sets can be combined into one line (see Example 4).

`set_ndmp_attr [-insert | -update | -delete | -display] -auth` [*ndmp-server-host*] [*user-name*] [*password*]

`set_ndmp_attr [-insert | -update | -delete | -display] -robot` [*ndmp-server-host*] [*robot-device*] [*scsi-controller scsi-id scsi-lun*]

`set_ndmp_attr -verify` [*ndmp-server-host*]

`set_ndmp_attr -probe` [*ndmp-server-host*] (not available for NDMP V2)

`set_ndmp_attr [-list | -l]`

`set_ndmp_attr [-list_compact | -lc]`

DESCRIPTION

Authorizes access and sets configuration values for robots attached to an NDMP host, and places them into the NDMP configuration database.

OPTIONS

`-insert` (optional)
: Allows user to insert a new authorize access entry or a new robot (must be used with `-auth` or `-robot`).

`-update` (optional)
: Updates an NDMP entry (must be used with `-auth` or `-robot`).

`-delete` (optional)
: Deletes an NDMP entry (must be used with `-auth` or `-robot`).

`-display` (optional)
: Displays an NDMP entry (must be used with `-auth` or `-robot`).

`-auth`
: Creates an entry to allow access to an NDMP client.

`-robot`
Sets the configuration values for an NDMP-attached robot.

`-verify`
Verifies that the NetBackup for NDMP server has access to the NDMP host. If a robot is configured on the NDMP host, this option verifies access to the robot.

`-probe`
Lists all devices attached to the NDMP host.

`-list or -l` (optional)
Lists the current entries in the NDMP configuration database.

`-list_compact or -lc` (optional)
Lists a short version of the NDMP configuration database.

Note If none of the following (`-insert`, `-update`, `-delete`, or `-display`) precedes the options `-robot` or `-auth`, the default is to either insert or update, depending on whether the host or robot already exists.

EXAMPLES

Example 1: Setting the authorization of an NDMP client

```
set_ndmp_attr -insert -auth stripes root
Passwd:XXXXX
Passwd:XXXXX
```

Example 2: Setting the configuration values for a robot attached to an NDMP client. The robot is on control 2, SCSI-ID 3, and LUN 0.

```
set_ndmp_attr -insert -robot stripes c2t3l0 2 3 0
```

Example 3: Running a verify

```
set_ndmp_attr -verify
Verify Host name: stripe
```

Result of Example 3:

```
Verify Host name: stripes
Connecting to host "stripes" as user "root"...
Waiting for connect notification message...
Opening session with NDMP protocol version 2...
Host info is:
  host name "stripes"
  os type "SunOS"
```

```
  os version "5.8"
  host id "80dd14ba"
  host supports TEXT authentication
  host supports MD5 authentication
Getting MD5 challenge from host...
Logging in using MD5 method...
Login was successful
Opening SCSI device "c2t3l0"...
Setting SCSI target controller 2 id 3 lun 0...
Inquiry result is "HP      C5173-7000      3.04"
```

Example of failed verification due to incorrect password:

```
Connecting to host "stripes" as user "root"...
Waiting for connect notification message...
Opening session with NDMP protocol version 2...
Host info is:
  host name "stripes"
  os type "SunOS"
  os version "5.8"
  host id "80dd14ba"
  host supports TEXT authentication
Logging in using TEXT method...
ndmp_connect_client_auth failed
set_ndmp_attr: host "stripes" failed
set_ndmp_attr: unable to continue
```

Example 4: This shows several sets of parameters combined

```
set_ndmp_attr -auth stripes root -robot stripes c2t3l0 2 3 0 -verify stripes
```

tl4d(1M)

NAME

tl4d - Tape Library 4MM (TL4) daemon

SYNOPSIS

```
/usr/openv/volmgr/bin/tl4d [-v]
```

DESCRIPTION

`tl4d` interfaces with Media Manager to mount and unmount tapes in a Tape Library 4MM (TL4) robot. It is started by `ltid` (the Media Manager device daemon), if the Media Manager device configuration shows drives in the robot.

Stopping `ltid` stops `tl4d`. You can stop or start `tl4d` independently of `ltid` using `/usr/openv/volmgr/bin/vmps` or your server's `ps` command to identify the `tl4d` process ID and entering the following commands:

`kill` *tl4d_pid*

`/usr/openv/volmgr/bin/tl4d [-v] &`

`tl4d` communicates with the robotics through a SCSI interface. When the connection is established (the path for robotics can be opened), tl4d puts the TL4 robot in the UP state and can mount and unmount tapes. If the robotics are inaccessible, `tl4d` changes the robot to the DOWN state. In this state, `tl4d` is still running and returns the robot to the UP state if it is able to make a connection.

The media ID and slot number information for 4 mm tapes in a robot must be defined in the Media Manager volume database before any tapes can be accessed through `ltid` and `tl4d`.

If a cleaning volume is used, it must be defined in the volume configuration. See `tpclean(1M)` for information on setting the frequency for automatic drive cleaning.

The Internet service port number for `tl4d` must be in `/etc/services`. If you are using NIS (Network Information Service), you should place the entry in this host's `/etc/services` file in the master NIS server database for services. To override the services file, create the file `/usr/openv/volmgr/database/ports/tl4d` with a single line containing the service port number for `tl4d`. The default service port number is 13713.

You must have root privileges to execute this command.

OPTIONS

`-v`

Logs debug information using `syslogd`. If you start `ltid` with `-v`, `tl4d` also starts with `-v`.

ERRORS

`tl4d` returns an error message if there is a copy of `tl4d` running.

Media Manager logs any Tape Library 4MM and robotic errors to `syslogd`. Log entries are also made when the state changes between UP and DOWN.

SEE ALSO

`ltid(1M), syslogd(8), tpclean(1M), tpconfig(1M), vmadm(1M)`

tl8d(1M)

NAME

tl8d, tl8cd - Tape Library 8MM (TL8) daemon and control daemon

SYNOPSIS

```
/usr/openv/volmgr/bin/tl8d [-v]
```

```
/usr/openv/volmgr/bin/tl8cd [-v] [-t] [-n]
```

DESCRIPTION

`tl8d` and `tl8cd` interface with Media Manager to mount and unmount volumes in a Tape Library 8MM robot.

`tl8d` directly interfaces with the Media Manager device daemon (`ltid`). A `tl8d` daemon runs on each host with a drive connection and sends mount and unmount requests to the control daemon `(tl8cd)`. `tl8cd` communicates with the robotics through a SCSI interface.

The following paragraph applies only to NetBackup Enterprise Server:

Tape Library 8MM robotic control software permits drives in the same robot to be configured on different hosts. `tl8cd` may be running on a different host than `tl8d`, depending on where the SCSI connection resides (see EXAMPLES). When the connection is established (that is, the path for robotics can be opened), `tl8d` puts the TL8 robot in the UP state and can mount and unmount volumes. If the robotics are inaccessible, `tl8d` changes the robot to the DOWN state. In this state, `tl8d` is still running and returns the robot to the UP state if `tl8cd` is able to make a connection.

The following paragraph applies only to NetBackup Enterprise Server:

If drives are on different NetBackup hosts, the robotic information must be entered in the Media Manager configuration on all machines and the robot number must be the same on all machines.

`tl8d` and `tl8cd` are automatically started when `ltid` is started and stopped when `ltid` is stopped. You can stop or start `tl8d` independently of `ltid` using `/usr/openv/volmgr/bin/vmps` or your server's `ps` command to identify the `tl8d` process id and then entering the following commands:

`kill` *tl8d_pid*

```
/usr/openv/volmgr/bin/tl8d [-v] &
```

The control daemon, `tl8cd`, is on the host that has the robotic control and is started by `tl8d` on that host (see EXAMPLES).

The media ID and slot number information for volumes in a robot must be defined in the volume database before any volumes can be accessed through `ltid`, `tl8d`, and `tl8cd`.

If a cleaning volume is used, it must be defined in the volume configuration. See `tpclean(1M)` for information on setting the frequency for automatic drive cleaning.

If the `vm.conf` configuration option `PREVENT_MEDIA_REMOVAL` is enabled when `tl8cd` is active, `tl8cd` disables access to the volumes and media access port by issuing a command to the TL8 robot. If it is necessary to open the door of the cabinet, you must terminate `tl8cd` first. By default, access to the library is allowed.

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 drive indexing.
- The robotic test utility, or experiment by mounting media and watching the operator display.

The Internet service port number for `tl8cd` must be in `/etc/services`. If you are using NIS (Network Information Service), the entry found in this host's `/etc/services` file should be placed in the master NIS server database for services. To override the services file, create the file `/usr/openv/volmgr/database/ports/tl8cd` file with a single line containing the service port number for `tl8cd`. The default service port number is 13705.

You must have root privileges to execute this command.

OPTIONS

`-v`

Logs debug information using `syslogd`. If you start `ltid` with `-v`, `tl8d` and `tl8cd` are also started with `-v`.

`-t`

Terminates `tl8cd`.

`-n`

Causes `tl8cd` to run with barcode checking disabled. This option is useful, if all or most of the volumes in the library do not contain barcodes, because it takes the robot a lot less time to scan volumes.

Note that if the volumes contain barcodes and the `-n` option is selected, the barcodes are ignored.

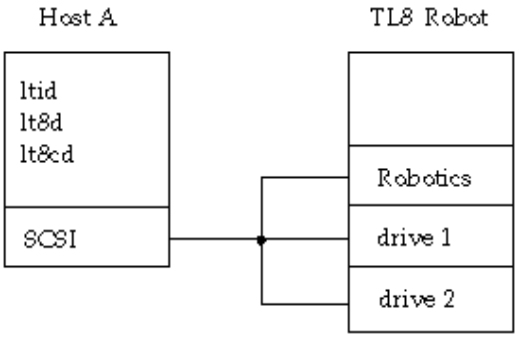
ERRORS

`tl8d` and `tl8cd` log error messages if there is a copy of the daemon running.

Media Manager logs any Tape Library 8MM and robotic errors to `syslogd`. Log entries are also made when the state changes between UP and DOWN.

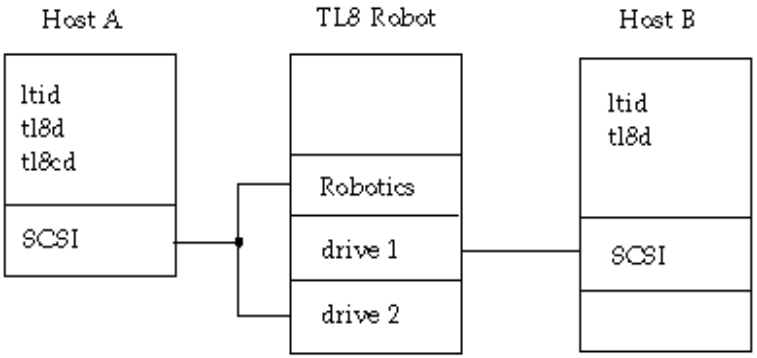
EXAMPLES

In the following diagram, the drives and the robotics are connected to a single host. `ltid` initiates `tl8d`, which in turn initiates `tl8cd`.



The following example applies only to NetBackup Enterprise Server:

In the following diagram, each host is connected to one drive in the robot and the robotics are connected to host A. `ltid` on each host initiates `tl8d`. The `tl8d` on host A also initiates `tl8cd`, since that is where the robotic control is defined. Requests to mount tapes from host B go to `tl8d` on host B, which sends the robotic command to `tl8cd` on host A.



SEE ALSO

`ltid(1M), syslogd(8), tpclean(1M), tpconfig(1M), vmadm(1M)`

tldd(1M)

NAME

tldd, tldcd - Tape Library DLT (TLD) daemon and control daemon

SYNOPSIS

```
/usr/openv/volmgr/bin/tldd [-v]
/usr/openv/volmgr/bin/tldcd [-v] [-t]
```

DESCRIPTION

`tldd` and `tldcd` interface with Media Manager to mount and unmount volumes in a Tape Library DLT (TLD) robot.

`tldd` directly interfaces with `ltid` (the Media Manager device daemon). `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 paragraph applies 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 (that is, the path for robotics can be opened), `tldd` puts the TLD robot in the UP state and 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.

The following paragraph applies only to NetBackup Enterprise Server:

If drives are on different NetBackup hosts, the robotic information must be entered in the Media Manager device configuration on all machines and the robot number must be the same on all machines.

`tldd` and `tldcd` are started when `ltid` is started and stopped when `ltid` is stopped. You can stop or start `tldd` independently of `ltid` using `/usr/openv/volmgr/bin/vmps` or your server's `ps` command to identify the `tldd` process ID and then entering the following commands:

`kill` *tldd_pid*

`/usr/openv/volmgr/bin/tldd [-v] &`

`tldcd` is on the host that has the robotic control and is automatically started by `tldd` on that host (see EXAMPLES).

The media ID and slot number information for volumes in the robot must be defined in the volume database before any volumes can be accessed through `ltid`, `tldd`, and `tldcd`.

If a cleaning volume is used, it must be defined in the volume configuration. See `tpclean(1M)` for information on setting the frequency for automatic drive cleaning.

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 drive indexing.
- The robotic test utility, or experiment by mounting media and watching the operator display.

The Internet service port number for `tldcd` must be in `/etc/services`. If you are using NIS (Network Information Service), the entry found in this host's `/etc/services` file should be placed in the master NIS server database for services. To override the services file, create the `/usr/openv/volmgr/database/ports/tldcd` file with a single line containing the service port number for `tldcd`. The default service port number is 13711.

You must have root privileges to execute this command.

OPTIONS

`-v`

Logs debug information using `syslogd`. If you start `ltid` with `-v`, `tldd` and `tldcd` are also started with `-v`.

`-t`

Terminates `tldcd`.

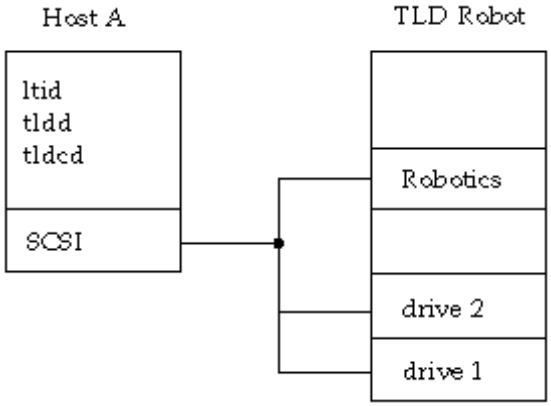
ERRORS

`tldd` and `tldcd` log an error message if there is another copy of the daemon running.

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.

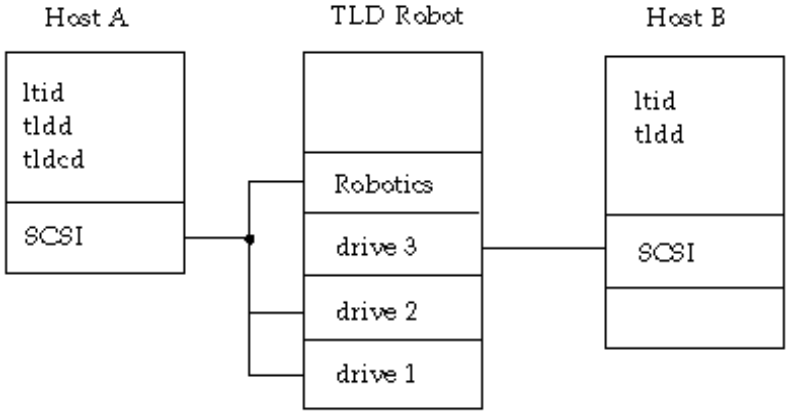
EXAMPLES

In the following diagram, the two drives and the robotics connect to Host A. `ltid` initiates `tldd`, which in turn initiates `tldcd`.



The following 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 machine 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.



SEE ALSO

`ltid(1M), syslog(8), tpclean(1M), tpconfig(1M), vmadm(1M)`

tlhd(1M)

NAME

tlhd, tlhcd - Tape Library Half-inch (TLH) daemon and control daemon

SYNOPSIS

```
/usr/openv/volmgr/bin/tlhd [-v]
/usr/openv/volmgr/bin/tlhcd [-v] [-t]
```

DESCRIPTION

`tlhd` and `tlhcd` interface with Media Manager to mount and unmount tape volumes in a Tape Library Half-inch (TLH) robot.

`tlhd` directly interfaces with `ltid` (the Media Manager device daemon). `tlhd` runs on each host with a drive connection and sends mount and unmount requests to the control daemon, `tlhcd`.

`tlhcd` communicates with the IBM Automated Tape Library (ATL) library manager, which processes all requests and control functions for the robotic library. TLH robotic control software permits drives in the same robot to be configured on different hosts. `tlhcd` can be running on a different host than `tlhd`, depending on where the IBM library control is configured (see EXAMPLES). When communication with the library is established, `tlhd` puts the TLH robot in the UP state and can request volume mounts and unmounts. If the library or control daemon is inaccessible, `tlhd` changes the robot to the DOWN state. In this state, `tlhd` is still running and returns the robot to the UP state if `tlhcd` is able to make a connection.

Note If drives are on different hosts, the robotic information must be entered in the Media Manager device configuration on all machines and the robot number must be the same on all machines.

`tlhd` and `tlhcd` are automatically started when `ltid` is started and stopped when `ltid` is stopped. You can stop and start `tlhd` independently of `ltid` using `/usr/openv/volmgr/bin/vmps` or your server's `ps` command to identify the `tlhd` process id and then entering the following commands:

`kill` *tlhd_pid*

`/usr/openv/volmgr/bin/tlhd [-v] &`

`tlhcd` is on the host that has the robotic control and is automatically started by `tlhd` on that host. `tlhcd` is terminated when you stop `ltid`.

The Media Manager media ID for volumes to be used in the library must be defined in the volume database before any volumes can be accessed using `ltid`, `tlhd`, and `tlhcd`. Both the initial volume database population and future updates can be accomplished using Media Manager robotic inventory options.

The drives are configured using IBM device names. The robotic test utility, `tlhtest` (or `robtest` if the robot is configured), can be used to determine the device names associated with the robot. You can also use this utility along with IBM's `mtlib` command-line interface to verify library communications, status, and functionality.

Drive cleaning for Tape Library Half-inch robotic control must be configured through an IBM library manager console, since these operations are not made available to applications that are using the IBM library manager. For this reason, cleaning volumes cannot be defined through Media Manager. In addition, you cannot use the Media Manager utilities or the `tpclean`(1M) command for cleaning operations on drives under TLH robotic control.

The Internet service port number for `tlhcd` must be in `/etc/services`. If you are using NIS (Network Information Service), the entry found in this host's `/etc/services` file should be placed in the master NIS server database for services. To override the services file, create the file `/usr/openv/volmgr/database/ports/tlhcd` with a single line containing the service port number for `tlhcd`. The default service port number is 13717.

You must have root privileges to execute this command.

OPTIONS

`-v`

Logs debug information using `syslogd`. If you start `ltid` with `-v`, `tlhd` and `tlhcd` are also started with `-v`.

`-t`

Terminates `tlhcd`.

NOTES

This command applies only to NetBackup Enterprise Server.

ERRORS

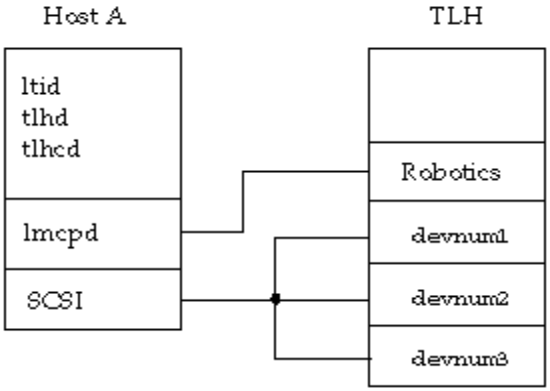
`tlhd` and `tlhcd` log an error message if there is a copy of the daemon running.

Media Manager logs any Tape Library Half-inch and robotic errors to `syslogd`. Log entries are also made when the state changes between UP and DOWN.

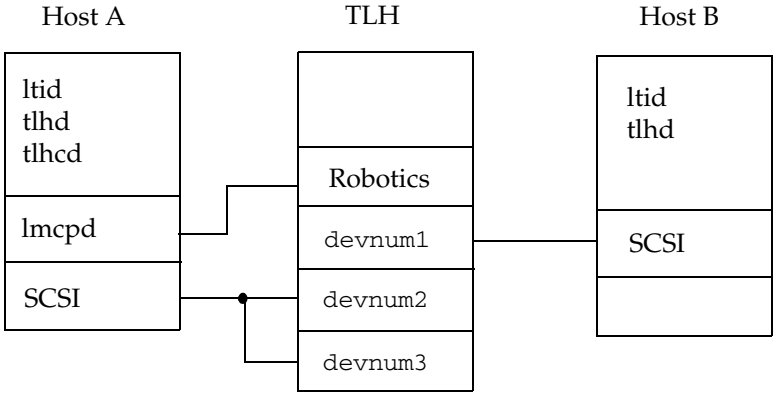
EXAMPLES

In the following examples the device hosts can be any supported Windows server, or the following UNIX servers: AIX, HP-UX, IRIX, or Solaris.

In the following diagram, the drives are attached to and the robotics are controlled from a single host. `ltid` initiates `tlhd`, which in turn initiates `tlhcd`. The IBM library manager control-point daemon (`lmcpd`) must be running on Host A.



In the following diagram, each host is connected to at least one drive and the robotics are controlled from Host A. `ltid` on each machine initiates `tlhd`. The `tlhd` on Host A also initiates `tlhcd`, since that is where the robotic control is defined. Requests to mount tapes from Host B go to `tlhd` on Host B, which sends the robotic command to `tlhcd` on Host A.



SEE ALSO

`ltid(1M), syslog(8), tpclean(1M), tpconfig(1M), vmadm(1M)`

tlmd(1M)

NAME

tlmd - Tape Library Multimedia (TLM) daemon

SYNOPSIS

```
/usr/openv/volmgr/bin/tlmd [-v]
```

DESCRIPTION

`tlmd` interfaces with Media Manager to mount and unmount tapes in a Tape Library Multimedia (TLM) robot. It is initiated by `ltid` (the Media Manager device daemon), if drives have been defined in Media Manager to be in a Tape Library Multimedia robot.

`tlmd` communicates with the ADIC Distributed AML Server (DAS), which is a client/server software product designed to provide shared access to the family of ADIC Automated Media Libraries (AML). When the connection is established, `tlmd` puts the TLM robot in the UP state and can request inventories as well as media mounts and dismounts. If the connection cannot be established or DAS errors occur, `tlmd` changes the robot to the DOWN state but keeps running. In this state, `tlmd` keeps running and returns the robot to the UP state when the problem no longer exists.

For each TLM robot defined, `tlmd` connects to the DAS server that is defined by the DAS server attribute in the TLM robot entry in the Media Manager device configuration. From the perspective of DAS, `tlmd` is connecting as a DAS client. The host running `tlmd` establishes communication as the DAS client that is specified by the `DAS_CLIENT` entry in the Media Manager configuration file, `/usr/openv/volmgr/vm.conf`. If no `DAS_CLIENT` entry exists, the DAS client name will be the standard host name for the host that is running `tlmd`.

You can stop and start `tlmd` independently of `ltid` using `/usr/openv/volmgr/bin/vmps` or your server's `ps` command to identify `tlmd`'s process id and then entering the following commands:

`kill` *tlmd_pid*

```
/usr/openv/volmgr/bin/tlmd [-v] &
```

The drives are configured using DAS drive names, based on information obtained from the DAS server. The robotic test utility, `tlmtest` (or `robtest` if the robot is configured), can be used to determine the drive names associated with the robot. You can also use ADIC's `DASADMIN` to verify library communications, status, and functionality.

The Internet service port number for `tlmd` must be in `/etc/services`. If you are using NIS (Network Information Service), you should place the entry in this the host's `/etc/services` file in the master NIS server database for services. To override the

services file, create the file `/usr/openv/volmgr/database/ports/tlmd` with a single line containing the service port number for `tlmd`. The default service port number is 13716.

You must have root privileges to execute this command.

OPTIONS

`-v`

Logs debug information using `syslogd`. If you start `ltid` with `-v`, `tlmd` also starts with `-v`.

NOTES

This command applies only to NetBackup Enterprise Server.

ERRORS

`tlmd` returns an error message if there is a copy of `tlmd` running.

Tape Library Multimedia robot and network errors are logged using `syslogd`. Log entries are also made when the state changes between UP and DOWN.

SEE ALSO

`ltid(1M), syslogd(8), tpconfig(1M), vmadm(1M)`

tpautoconf(1M)

NAME

tpautoconf - Manage the global device database host

SYNOPSIS

```
/usr/openv/volmgr/bin/tpautoconf -get_gdbhost

/usr/openv/volmgr/bin/tpautoconf -set_gdbhost host_name

/usr/openv/volmgr/bin/tpautoconf -preview Global Database host
         1 Global Database host 2

/usr/openv/volmgr/bin/tpautoconf -merge Global Database host 1
         Global Database host 2

/usr/openv/volmgr/bin/tpautoconf -report_disc

/usr/openv/volmgr/bin/tpautoconf -replace_drive drive_name
         -path drive_path

/usr/openv/volmgr/bin/tpautoconf -replace_robot robot_number
         -path robot_path
```

DESCRIPTION

`tpautoconf` is normally used by the Device Configuration wizard to automatically discover and configure devices. This wizard calls `tpautoconf` with a different set of options.

The `get` and `set` options described here are useful only in special situations; for example, to specify a different host as the global device database host. The global device database host name is automatically defined when NetBackup is installed. See the Configuring Storage Devices chapter of the NetBackup Media Manager system administrator's guide for information about managing the global device database host.

The merge and preview options are also useful in very specific situations. These options provide users with an automated utility for merging device domains (for example, merging global databases). In the synopsis above, the Media and Device Management (MDM) Domain Server is the host_name_1.

A user can use the `-report_disc`, `-replace_drive`, and `-replace_robot` options to re-configure the device databases to reflect a serial number change caused by the replacement of configured device. The correction process requires that after hardware replacement, at least one system must be made available through the operating system. This may require re-mapping, re-discovery, and/or rebooting the system. Refer to, "Making Changes to your Existing Configuration", in the *NetBackup Shared Storage System Administrator's Guide* for instruction on how to reconfigure the Media Manager device

databases. After you configure the server(s), use the `-report_disc` option to scan the current hardware, and compare it with the configured hardware. A list of discrepancies is produced and shows the replaced hardware, and the new hardware.

Note: Not all servers will have access to Robotic hardware. Even though this is expected, these robots will be listed as missing.

All servers must be running NetBackup 5.0 or better for `-replace_drive` or `-replace_robot` to properly reconfigure them. For servers that are running older versions of NetBackup, manual reconfiguration are required (see `tpconfig`) after running `-replace_drive` and `-replace_robot`.

The final step to adding replacement hardware is to configure the hardware on all servers via their Operating Systems and then run the Device Configuration wizard to configure the new path information. Again, refer to, "Making Changes to Your Hardware Configuration", in the reference topics appendix in the *NetBackup Media Manager System Administrator's Guide for UNIX.*

You must have root privileges to execute this command.

OPTIONS

`-get_gdbhost`
: Returns the name of the host where the global device database is stored.

`-merge` *`host_name_1 host_name_2`*
: Merge the contents of Global Database host 2 into Global Database host 1. The host name variables can contain global database host names.

`-preview` *`host_name_1 host_name_2`*
: Preview a merge of Global Database host 2 into Global Database host 1. The host name variables can contain global database host names.

`-set_gdbhost host_name`
: Set the name of the host where the global device database will be stored.

`-report_disc`
: Report discrepancies between detected devices and Global Database.

`-replace_drive` *`drive_name`* `-path` *`drive_path`*
: After drive hardware replacement, correct the serial number in the local and Global Databases.

`-replace_robot` *`robot_number`* `-path` *`robot_path`*
: After robotic controller hardware replacement, correct the serial number in the local and Global Databases.

NOTES

Only limited validation of the option parameters is done.

All affected databases will be saved before they are altered with the extension .tpacbak. All hosts must be at the same version of NetBackup and all must be running NetBackup before this utility will attempt to merge databases.

The intent of this utility is to provide a way for users to centralize their NetBackup Media Manager databases. Having all NetBackup Media Manager databases centralized and merged is preferable to distributing media and device domains for one NetBackup Master Server. For more information see, "NetBackup Media Manager Best Practices" in the *NetBackup Media Manager System Administrator's Guide*.

EXAMPLES

Example 1

The following command returns the name of the host where the global device database is stored:

```
tpautoconf -get_gdbhost
```

Example 2

The following command sets the global device database host to be the host niagra:

```
tpautoconf -set_gdbhost niagra
```

Example 3

The following command merges the contents of the global database on host "spain" into the global database on host "flash"

```
tpautoconf -merge flash spain
```

Example 4

The following command reports the ability of this utility to merge the global database on host "spain" into the global database on host "flash" with specific merge conflicts the user must resolve before merging

```
tpautoconf -merge flash spain
```

Example 5

The following example shows how the `-report_disc` command is used to report discrepancies between detected devices and Global Database. In addition, an example of how to use the `-replace` *drive_name* `-path` *drive_path* command is included.

```
# /usr/openv/volmgr/bin/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 = dandelion
  Host = avocadocat


# /usr/openv/volmgr/bin/tpautoconf -replace_drive QUANTUMDLT800014
-path /dev/rmt/119cbn
Found a matching device in global DB, QUANTUMDLT800014 on host
dandelion
 update of local DB on host dandelion completed
 globalDB update for host dandelion completed
Found a matching device in global DB, QUANTUMDLT800014 on host
avocadocat
 update of local DB on host avocadocat completed
 globalDB update for host avocadocat completed
```

EXAMPLES

tpconfig(1M), vmdb_merge(1M)

tpclean(1M)

NAME

tpclean - manages tape drive cleaning

SYNOPSIS

```
/usr/openv/volmgr/bin/tpclean -L
/usr/openv/volmgr/bin/tpclean -C drive_name
/usr/openv/volmgr/bin/tpclean -M drive_name
/usr/openv/volmgr/bin/tpclean -F drive_name cleaning_frequency
```

DESCRIPTION

`tpclean` enables you to monitor Media Manager tape drive usage and optionally configure tape drives to be automatically cleaned (except drives in ACS, LMF, ODL, RSM, or TLH robots; or shared (SSO) drives; 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.

Drive cleaning occurs, if the following 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 will contain the message, NEEDS CLEANING, if the following are true. You can then manually clean the drive and reset the mount time using the `-M` option.

- The mount time exceeds the cleaning frequency.
- The drive is a standalone drive or does not have a cleaning tape defined.

For the `-C`, `-M`, and `-F` options, `ltid` must be running. You must also have root privileges to execute this command.

See the reference topics appendix of the Media Manager system administrator's guide for information about the TapeAlert feature that is available with most tape drives, and other related drive cleaning topics.

You must have root privileges to execute 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 cleaning tape defined 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.

`-L`

Prints cleaning statistics to `stdout`.

`-M` *drive_name*

Use this option to indicate that the drive has been 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 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 0 and 10,000 hours.

The following applies only to NetBackup Enterprise Server:

Frequency-based cleaning is not supported for shared drives.

NOTES

tpconfig -d, tpconfig -l, and vmoprcmd may truncate long drive names. Please use tpconfig -dl to obtain the full drive name.

tpclean truncates drive names to 22 characters.

EXAMPLES

The following example displays cleaning statistics. An asterisk next to the drive type means the device is defined as robotic.

```
#tpclean -L
Drive Name    Type    Mount Time   Frequency    Last Cleaned    Comment
**********    ****    **********   **********   ************    *******
rob_A_drv1    8mm*       11.4         30        14:33 05/29/92
4mm_drv5      4mm         5.6         10        13:01 06/02/92
dlt_drv6      dlt         3.0          0            N/A
```

The following example sets the cleaning frequency for the drive named `dlt_drv6` to 25 hours. The drive will be flagged as needing cleaning after 25 hours of mount time has occurred.

```
tpclean -F dlt_drv6 25
```

The following example resets the mount time for the drive named `rob_A_drv1` to zero. You would normally use this command after you had manually cleaned the drive.

```
tpclean -M rob_A_drv1
```

The following example initiates the cleaning of drive `rob_A_drv1`. This example assumes 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 prior to reaching *cleaning_frequency*. Normally, robotic drives are cleaned automatically when their mount time exceeds the cleaning frequency.

```
tpclean -C rob_A_drv1
```

Note To use a cleaning tape, the Cleanings Remaining for that tape (as shown in the volume list of the **Media** node in the NetBackup Administration Console or from the `vmquery` command) must be greater than zero. This cleaning count refers to how many more times the cleaning tape can be used. You can change this count using the **Media** node or the `vmchange` command.

SEE ALSO

`ltid(1M), tpconfig(1M), vmadm(1M)`

tpconfig(1M)

NAME

tpconfig - tape configuration utility

SYNOPSIS

```
/usr/openv/volmgr/bin/tpconfig [-noverify]

/usr/openv/volmgr/bin/tpconfig -d

/usr/openv/volmgr/bin/tpconfig -dl

/usr/openv/volmgr/bin/tpconfig -l

/usr/openv/volmgr/bin/tpconfig -lsavdbhost

/usr/openv/volmgr/bin/tpconfig -add -drive -type drvtype -path
        drivepath [-vhname opticalvolhdrdrvname] [-asciiname
        asciidrivename] [-index drvindex] [-shared [yes|no]]
        [-cleanfreq hours] [-comment comment] [-drstatus
        [UP|DOWN]] [-robot robnum -robtype robtype] [-noverify]
        [-robdrnum robdrvnum | -VendorDrvName venddrvname | -ACS
        acsnum -LSM lsmnum -PANEL panelnum -DRIVE drivenum]

/usr/openv/volmgr/bin/tpconfig -update -drive drvindex [-type
        drvtype] [-path drivepath] [-vhname opticalvolhdrdrvname]
        [-newasciiname asciidrivename] [-shared [yes|no]]
        [-cleanfreq hours] [-comment comment] [-drstatus
        [UP|DOWN]] [-robot robnum -robtype robtype] [-noverify]
        [-robdrnum robdrvnum | -VendorDrvName venddrvname | -ACS
        acsnum -LSM lsmnum -PANEL panelnum -DRIVE drivenum]

/usr/openv/volmgr/bin/tpconfig -delete -drive drvindex

/usr/openv/volmgr/bin/tpconfig -multiple_delete -drive
        drvindex1:drvindex2: ... drvindexN

/usr/openv/volmgr/bin/tpconfig -add -robot robnum -robtype
        robtype -robpath robpath [-vdbhost volume_database_host]

/usr/openv/volmgr/bin/tpconfig -add -robot robnum -robtype
        robtype -cntlhost cntlhost [-vdbhost volume_database_host]

/usr/openv/volmgr/bin/tpconfig -update -robot robnum [-robtype
        robtype] [-robpath robpath] [-cntlhost cntlhost] [-vdbhost
        volume_database_host]

/usr/openv/volmgr/bin/tpconfig -delete -robot robnum
```

`/usr/openv/volmgr/bin/tpconfig -multiple_delete -robot` *robnum1*`:`*robnum2*`: ...` *robnumN*

`/usr/openv/volmgr/bin/tpconfig -savdbhost` *standalone_volume_database_host*

DESCRIPTION

`tpconfig` can be used as a command line interface or menu interface to configure robots and drives for use with NetBackup.

`/usr/openv/volmgr/bin/tpconfig [-noverify]` starts the Media Manager Device Configuration Utility. This menu-based utility creates and modifies databases in the `/usr/openv/volmgr/database` directory. These databases identify the robotics and drives that are under control of `ltid` (the Media Manager device daemon). `ltid` uses these files 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 recognized by the system 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 and then specify this device path for the drive. `tpconfig` then records the device path in the appropriate device database.

After using `tpconfig` to change your device configuration, use the `stopltid` command to stop the `ltid` and `avrd` (automatic volume recognition) daemons (if they are running). Then use the `ltid` command to start the daemons again. See `ltid(1M)` for more information.

You must have root privileges to execute this utility.

OPTIONS

`-l`
: Lists the current device configuration (to `stdout`), without volume database host names.

`-d`
: Lists the current configuration information (to `stdout`), including volume database host names.

`-dl`
: Lists the full drive name.

`-lsavdbhost`
: Lists the volume database host for standalone drives. This is the host where the Media Manager volume daemon maintains the volume configuration for standalone drives.

`-noverify`

If this option is specified, 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 no rewind, variable, Berkeley-style, and so on. This option is normally not required, but may be helpful if using non-standard platform device files. If this option is specified, caution should be taken in making sure the device files are correct.

`-add`

Adds a drive or a robot, depending on the accompanying options.

`-update`

Changes the configuration information for a drive or robot. For example, you can add a drive to a robot.

`-delete`

Deletes a drive or robot, depending on the accompanying options.

`-multiple_delete`

Deletes multiple drives or robots, depending on the accompanying options.

`-savdbhost` *standalone_volume_database_host*

Sets the volume database host for standalone drives that attach to this specified host.

`-drive`

Use this option with the `-add` option to specify that the action is for a drive.

`-drive` *drvindex*

Use this option with the `-update`, `-delete`, or `-multiple_delete` options to specify the drive index and that the action is for a drive.

`-type` *drvtype*

Specifies the type of drive that you are configuring.

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, `odiskwm` for optical disk-write many drive, `odiskwo` for optical disk-write once drive.

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.

`-path` *drivepath*
: Specifies the system name for the drive. For example, `/dev/rmt/0cbn`.

`-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.

`-index` *drvindex*
: A drive index is 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 the next available drive index is used by Media Manager. Each drive on a particular host must have a unique index number.

`-drstatus UP|DOWN`
: Sets the initial status of the drive to the UP or DOWN state. You can also perform this action with options in the Device Management window.

`-cleanfreq` *hours*
: Specifies the number of hours between drive cleanings. When you add a drive, NetBackup starts recording 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, cleaning occurs when the accumulated mount time exceeds the time that you specify for cleaning frequency. NetBackup resets the mount time when the drive is cleaned.

  If the drive is standalone or if a cleaning tape is not defined, the message NEEDS CLEANING appears in the comment field of the `tpclean -L` output. To clean the drive, use the `tpclean` command.

  Frequency-based cleaning is not needed if TapeAlert is used.

`-robot` *robnum*
: A unique number that identifies the robot to NetBackup. You assign the robot number when you add the robot using the `add` option.

  Robot numbers must be unique for all robots, regardless of the robot type or the host that controls them.

`-robtype` *robtype*
: Specifies the type of robot that you are configuring and can be any of the types supported by NetBackup. Check the VERITAS support web site 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, `lmf` for Library Management Facility, `tl4` for Tape Library 4mm, `tl8` for Tape Library 8mm, `tld` for Tape Library DLT, `tlh` for Tape Library Half-inch, `tlm` for Tape Library Multimedia, `ts8` for Tape Stacker 8mm, `tsd` for Tape Stacker DLT, `tsh` for Tape Stacker Half-inch, `odl` for Optical Disk Library.

Robot type can be any of the following for NetBackup Server:

`tl4` for Tape Library 4mm, `tl8` for Tape Library 8mm, `tld` for Tape Library DLT, `ts8` for Tape Stacker 8mm, `tsd` for Tape Stacker DLT.

`-robdrnum` *robdrvnum*

Specifies the physical location (within the robot) of the drive. If you assign the wrong number, NetBackup does not detect it, but an error eventually occurs because the robotic control attempts 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.

The Robot Slot and Layout appendix of the Media Manager system administrator's guide shows drive layouts for many of the robots that NetBackup supports.

`-ACS` *acsnum*

`-LSM` *lsmnum*

`-PANEL` *panelnum*

`-DRIVE` *drivenum*

These four options are only applicable for NetBackup Enterprise Server.

These options specify the configuration for ACS (Automated Cartridge System) robots.

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.

`-VendorDrvName` *venddrvname*

Specifies the IBM device name for a TLH robotic drive or the DAS drive name for a TLM robotic drive.

`-vhname` *opticalvolhdrdrvname*

Specifies the volume header path for an optical drive.

`-shared yes|no`

This option is only applicable for NetBackup Enterprise Server.

Specify `yes`, if the drive you are adding or updating will be shared among hosts.

`-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.

The following applies only to NetBackup Enterprise Server:

If you are adding or updating shared drives (SSO option), make this name as descriptive as possible.

`-newasciiname` *asciidrivename*
Specifies a new name for the drive.

`-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 LMF, TL8, TLD, and TLH, robots that can have the robotic control on another host, and for ACS and TLM robots.

For an ACS robot, specify the host name where the ACS library software is installed.

For a TLM robot, specify the host name where the DAS server software is installed.

`-robpath` *robpath*
If the robot that you are adding or updating is a UNIX host or Windows 2000 host with the robotic control, use this option.

`-vdbhost` *volume_database_host*
This option is only applicable for NetBackup Enterprise Server.

For a robot, this specifies the volume database host. This is the host that will have the information about the media in the robot.

NOTES

The `-cleanfreq` option cannot be used with shared drives.

tpconfig -d may truncate drive names to 22 characters.

tpconfig -l may truncate drive names to 32 characters.

Use tpconfig -dl to obtain the full drive name.

FILES

`/usr/openv/volmgr/database/ltidevs`

```
/usr/openv/volmgr/database/robotic_def
/usr/openv/volmgr/help/tpconfig* (Help files)
```

SEE ALSO

ltid(1M)

tpformat(1M)

NAME

tpformat - formats optical disks for use by Media Manager

SYNOPSIS

```
/usr/openv/volmgr/bin/tpformat -m media_id [-d odiskwm |
         odiskwo] [-f] [-o] [-rn robot_number]
```

DESCRIPTION

The `tpformat` command writes a volume label (including a media ID) on an optical disk platter. When used with the `-f` option, this command also formats the platter.

The volume label, a partition table required by disk drivers on most operating system platforms, contains the media ID. The recorded media ID is also kept in the volume database as the media ID. When a platter is mounted, Media Manager compares the recorded media ID to the media ID that was requested to verify that the correct platter is mounted.

You specify a media ID to be written on the disk. An external media ID is an identifier that is written on the outside of the volume so the operator can find the volume. The recorded media ID and external media ID must always be the same or the wrong volume will be mounted.

Whether it is necessary to label an optical disk with `tpformat` depends on the platform that has the optical disk drive as follows:

- On Sun Solaris and SGI IRIX platforms, you must use `tpformat` to write a system-specific volume label (that is, a partition table) and media ID on each side of a platter before you can use it with Media Manager. This action is required regardless of whether the platter has been formatted. However, if the platter is preformatted you do not have to reformat it.
- On HP-UX and IBM AIX systems, volume labels do not apply and it is not mandatory to use `tpformat`, unless you must use it to format the volume. However, labeling is still recommended so the volume will have an media ID that Media Manager can use to verify that the correct volume is mounted.

All optical disk platters must be formatted before Media Manager can use them. You can purchase preformatted platters (recommended) or format them manually with the `-f` option.

You must be a root user to execute `tpformat` and you can use it only on the server that has the optical drive. For example, you cannot use `tpformat` on a NetBackup master server to format media that is mounted in a drive on a NetBackup media server. In addition, the drive must be under control of Media Manager, with the device daemon (`ltid`) running.

This command causes a mount request to appear in the operator displays; or if the volume is in a robot and the media ID that you specify exists in the volume database, the volume is automatically mounted.

When using one of the available media management interfaces to add media to Media Manager, you can choose the label option, making it unnecessary to use `tpformat`.

You must have root privileges to execute this command.

OPTIONS

`-m` *media_id*

Writes a media ID on an optical platter. You can specify up to six alpha-numeric characters for the ID. This media ID is also referred to as the recorded media ID when it is read from the platter.

`-d odiskwm | odiskwo`

The density (media type) that is being formatted. The default is `odiskwm`.

`odiskwm` specifies rewritable (write many) media.

`odiskwo` specifies write once (WORM) media. WORM media can be formatted only once by `tpformat`.

`-f`

Formats the selected disk surface. Since it takes approximately 25 minutes per surface to format, use this option only for disks not formatted at the factory.

`-o`

You must specify this option (overwrite) to use `tpformat` on a platter that has an recorded media ID (that is, the platter contains a label).

`-rn` *robot_number*

Verifies that the robot number specified is configured and is a valid robot type that supports the formatting of optical volumes.

NOTES

This command applies only to NetBackup Enterprise Server.

EXAMPLES

The following example writes `diska` as the media ID and a volume header to a rewritable optical disk:

```
tpformat -m diska -d odiskwm
```

In the following example a platter has a recorded media ID. To overwrite the current label and specify a new media ID you must specify the `-o` option:

```
tpformat -o -m disk1 -d odiskwm
```

SEE ALSO

`ltid(1M), tpconfig(1M), tpreq(1), vmadm(1M)`

tpreq(1)

NAME

tpreq - request a tape volume for mounting and associate a file name with the assigned drive

SYNOPSIS

`/usr/openv/volmgr/bin/tpreq -m` *media_id* `[-a` *accessmode*`] [-d` *density*`] [-p` *poolname*`] [-f]` *filename*

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 and 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` will 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.

When a `tpreq` command is executed, a call is made to the script `drive_mount_notify` immediately after the media has been successfully placed in a pre-selected drive. This script is located in the `/volmgr/bin` directory and usage information is documented within the script. This script is only called from the `tpreq` command for drives that are in robots and is not valid for standalone drives.

The following applies only to NetBackup Enterprise Server:

If you request optical disk densities (`odiskwm` or `odiskwo`), `tpreq` acts differently than with sequential tape devices. The logical file name is a link to the data partition of the disk device. By default, it is the character device. Optical platters are labeled by `tpformat` with the volume-header partition being the label and the data partition being the rest of the disk.

You must have root privileges to execute this command.

OPTIONS

`-m` *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.

`-a` *accessmode*

Specifies the access mode of the volume. Valid access modes are `w` and `r`. If the access mode is `w` (write), the media must be mounted with write enabled. The default is `r` (read), which means the media may be write protected.

`-d` *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 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, hcart for 1/2 Inch cartridge, hcart2 for 1/2 Inch cartridge 2, hcart3 for 1/2 Inch cartridge 3, odiskwm for Optical disk-write many, odiskwo for Optical disk-write once, qscsi for 1/4-inch cartridge.

The following applies only to NetBackup Enterprise Server:

The half-inch cartridge densities (hcart, hcart2, and 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, a tape request with density hcart2 specifying a media ID with media type HCART2 will be assigned to an hcart2 drive. Likewise, a tape request with density hcart specifying an media ID with media type HCART will be assigned to an hcart drive. The same rules apply to the DLT densities (dlt, dlt2, and 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, 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.

`-p` *poolname*

Specifies the volume pool where the volume resides. *poolname* is case sensitive. The default is None.

`-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 named in the path. *filename* cannot be an existing file.

Specifying `-f` before *filename* is optional.

SEE ALSO

`tpformat(1M), tpunmount(1), vmadm(1M)`

tpunmount(1)

NAME

tpunmount - removes a tape volume from a drive and tape file from the directory

SYNOPSIS

`/usr/openv/volmgr/bin/tpunmount [-f]` *filename* `[-force]`

DESCRIPTION

`tpunmount` removes a tape file from the directory and removes the tape volume from the drive (if the media was mounted).

Standalone drives are *not* unloaded (if the `-force` option is *not* specified) in the following cases:

- The `ltid` option, `-nsu` (no standalone unload) was specified.
- The `DO_NOT_EJECT_STANDALONE` option was specified in the `vm.conf` file.

When a `tpunmount` command is executed for drives that are not NDMP drives, a call is made to the script `drive_unmount_notify`. This script is located in the `/volmgr/bin` directory and usage information is documented within the script.

The tape file and the device must be closed before you can use `tpunmount`.

You must have root privileges to execute this command.

OPTIONS

`-f` *filename*

Specifies the file associated with the media. You must specify a file name.

Specifying `-f` before *filename* is optional.

`-force`

Ejects the volume from a standalone drive, even if the `-nsu` option was specified for `ltid` or `DO_NOT_EJECT_STANDALONE` was specified in the `vm.conf` file, at the time `ltid` was started.

EXAMPLE

The following command unmounts the tape volume associated with file `tape1` and removes the file from the current directory:

```
tpunmount tape1
```

SEE ALSO

`tpreq(1), ltid(1M)`

ts8d(1M)

NAME

ts8d - Tape Stacker 8MM (TS8) daemon

SYNOPSIS

```
/usr/openv/volmgr/bin/ts8d [-v]
```

DESCRIPTION

`ts8d` interfaces with Media Manager to mount and unmount tapes in a Tape Stacker 8MM robot. It is initiated by `ltid` (the Media Manager device daemon), if the Media Manager device configuration shows drives in a Tape Stacker 8MM.

Stopping `ltid` stops `ts8d`. You can stop or start `ts8d` independently of `ltid` using the `/usr/openv/volmgr/bin/vmps` command or your server's `ps` command to identify the `ts8d` process id and then entering the following commands:

`kill` *ts8d_pid*

`/usr/openv/volmgr/bin/ts8d [-v] &`

`ts8d` communicates directly with the robotics through a SCSI interface. When the connection is established (the path for robotics can be opened), `ts8d` puts the TS8 robot in the UP state and can mount and unmount tapes. If the robotics are inaccessible, `ts8d` changes the robot to the DOWN state. In this state, `ts8d` is still running and returns the robot to the UP state if it is able to make a connection.

The media ID and slot number information for 8mm tapes in a robot must be defined in the volume database before any tapes can be accessed through `ltid` and `ts8d`.

If a cleaning volume is used, it must be defined in the volume configuration. See `tpclean(1M)` for information on setting the frequency for automatic drive cleaning.

The Internet service port number for `ts8d` must be in `/etc/services`. If you are using NIS (Network Information Service), you should place the entry in this host's `/etc/services` file in the master NIS server database for services. To override the services file, create the file `/usr/openv/volmgr/database/ports/ts8d` with a single line containing the service port number for ts8d. The default service port number is 13709.

You must have root privileges to execute this command.

OPTIONS

`-v`

Logs debug information using `syslogd`. If you start `ltid` with `-v`, `ts8d` also starts with `-v`.

ERRORS

`ts8d` returns an error message if there is a copy of `ts8d` running.

Media Manager logs any Tape Stacker 8MM and robotic errors to `syslogd`. Log entries are also made when the state changes between UP and DOWN.

SEE ALSO

`ltid(1M), syslogd(8), tpclean(1M), tpconfig(1M), vmadm(1M)`

tsdd(1M)

NAME

tsdd - Tape Stacker DLT (TSD) daemon

SYNOPSIS

```
/usr/openv/volmgr/bin/tsdd [-v]
```

DESCRIPTION

`tsdd` interfaces with Media Manager to mount and unmount tapes in Tape Stacker DLT (TSD) robots. It is initiated by `ltid` (the Media Manager device daemon), if the Media Manager device configuration shows drives in the Tape Stacker DLT (TSD).

Stopping `ltid` stops `tsdd`. You can stop or start `tsdd` independently of `ltid` using the `/usr/openv/volmgr/bin/vmps` command or your server's `ps` command to identify the process id for `tsdd`, and then entering the following commands:

`kill` *tsdd_pid*

```
/usr/openv/volmgr/bin/tsdd [-v] &
```

`tsdd` communicates directly with the robotics using a SCSI interface. When the connection is established (the path for robotics can be opened), `tsdd` puts the TSD robot in the UP state and can mount and unmount tapes. If the robotics are inaccessible, `tsdd` changes the robot to the DOWN state. In this state, `tsdd` is still running and returns the robot to the UP state if it is able to make a connection.

The media ID and slot number information for DLT tapes in a robot must be defined in the volume database before any tapes can be accessed through the `ltid` and `tsdd`.

If a cleaning volume is used, it must be defined in the volume configuration. See `tpclean(1M)` for information on setting the frequency for automatic drive cleaning.

The Internet service port number for tsdd must be in `/etc/services`. If you are using NIS (Network Information Service), you should place the entry in this host's `/etc/services` file in the master NIS server database for services. To override the services file, create the file `/usr/openv/volmgr/database/ports/tsdd` with a single line containing the service port number for `tsdd`. The default service port number is 13714.

You must have root privileges to execute this command.

OPTIONS

`-v`

Logs debug information using `syslogd`. If you start `ltid` with `-v`, `tsdd` also starts with `-v`.

ERRORS

`tsdd` returns an error message if there is a copy of `tsdd` running.

Media Manager logs any Tape Stacker DLT robot and robotic errors to `syslogd`. Log entries are also made when the state changes between UP and DOWN.

SEE ALSO

`ltid(1M), tpclean(1M), tpconfig(1M), vmadm(1M)`

tshd(1M)

NAME

tshd - Tape Stacker Half-inch (TSH) daemon

SYNOPSIS

```
/usr/openv/volmgr/bin/tshd [-v]
```

DESCRIPTION

`tshd` interfaces with Media Manager to mount and unmount tapes in Tape Stacker Half-inch (TSH) robots. It is initiated by `ltid` (the Media Manager device daemon), if drives have been defined in Media Manager to be in a TSH robot.

This daemon communicates directly with the robotics using a SCSI interface. When the connection is established (that is, the path for robotics can be opened), `tshd` puts the TSH robot in the UP state and can mount and unmount tapes. If the robotics are inaccessible, `tshd` changes the robot to the DOWN state. In this state, `tshd` is still running and it returns the robot to the UP state when it is able to make a connection.

You can stop or start `tshd` independently of `ltid` using the `/usr/openv/volmgr/bin/vmps` command or your server's `ps` command to identify `tshd`'s process id and then entering the following commands:

`kill` *tshd_pid*

`/usr/openv/volmgr/bin/tshd [-v] &`

The media ID and slot number information for half-inch tapes in a TSH robot must be defined in the volume database before any tapes can be accessed using `ltid` and `tshd`.

A cleaning volume can also reside in the tape stacker and if so, must be defined. See `tpclean(1M)` for information on setting the frequency for automatic drive cleaning.

The Internet service port number for `tshd` must be in `/etc/services`. If you are using NIS (Network Information Service), you should place the entry in this host's `/etc/services` file in the master NIS server database for services. To override the services file, create the file `/usr/openv/volmgr/database/ports/tshd` with a single line containing the service port number for `tshd`. The default service port number is 13715.

You must have root privileges to execute this command.

OPTIONS

`-v`

Logs debug information using `syslogd`. If you start `ltid` with `-v`, `tshd` also starts with `-v`.

NOTES

This command applies only to NetBackup Enterprise Server.

ERRORS

`tshd` returns an error message if there is another copy of `tshd` running.

Any Tape Stacker Half-inch and robotic errors are logged using `syslogd`. Log entries are also made when the state changes between UP and DOWN.

SEE ALSO

`ltid(1M), tpclean(1M), tpconfig(1M), vmadm(1M)`

verifytrace(1M)

NAME

verifytrace – trace debug logs for verify job[s]

SYNOPSIS

```
verifytrace [-master_server name] -job_id number [-start_time
         hh:mm:ss] [-end_time hh:mm:ss] [-install_path path]
         mmddyy [mmddyy _]

verifytrace [-master_server name] -backup_id id [-start_time
         hh:mm:ss] [-end_time hh:mm:ss] [-install_path path]
         mmddyy [mmddyy _]

verifytrace [-master_server name] [-policy_name name]
         [-client_name name] [-start_time hh:mm:ss] [-end_time
         hh:mm:ss] [-install_path path] mmddyy [mmddyy _]
```

DESCRIPTION

The `verifytrace` command consolidates the debug log messages for the specified verify job[s] and writes them to standard output. The messages will be sorted by time. *verifytrace* will attempt to compensate for time zone changes and clock drift between remote servers and clients.

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

If either `-job_id` or `-backup_id` is specified, `verifytrace` uses this option as the sole criteria for selecting the verify job[s] it will trace. The options `-policy_name` or `-client_name` cannot be used in conjunction with `-job_id` or `-backup_id`. If `-job_id` or –backup_id are not specified then all verify jobs that match the specified selection criteria will be selected. If none of the options namely, -job_id, -backup_id, -policy_name or -client_name is specified, then all the verify jobs executed on the days specified by day stamps (*mmddyy*) will be traced. If –start_time/-end_time options are used then the debug logs in the specified time interval are examined.

If `verifytrace` is started with the –backup_id <bid>option then verifytrace will look for a verify job started via bpverify with –backup_id <bid> option where the backup ids (<bid>) match.

If `verifytrace` is started with the –policy_name <policy> option then verifytrace will look for a verify job started via bpverify with –policy <policy> option where the policy names (<policy>) match.

If verifytrace is started with the –client_name <client> option then verifytrace will look for a verify job started via bpverify with –client <client> option where the client names (<client>) match.

`verifytrace` writes error messages to standard error.

You must have root privileges to execute this command.

OPTIONS

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

`-job_id`
: Job ID number of the verify job to analyze. Default is any job id.

`-backup_id`
: Backup ID number of the backup image verified by the verify job to analyze. Default is any backup ID.

`-policy_name`
: Policy name of the verify jobs to analyze. Default is any policy.

`-client_name`
: Client name of the verify jobs to analyze. Default is any client.

`-start_time`
: Earliest time stamp to start analyzing the logs. Default is 00:00:00.

`-end_time`
: Latest time stamp to finish analyzing the logs. Default is 23:59:59.

`-install_path`
: The NetBackup install path on the Windows NT and Windows 2000 server. Default is c:\Program Files\VERITAS.

  Note that the install path must be enclosed in quotes if the path includes a space.

`mmddyy`
: One or more “day stamps”. This identifies the log file names (log.mmddyy for UNIX, mmddyy.log for Windows NT and Windows 2000) that will be analyzed.

OUTPUT FORMAT

The format of an output line is:

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

`daystamp`
: The day of the log in yyyymmdd format.

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

`program`
: The name of program (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 actually appears in the debug log file.

EXAMPLES

Example 1

The following example analyzes the log of verify job with job ID 2 executed on August 6, 2002.

```
verifytrace -job_id 2 080602
```

Example 2

The following example analyzes the log of verify jobs that verify backup image with backup id *pride_1028666945* executed on *20th August 2002*. This command would analyze only those verify jobs, which were executed with option -backupid *pride_1028666945*.

```
verifytrace -backup_id pride_1028666945 082002
```

Example 3

The following example analyzes the log of verify jobs executed on policy *Pride-Standard* and client *pride* on August 16, 2002 and August 23, 2002. This command would analyze only those verify jobs, which were executed with options -policy *Pride-Standard* and -client *pride*.

```
verifytrace -policy_name Pride-Standard -client_name pride 081602
082302
```

Example 4

The following example analyzes the log of all verify jobs that are executed on August 5, 2002 and August 17, 2002.

```
verifytrace 080502 081702
```

vltadm(1M)

NAME

`vltadm` - Start the NetBackup Vault menu interface for administrators.

SYNOPSIS

```
/usr/openv/netbackup/bin/vltadm [-version]
```

DESCRIPTION

The `vltadm` utility is a menu interface that an administrator can use to configure NetBackup Vault. You must have root privileges to execute this command. In addition, this interface 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 System 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 returned to the system is 252, and 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

`/usr/openv/netbackup/help/vltadm/*`

`/usr/openv/netbackup/db/vault/vault.xml`

`/tmp/bp_robots`

`/tmp/bp_robots`

`/tmp/bp_vaults`

`/tmp/bp_profiles`

`/tmp/bp_duplicates`

`/tmp/_tmp`

SEE ALSO

`vltrun(1M)`

vltcontainers(1M)

NAME

`vltcontainers` - Move volumes logically into containers

SYNOPSIS

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

-run [-rn robot_number]

-run -usingbarcodes [-rn robot_number]

-run -vltcid container_id -vault vault_name -sessionid
         session_id

-run -vltcid container_id -f file_name [-rn robot_number]
         [-usingbarcodes]

-view [-vltcid container_id]

-change -vltcid container_id -rd return_date

-delete -vltcid container_id

-version
```

DESCRIPTION

`vltcontainers` logically adds media ejected from one or more vault sessions to containers. `vltcontainers` also can view, set, or change the return date of containers that are going off-site or are already at the off-site vault. `vltcontainers` can 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 media IDs.
- Use a keyboard interface bar code reader to scan the container 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 bar codes of all the media that will be added to one container. To add media to more than one container, you must enter the IDs using the keyboard or a keyboard interface bar code reader or you must invoke the `vltcontainers` command again and specify different container and filename options.
- Add all the media ejected by a specific session to one container. To add media from a single eject session into more than one container, you must enter the IDs using the keyboard or a keyboard interface bar code reader.

The `vltcontainers` command must be invoked from a NetBackup master server licensed for Vault.

If a directory named `/usr/openv/netbackup/logs/vault` with public-write access exists, `vltcontainers` will write to the daily debug log file (`log.DDMMYY` where *DDMMYY* is the current date) in this directory. Public-write access is required because not all executable files that write to this file 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 will be returned the latest. Requires the `-vltcid` *`container_id`* option and argument.

`-delete`
: Deletes the container record from the NetBackup and Media Manager catalogs. You can delete a container only if it contains no media. Requires the `-vltcid` *`container_id`* option and argument.

`-f` *`file_name`*
: Specifies the file from which to read media IDs. All media listed in the file will be added to the container specified by the `-vltcid` option. The file can be a list of media IDs (one per line) or the numeric equivalents of bar codes (one per line) scanned into a file by a bar code 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 volume database host from which the `vltcontainers` command should obtain media information. If `-rn` *`robot_number`* is not used, the master server is considered as the volume database host. Only media in the database on the volume database host can be added to containers.

`-run`
: Logically adds media to the container. If you specify no other options, you must enter the container and media IDs by using the keyboard. To use a bar code reader to scan the container and media IDs, specify the `-usingbarcodes` option. To add the media ejected by a specific session, use the `-vault` *`vault_name`* and `-sessionid` *`session_id`* options. To add the media specified in a file, use the `-f` *`file_name`* option. To specify a volume database host other than the master server, use the `-rn` *`robot_number`* option.

`-sessionid` *`session_id`*
: The ID of a vault session. All media ejected by the session specified will be added to the container specified by the `-vltcid` option.

`-usingbarcodes`
: Specifies that a keyboard interface bar code reader will be used to scan the container IDs and media IDs or that bar code numbers are used in the file specified by the `-f` *`file_name`* option. Keyboard interface bar code readers (also called keyboard wedge bar code 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`
: Display the `vltcontainers` version and exit.

`-view [-vltcid` *`container_id`*`]`
: Shows the return date assigned to all containers. Use the `-vltcid` *`container_id`* option and argument to show the return date of a specific container.

`-vltcid` *`container_id`*
: Specifies the container ID. Container ID can be a string of up to 29 alphanumeric characters (no spaces). When changing a container return date, requires the `-rd` *`return_date`* option and argument.

EXAMPLES

Example 1:

To add the volumes ejected from robot number 0 to containers and use a bar code reader to scan the container and media IDs, use the following command:

```
vltcontainers -run -usingbarcodes -rn 0
```

Example 2

To view the return date of container ABC123, use the following command:

```
vltcontainers -view -vltcid ABC123
```

Example 3

To change the return date of container ABC123 to December 07, 2004, use the following command:

```
vltcontainers -change -vltcid ABC123 -rd 12/07/2004
```

Example 4

To delete container ABC123 from the NetBackup and Media Manager catalogs, use the following command:

```
vltcontainers -delete -vltcid ABC123
```

Example 5

To add all media ejected by session 4 of vault MyVault_Cntrs to container ABC123, use the following command:

```
vltcontainers -run -vltcid ABC123 -vault MyVault_Cntrs -sessionid
4
```

Example 6

To add media listed in file `/home/jack/medialist` that are ejected from robot number 0 to container ABC123, use the following command:

```
vltcontainers -run -vltcid ABC123 -f /home/jack/medialist -rn 0
```

Example 7

To add media to container ABC123 that was ejected from a robot that is attached to the master server and read the bar codes for that media from file `/home/jack/medialist`, use the following command:

```
vltcontainers -run -vltcid ABC123 -f /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 returned to the system is 252, and 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 for UNIX and Windows* and in the NetBackup *Troubleshooting Wizard*.

FILES

`/usr/openv/netbackup/vault/sessions/cntrDB`

`/usr/openv/netbackup/db/vault/vault.xml`

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

SEE ALSO

`vltadm`, `vltoffsitemedia`, `vltopmenu`

vlteject(1M)

NAME

`vlteject` - Eject media and/or generate reports for previously run sessions

SYNOPSIS

The syntax for the command is:

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

-eject [-profile profile_name] [-robot robot_name] [-vault
         vault_name [-sessionid id]] [-auto y|n] [-eject_delay
         seconds] [-version]

-report [-profile profile_name] [-robot robot_name] [-vault
         vault_name [-sessionid id]] [-version]

-eject -report [-profile profile_name] [-robot robot_name]
         [-vault vault_name [-sessionid id]] [-auto y|n]
         [-eject_delay seconds] [-version]

vlteject -preview [-profile profile_name] [-robot robot_name]
         [-vault vault_name [-sessionid id]]
```

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/or reports for all sessions, for a specific robot, for a specific vault, or for a specific profile. To process all pending ejects and/or 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.

Depending on how it is called it can run interactively or not. Running interactively is most useful when you will be ejecting more media than will fit 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 NetBackup policy scheduling. 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 a directory named `/usr/openv/netbackup/logs/vault` with public-write access exists, `vltcontainers` will write to the daily debug log file (`log.DDMMYY` where *DDMMYY* is the current date) in this directory. Public-write access is required because not all executable files that write to this file run as administrator or root user. The host property **Keep vault logs for n days** determines how long the vault session directories are retained.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's 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 (n, the default), vlteject runs interactively, accepting input and displaying output.

`-eject`
: Eject media for the indicated sessions. This is optional in case eject has been done and only printing is desired. If you specify both the `-sessionid` and `-report` options, reports will be generated even if the eject stage has not been completed (although reports produced after the eject stage is completed will not be generated). If you do not specify the `-sessionid` option, the eject stage must be completed for the session before you can use `vlteject` to generate reports.

`-eject_delay` *`seconds`*
: The number of seconds to delay before ejecting. This is desirable if an operation such as backing up or duplication has just occurred on the affected media. The default is 0. The maximum is 3600 (one hour).

`-help`
: Displays a synopsis of command usage when it is the only option on the command line.

`-preview`
: Lists the sessions and the media that will be ejected for the sessions. Does not eject the media.

`-profile` *`profile_name`*
: The name of a profile or a robot number, vault, and profile for which to eject media and/or generate reports. If profile is used without robot and vault, the profile must be unique. To process all pending ejects and/or reports, do not use the `-profile`, `-robot`, or `-vault` option.

`-report`
: Generate reports for the indicated sessions. If you specify both the -sessionid and -report options, reports will be generated even if the eject stage has not been completed (although reports produced after the eject stage is completed will not be generated). If you do not specify the -sessionid option, the eject stage must be completed for the session before you can use `vlteject` to generate reports.

`-robot` *`robot_name`*
: The robot for which to eject media and/or generate reports. All vaults in the robot should use the same off-site volume group. To process all pending ejects and/or reports, do not use the `-profile`, `-robot`, or `-vault` option.

`-sessionid` *`id`*
: The numeric session ID. If the `-profile`, `-robot`, or `-vault` option is specified but the `-session` *`id`* option is not specified, `vlteject` will operate on all sessions for the specified profile, robot, or vault.

`-vault` *`vault_name`*
: The vault for which to eject media and/or generate reports. To process all pending ejects and/or reports, do not use the `-profile`, `-robot`, or `-vault` option.

`-version`
: Display the `vlteject` version and exit.

EXAMPLES

Example 1

To eject media and generate reports for all robots that have sessions for which media have not yet been ejected, enter the following:

```
vlteject -eject -report
```

Example 2

To eject all media that have not yet been ejected for all sessions for the CustomerDB vault and to generate corresponding reports, enter the following:

```
vlteject -vault CustomerDB -eject -report
```

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 returned to the system is 252, and 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 for UNIX and Windows* and in the NetBackup *Troubleshooting Wizard*.

FILES

/usr/openv/netbackup/db/vault/vault.xml

/usr/openv/netbackup/logs/bpbrmvlt/log.*mmddyy*

/usr/openv/netbackup/logs/vault/log.*mmddyy*

/usr/openv/netbackup/vault/sessions/*vault_name*/sid*xxx*/detail.log

/usr/openv/netbackup/vault/sessions/*vault_name*/sid*xxx*/summary.log

/usr/openv/netbackup/vault/sessions/*vault_name*/sid*xxx*/vlteject_status

/usr/openv/netbackup/vault/sessions/vlteject.mstr

/usr/openv/netbackup/bp.conf

SEE ALSO

vltopmenu(1M)

vltinject (1M)

NAME

`vltinject` – inject volumes into a robot for a specified vault configuration

SYNOPSIS

`/usr/openv/netbackup/bin/vltinject` *profile* | *robot/vault/profile* `[-version]`

DESCRIPTION

`vltinject` injects volumes into a robot and updates the Media Manager volume database. It accomplishes this by running the `vmupdate` command, giving it the robot number, robot type, and robotic volume group from the vault configuration matching the specified profile.

If you create a directory named `/usr/openv/netbackup/logs/vault` with public-write access, `vltinject` will create a daily debug log called `log.DDMMYY` (where *DDMMYY* is the current date) file in this directory that can be used for troubleshooting. Public-write access is needed because not all executables that write to this file run as root.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

profile | *robot/vault/profile*

The name of a profile or a robot number, vault, and profile 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.

`-version`

Display the `vltinject` version and exit.

EXAMPLE

Example 1

To inject volumes that were vaulted by the Payroll profile and that have been returned from the offsite vault, the user would enter the following:

```
vltinject Payroll
```

Example 2

To inject volumes that were vaulted by the Weekly profile in the Finance vault and that have been returned from the offsite vault, the user would enter the following:

```
vltinject 8/Finance/Weekly
```

RETURN VALUES

```
0        The Volume Database was successfully updated.

not = 0  There was a problem updating the Volume 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 returned to the system is 252, and 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

`/usr/openv/netbackup/logs/vault/log.`*`mmddyy`*

vltoffsitemedia (1M)

NAME

`vltoffsitemedia` - list the offsite parameter values for a group of media, or change the offsite parameter value for a single media.

SYNOPSIS

```
/usr/openv/netbackup/bin/vltoffsitemedia -list [-W] [-vault
         vault_name] [-voldbhost host_name]

/usr/openv/netbackup/bin/vltoffsitemedia -change -m media_id
         [-voldbhost host_name] [-d media_description]
         [-vltname vault_name] [-vltsent date][-vltreturn date]
         [-vltslot slot_no] [-vltcid container_id] [-vltsession
         session_id]

/usr/openv/netbackup/bin/vltoffsitemedia -version
```

DESCRIPTION

Allows the user to change the vault-specific parameters of a given media. This allows the user to change one or more parameters using a single command. It allows the user to view the various vault parameters of all media for a particular volume database host or vault.

If you create a directory named:

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

`Windows: install_path\netbackup\logs\vault`

with public-write access, `vltoffsitemedia` will create a daily debug log called `log.DDMMYY` (where *DDMMYY* is the current date) file in this directory that can be used for troubleshooting. Public-write access is needed because not all executables that write to this file run as root.

OPTIONS

`-change`

Change 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 the vm.conf file. For more information about vm.conf file parameters, see the NetBackup Media Manager System Administrator's Guide.

`-list`

Lists the off-site parameters for the media in the local volume database. To restrict the list to a specific vault for the local volume database, include the -vault option with the command. To list the off-site parameters for media for a specific volume 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`

Name of the vault for which all media ids and their vault-specific parameters are to be listed.

`-version`

Display 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 volume database host to a container that has media from a different volume database host. Use the `-m` option to specify the media ID of the volume.

`-vltname vault_name`

Specifies the name of the logical vault 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 is the date that the media will be requested for return from the vault vendor.

The format of *date* depends on the user's locale setting. See the NOTES section for more information. For the C locale, the date syntax is as follows:

mm / *dd* / *yyyy* [*hh*[: *mm*[: *ss*]]]

`-vltsent` *date*

Specifies the date and time the media was sent to the offsite vault.

The format of *date* depends on the user's locale setting. See the NOTES section for more information. For the C locale, the date syntax is as follows:

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`
Name of the volume database host.

`-W`
Specifies 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 separated line of column labels; the output data lines are space separated fields.

EXAMPLES

Example 1

The following command will change the vault name and the vault sent dates of the media with the ID BYQ123:

```
vltoffsitemedia -change -m BYQ123 -vltname THISTLE -vltsent
08/01/2003 12:22:00
```

Example 2

The following command will change the vault slot number to 100 for a media with ID 000012:

```
vltoffsitemedia -change -m 000012 -vltslot 100
```

Example 3

The following command can be used to 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

To change the container ID and media description of volume ABC123:

```
vltoffsitemedia -change -m ABC123 -vltcid Container001 -d "Media
Added By Jack"
```

Example 5

To 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/update the volume database. If the `vltoffsitemedia` command fails, look at the debug log in the *install_path*\netbackup\logs\vault directory for detailed information about the actual Media Manager command that failed. Status codes returned by Media Manager commands are documented in Chapter 5 of the NetBackup *Troubleshooting Guide*, Media Manager Status Codes and Messages.

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 returned to the system is 252, and 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`.

NOTES

The format that you use for date and time option values varies according to your locale setting. The examples in this command description are for a locale setting of C.

For more information on locale, see the locale(1) man page for your system.

vltopmenu (1M)

NAME

`vltopmenu` - Start the NetBackup Vault menu interface for operators

SYNOPSIS

```
/usr/openv/netbackup/bin/vltopmenu [-version]
```

DESCRIPTION

Allows the user to invoke a menu screen containing the various options that an Operator of the NetBackup Vault feature can use. It allows the user to eject or inject media, print various reports individually or collectively, as well as consolidate all reports and ejects for all sessions which have not yet ejected media. This interface can be used from any character-based terminal (or terminal emulation window) for which the user has a termcap or terminfo definition.

See the NetBackup *Operator's Guide* for detailed operating instructions.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide*.

OPTIONS

`-version`
: Display the vltopmenu 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 returned to the system is 252, and 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

`/usr/openv/netbackup/vault/sessions/vlteject.mstr`

`/usr/openv/netbackup/vault/sessions/vlteject_status.log.`*`timestamp`*

`/usr/openv/netbackup/vault/sessions/*/sid*/detail.log`

vltrun(1M)

NAME

`vltrun` - Run a NetBackup Vault session

SYNOPSIS

```
/usr/openv/netbackup/bin/vltrun profile | robot/vault/profile
        [-preview] [-verbose|-v] [-version] [-help]
```

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`*
: 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.

`-preview`
: Generate 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`
: Report verbosely on the session in the vault debug log.

`-version`
: Display the vltrun version and exit.

`-help`
: Displays a synopsis of command usage when it is the only option on the command line.

USAGE

The `vltrun` session follows this sequence:

- Run the `vlt_start_notify` script
- Inventory media
- Initialize Media Manager database for vault media 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
- Backup 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 GUI 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 created by vltrun and the vault engine during the session.

The vault session directory is `/usr/openv/netbackup/vault/sessions/`*`vault_name`*`/sid`*`xxx`* where *xxx* 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 will be sent to this address at the end of the session, reporting the results. By default, email is sent to root.

`vltrun` produces an overview of the session, called `summary.log`, in the session directory.

You can control vault processing 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 *System 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:

- Choosing Images
- Duplicating Images
- Choosing Media
- Catalog Backup
- Eject and Report
- Done

If you create a directory named `/usr/openv/netbackup/logs/vault` with public-write access, `vltrun` will create a daily debug log called `log.DDMMYY` (where *DDMMYY* is the current date) file in this directory that can be used for troubleshooting. Public-write access is needed because not all executables that write to this file run as root.

You can adjust the level of logging information provided in this log file by adjusting the vault logging level parameter on the **Logging** page of the master server's properties via **Host Properties** on the NetBackup Console.

You must have root privileges on the master server to execute this command.

EXAMPLES

Example 1

To vault the profile my_profile, enter:

```
vltrun my_profile
```

Example 2

The following command vaults the images for robot 0, vault Financials, and profile Weekly:

```
vltrun 0/Financials/Weekly
```

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 returned to the system is 252, and 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

`/usr/openv/netbackup/vault`

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

`/usr/openv/netbackup/logs/bpbrmvlt/log.`*`mmddyy`*

`/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`*`/sid`*`xxx`*

`/usr/openv/netbackup/vault/sessions/`*`vault_name`*`/sid`*`xxx`*`/summary.log`

`/usr/openv/netbackup/vault/sessions/`*`vault_name`*`/sid`*`xxx`*`/detail.log`

SEE ALSO

`vltadm(1M)`, `vlteject(1M)`, `vltinject(1M)`, `vltoffsitemedia(1M)`, `vltopmenu(1M)`

vmadd(1M)

NAME

vmadd - Add volumes to the volume database

SYNOPSIS

```
/usr/openv/volmgr/bin/vmadd -m media_id -mt media_type [-h
        volume_database_host] [-verbose] [-b barcode] [-rt
        robot_type] [-rn robot_number] [-rh robot_host] [-rc1
        rob_slot] [-rc2 rob_side] [-p pool_number] [-mm max_mounts
        | -n cleanings] [-op optical_partner] [-d "media_description"]
```

DESCRIPTION

Add volumes to the Media Manager volume database.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide* or the *NetBackup Media Manager System Administrator's 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 following applies only to NetBackup Enterprise Server:

If you are adding an optical disk, specify the media ID for the A side of the optical platter. Media IDs for an API robot type (ACS, TLH, TLM, LMF, or RSM) must always match the barcodes.

The following applies only to NetBackup Server:

Media IDs for an RSM robot must always match the barcodes.

`-mt` *media_type*

Specifies the media type of the volume to add.

Valid media types for NetBackup Enterprise Server follow:

4mm, 8mm, 8mm2, 8mm3, dlt, dlt2, dlt3, dtf, hcart, hcart2, hcart3, odiskwm, odiskwo, 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.

`-h` *volume_database_host*

This option is only applicable for NetBackup Enterprise Server.

Name of the host with the volume database where the volume will be added. You should ensure that the host specified matches the volume database host name associated with the robot or set of standalone drives, as indicated in the device configuration. If no host is specified, the host where you execute the command is default.

`-verbose`

Selects verbose mode.

`-b` *barcode*

Specifies the barcode 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 follow:

none, acs, lmf, odl, rsm, tl4, tl8, tld, tlh, tlm, ts8, tsd, tsh.

Valid robot types for NetBackup Server follow:

none, rsm, tl4, tl8, tld, ts8, tsd.

`-rn` *robot_number*

Unique, logical identification number for the robot where the volume is located.

`-rh` *robot_host*

Name of the host which controls the robot, where the volume is located.

`-rc1` *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.

The following applies only to NetBackup Server:

Do not enter slot information for Media Manager RSM robot types. The robot software tracks the slot locations for these robots.

`-rc2` *rob_side*

This option is only applicable for NetBackup Enterprise Server.

Robot coordinate 2 is the platter side for optical disks (A or B).

`-p` *pool_number*

Index of the volume pool which will contain this volume. You can use `vmpool -listall` to determine the index for a given pool name.

`-mm` *max_mounts*
: Maximum number of mounts 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*
: Number of cleanings remaining for this volume. Only used for cleaning media.

`-op` *optical_partner*
: *This option is only applicable for NetBackup Enterprise Server.*

  If this is an optical disk, specify the media ID of the opposite side of the optical platter.

`-d "`*media_description*`"`
: Media description of the volume. The double quote marks are required if the description contains any spaces.

EXAMPLES

The following command adds volume AJU244 in the NetBackup volume pool to the volume database on the host named llama.

The volume, with a barcode of AJU244, 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:

There is only one host (the master), 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

`vmchange(1M), vmdelete(1M), vmpool(1M), vmquery(1M)`

vmadm(1M)

NAME

vmadm - character-based media management utility

SYNOPSIS

```
/usr/openv/volmgr/bin/vmadm [-l] [-t]
```

DESCRIPTION

`vmadm` can be used to manage volumes and volume pools, manage barcode rules, and inventory robots controlled by the Media Manager volume daemon (`vmd`). Any actions performed using this utility are serviced by making requests to `vmd`. You must have root privileges to execute this utility.

This utility has a character-based user interface and can be used from any terminal. When this utility is initiated, the administrator is presented with a menu of operations that can be performed.

You can also start the `tpconfig` utility from `vmadm`.

OPTIONS

`-l`
: Requests that the Media Manager volume daemon log the current status. If `vmd` can handle the request; no output is visible, but log messages are written to the debug log (if the log is enabled).

`-t`
: Terminates the Media Manager volume daemon.

ERRORS

If `vmd` is not running, most `vmadm` operations fail and the following message appears:

```
unable to validate server: cannot connect to vmd (70)
```

See `vmd(1M)` to obtain additional debugging information should problems persist.

FILES

`/usr/openv/volmgr/help/vmadm*` (these are help files)

`/usr/openv/volmgr/database/volDB`

SEE ALSO

`ltid(1M), tpconfig(1M), vmd(1M)`

vmchange(1M)

NAME

vmchange - change media information in the Media Manager volume database

SYNOPSIS

Change volume group residence

```
/usr/openv/volmgr/bin/vmchange [-h volume_database_host] -vg_res
        -rt robot_type -rn robot_number -rh robot_control_host -v
        volume_group
```

Change volume residence

```
/usr/openv/volmgr/bin/vmchange [-h 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 [-rc2
        rob_side]
```

Change volume expiration date

```
/usr/openv/volmgr/bin/vmchange [-h volume_database_host] -exp date
        -m media_id
```

Change the barcode for a volume

```
/usr/openv/volmgr/bin/vmchange [-h volume_database_host] -barcode
        barcode -m media_id [-rt robot_type]
```

Change the container ID for a volume by media ID

```
/usr/openv/volmgr/bin/vmchange [-h volume_database_host] -m
        media_id -vltcid vault_container_id
```

Change the container ID for a volume by bar code

```
/usr/openv/volmgr/bin/vmchange [-h volume_database_host]
        -barcode barcode -vltcid vault_container_id
```

Change the media description for a volume

```
/usr/openv/volmgr/bin/vmchange [-h volume_database_host] -d
        "media_description" -m media_id
```

Associate this volume with a different pool

```
/usr/openv/volmgr/bin/vmchange [-h volume_database_host] -p
        pool_number -m media_id
```

Change a volume's maximum mount count

```
/usr/openv/volmgr/bin/vmchange [-h volume_database_host]
        -maxmounts max_mounts -m media_id
```

Change a volume's number of mounts count or cleanings

```
/usr/openv/volmgr/bin/vmchange [-h volume_database_host] -n
        num_mounts/cleanings -m media_id
```

Change a volume's media type

```
/usr/openv/volmgr/bin/vmchange [-h volume_database_host] -new_mt
        media_type -m media_id
```

Change a volume's robot type

```
/usr/openv/volmgr/bin/vmchange [-h volume_database_host] -new_rt
        robot_type -m media_id -rn robot_number
```

Change a volume's group

```
/usr/openv/volmgr/bin/vmchange [-h volume_database_host] -new_v
        volume_group [-m media_id |{-b barcode -mt media_type -rt
        robot_type}]
```

Change a volume's vault name

```
/usr/openv/volmgr/bin/vmchange [-h volume_database_host] -vltname
        vault_name -m media_id
```

Change the date the volume was sent to the vault

```
/usr/openv/volmgr/bin/vmchange [-h volume_database_host] -vltsent
        date -m media_id
```

Change the date when the volume returns from the vault

```
/usr/openv/volmgr/bin/vmchange [-h volume_database_host]
        -vltreturn date -m media_id
```

Change a volume's vault slot number

```
/usr/openv/volmgr/bin/vmchange [-h volume_database_host] -vltslot
        vault_slot -m media_id
```

Change the volume's vault session id

```
/usr/openv/volmgr/bin/vmchange [-h volume_database_host]
        -vltsession vault_session_id -m media_id
```

Move (eject) volumes from an ACS, TLH, or TLM robot to standalone

```
/usr/openv/volmgr/bin/vmchange -api_eject -map
        map_id:mapid:...:mapid | any -w [-h volume_database_host] -res
        -ml media_id:media_id: ...:media_id -rt robot_type -rn
        robot_number -rh robot_host [-v volume_group]
```

Move (eject) multiple volumes from a TL8 or TLD robot to standalone

```
/usr/openv/volmgr/bin/vmchange -multi_eject -w [-h
        volume_database_host] -res -ml media_id:media_id: ...:media_id
        -rt robot_type -verbose -rn robot_number -rh
        robot_control_host
```

Move (inject) multiple volumes into a TL8 or TLD robot

```
/usr/openv/volmgr/bin/vmchange -multi_inject -w -res -rt
        robot_type -verbose -rn robot_number -rh robot_control_host
```

Get robot information for a TL8 or TLD robot type

```
/usr/openv/volmgr/bin/vmchange -res -robot_info -verbose -rn
        robot_number -rt robot_type -rh robot_control_host
```

DESCRIPTION

Change volume information in the Media Manager volume database.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide* or the *NetBackup Media Manager System Administrator's Guide*.

OPTIONS

`-h` *volume_database_host*

This option is only applicable for NetBackup Enterprise Server.

Name of the host that has the volume database which keeps information about the media in robots and standalone drives. If no host is specified, the host where you execute the command is default.

`-vg_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, lmf, odl, rsm, tl4, tl8, tld, tlh, tlm, ts8, tsd, tsh.

Valid robot types for NetBackup Server follow:

none, rsm, tl4, tl8, tld, ts8, tsd.

`-rn` *robot_number*

Unique, logical identification number for the robot where the volume is located.

`-rh` *robot_control_host*

Name of the host which 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`

Change 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, dtf, hcart, hcart2, hcart3, odiskwm, odiskwo, 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.

`-rc1` *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 API robot types. The robot software tracks the slot locations for these robots.

The following applies only to NetBackup Server:

Do not enter slot information for RSM robot types. The robot software tracks the slot locations for these robots.

`-rc2` *rob_side*

This option is only applicable for NetBackup Enterprise Server.

Robot coordinate 2 is the platter side for optical disks (A or B).

`-exp` *date*

Expiration date for this volume.

The format of *date* depends on the user's locale setting. See the NOTES section for more information. For the C locale, the date syntax is as follows:

mm/*dd*/*yyyy* [*hh*[: *mm*[: *ss*]]]

`-barcode` *barcode*
Specifies the barcode 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 which will contain this volume. You can get the pool index using `vmpool -listall`.

`-maxmounts` *max_mounts*
Maximum number of mounts allowed for this volume. Only used for non-cleaning media.

`-n` *num_mounts/cleanings*
For non-cleaning media, *num_mounts* is the number of times this volume has been mounted.

For cleaning media, *cleanings* is the number of cleanings left 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 attached to the volume.

`-vltcid` *`vault_container_id`*
Change 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 configured for the robot that ejected the volume.

`-vltsent` *date*
Specifies the date the volume was sent offsite.

The format of *date* depends on the user's locale setting. See the NOTES section for more information. 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 is the date that the volume will be requested for return from the vault vendor.

The format of *date* depends on the user's locale setting. See the NOTES section for more information. For the C locale, the date syntax is as follows:

mm/*dd*/*yyyy* [*hh*[:*mm*[:*ss*]]]

`-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, TLH, or TLM volumes from the specified robot. For ACS and TLM robots, the ejection timeoout period is one week. For TLH robots, the robot allows an unlimited period to remove media.

`-map` *map_id:mapid: ...:mapid | any*

For ACS robots, this command 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 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 specified using a nearest MAP algorithm. The algorithm assumes that the LSMs are connected in a line; if your LSMs are connected in a configuration other than a line, see Adjacent LSM Specification for ACS Robots and Media Access Port Default for ACS Robots in the *NetBackup Media Manager System Administrator's Guide*.

For TLM robots, use map_id "ANY" to eject to the MAP configured for each media type on the DAS/SDLL server.

For TLH robots, select the "standard" MAP or the "BULK" MAP, depending on the library's hardware configuration.

`-w`

Wait flag. This flag must be used with the eject, multiple eject, and multiple inject commands.

`-verbose`

Selects verbose mode.

`-ml` *media_id:media_id: ...:media_id*

Specifies a list of media to be ejected from the robot.

`-multi_eject`
This option is valid only for TL8 and TLD robot types. Use the robotic library's media access port to eject multiple volumes. The ejection timeout period is 30 minutes.

`-multi_inject`
This option is valid only for TL8 and TLD robot types. Used the robotic library's media access port to inject multiple volumes.

`-robot_info`
Used to retrieve information about a robotic library. This option is valid only for TLD and TL8 robot types

CAUTIONS

Some robotic libraries implement different functionality for their media access ports. For example, some libraries have front-panel inject and 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 using the media access port (for example, Spectra Logic Gator).

If you are using an eject option and the media is not removed and a time-out condition occurs, the media is returned to (injected into) the robot. If this occurs, you should inventory the robot and then eject the media that was returned to the robot.

Make sure you read the operator manual for your robotic library to gain an understanding of its media access port functionality. Libraries such as the ones noted may not be fully compatible with NetBackup's inject and eject features if not properly handled. Other libraries may not be compatible at all. In addition, VERITAS performs limited validation of these option parameters.

EXAMPLES

Example 1

The following command changes the expiration date of volume AJS100:

```
vmchange -exp 12/31/99 23:59:59 -m AJS100
```

Example 2

The following command changes the pool (which contains volume AJS999) to pool 1 (which is the NetBackup pool):

```
vmchange -h dill -p 1 -m AJS999
```

Example 3

The following command ejects 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

The following command changes the container ID of volume ABC123:

```
vmchange -vltcid Container001 -m ABC123
```

NOTES

The format that you use for date and time option values varies according to your locale setting. The examples in this command description are for a locale setting of C.

For more information on locale, see the locale(1) man page for your system.

SEE ALSO

vmadd(1M), vmdelete(1M), vmpool(1M), vmquery(1M)

vmcheckxxx(1M)

NAME

vmcheckxxx - Report the media contents of a robotic library

SYNOPSIS

```
/usr/openv/volmgr/bin/vmcheckxxx -rt robot_type -rn robot_number
        [-rh robot_host] [-h volume_database_host] [[-if
        inventory_filter_value] [-if inventory_filter_value] ...] [-full]
        [-list]
```

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.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide* or the *NetBackup Media Manager System Administrator's Guide*.

OPTIONS

`-rt` *robot_type*

Specifies the robot type of the robot to inventory.

Valid robot types for NetBackup Enterprise Server follow:

none, acs, lmf, odl, rsm, tl4, tl8, tld, tlh, tlm, ts8, tsd, tsh.

Valid robot types for NetBackup Server follow:

none, rsm, tl4, tl8, tld, ts8, tsd.

`-rn` *robot_number*

Unique, logical identification number of the robot to inventory.

`-rh` *robot_host*

Name of the host which controls the robot. If no host is specified, the host where you execute this command is assumed.

`-h` *volume_database_host*

This option is only applicable for NetBackup Enterprise Server.

Name of the host that has the volume database which contains information about the volumes in a robot. If no host is specified, the host where you execute this command is assumed.

`-if` *inventory_filter_value*

This option is only applicable for NetBackup Enterprise Server.

Specifies inventory filter values. Multiple `-if` options may be specified. The inventory filter value is an ACS scratch pool ID, a TLH volume category, or an LMF barcode prefix.

The `-if` and `-full` options cannot be specified together.

`-full`

Specifies 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

The following command lists the media contents of TLD robot 1 and the volume configuration for that robot on the host named niagra, along with a list of any mismatches that are detected:

```
vmcheckxxx -rt tld -rn 1 -rh niagra -h niagra
```

The following command lists the contents of TLH robot 2 that is connected to the host where the vmcheckxxx command was executed:

```
vmcheckxxx -rt tlh -rn 2 -list
```

SEE ALSO

`vmupdate(1M)`

vmd(1M)

NAME

vmd - Media Manager volume daemon

SYNOPSIS

```
/usr/openv/volmgr/bin/vmd [-v]
```

DESCRIPTION

vmd manages the volume database, responding to requests to add, change, list, or delete volumes. By maintaining the location of media, vmd allows volumes to be removed and recognized by Media Manager. vmd is used with the Media Manager device daemon (ltid) to determine the location of requested volumes and keep track of the number of mounts and last mount time. vmd is initiated by ltid, but remains running when ltid is terminated using stopltid.

ltid does not require volumes to be defined in the volume database before being used.

The following paragraph applies only to NetBackup Enterprise Server:

Automatic mounting of volumes in robotic devices does not take place until volumes are defined and their slot information (for non API robots) is entered in the volume database.

A direct interface to the volume database is provided to easily facilitate volume database administrative activities. 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 global device databases.

The Internet service port number for vmd must be in /etc/services. If you are using NIS (Network Information Service), the entry found in this host's /etc/services file should be placed in the master NIS server database for services. To override the services file, create the file /usr/openv/volmgr/database/ports/vmd with a single line containing the service port number for vmd. The default service port number is 13701.

The following paragraphs apply only to NetBackup Enterprise Server:

In addition vmd is the device allocator (DA) for shared drives. vmd/DA maintains shared drive and host information, such as a list of hosts that are registered to share a drive and which host currently has the drive reserved.

Shared drive information is modified only by requests from ltid. When ltid initializes on a device host, it calls vmd/DA with a list of shared drives. vmd/DA adds these drives and the host name to its configuration, if necessary. Since ltid passes a complete list of

drives each time, vmd/DA deletes references to drives for that host when a change in configuration removes them from that host's shared drive list. This deletion occurs when ltid shuts down gracefully or after it is restarted.

OPTIONS

-v

Logs detailed 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 running.

vmd logs an error message using syslogd, if the port that it binds to is in use. If this occurs, it may be necessary to override the services file using the mechanism described under DESCRIPTION.

To run vmd in debug mode do the following:

1. Before starting vmd, create the following directory:

   /usr/openv/volmgr/debug/daemon

   If vmd is running, stop and restart it after creating the directory.

2. Start vmd in verbose mode as follows or put a VERBOSE entry in vm.conf.

   /usr/openv/volmgr/bin/vmd -v

3. Check the log 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. Running vmd in debug mode should be done only when necessary.

FILES

/usr/openv/volmgr/database/volDB

/usr/openv/volmgr/database/poolDB

/usr/openv/volmgr/database/ruleDB

/usr/openv/volmgr/database/globDB

/usr/openv/volmgr/debug/daemon/*

/usr/openv/volmgr/debug/reqlib/*

SEE ALSO

ltid(1M), vmadm(1M), vmadd(1M), vmchange(1M), vmdelete(1M), vmquery(1M)

vmdb_merge(1M)

NAME

vmdb_merge - Merges NetBackup volume databases and updates associated configuration files

SYNOPSIS

```
/usr/openv/volmgr/bin/vmdb_merge [-preview | -merge] -target
         target volume database hostname -source source volume
         database hostname [-cache_block_size number of
         records] [-no_standalone] [-time] [-status_file merge
         status output filename] [-verbose]
```

DESCRIPTION

Merges NetBackup Media Manager volume databases, pool databases and media databases. In the usage statements above, the Media and Device Management (MDM) Domain Server is the target. Before merging volume domains, the user should have already merged the corresponding device domains - that is, all affected hosts should have the same global database host. Therefore, vmdb_merge will insist that the target volume database host is also the global device database host.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the NetBackup System Administrator's Guide or the NetBackup Media Manager System Administrator's Guide.

Caution: Merging volume databases always involves some risk. It is strongly recommended that the user have a rollback plan for this operation. This operation can also take a very long time, and should be done during NetBackup system quiet time. Running backups while this utility runs could create merge conflicts in the resulting database that are undetected by NetBackup, causing future backups and or restores to fail.

OPTIONS

`-preview (default)`
: Specifies that the user wishes only to preview any merge conflicts and their causes and not to alter any databases.

`-merge`
: Replicates all volumes in the source volume database host's database into the volume database host on the target. Updates device configurations for all robotic libraries that previously used the source host for a volume database host to now use the target as the volume database host. Merges all volume pools, based on their unique pool name, and updates all

merged volumes' pool ids to match the new pool databases pool id for that volume's pool name. Updates media database records' pool ids as necessary.

`-target`
: The name of the volume database host that will end up with the combined volume database.

`-source`
: The name of the volume database host that will no longer be a volume database host. Volumes in this host's volume database will be merged into the database on the host specified by target.

`-cache_block_size`
: The number of volumes to buffer from either server at a given time. This parameter can control the amount memory to use when performing a merge or a preview. Volumes from both databases are read in blocks and analyzed for conflicts as blocks, thus capping the amount of memory the utility needs regardless of the size of the database.

`-no_standalone`
: The utility may have trouble determining what media server standalone volumes belong to since there is no robot number to cross-reference in the global database. By specifying this option, the utility will not move any standalone volumes to the target volume database host.

`-time`
: Time the operations.

`-status_file`
: Name of file to redirect output to rather than sending output to standard out.

`-verbose`
: Specifying this option increases the amount of information you are given about merge conflicts, and in some cases, advises how to resolve them.

NOTES

Only limited validation of the option parameters is done.

All affected databases will be saved before they are altered with the extension .bak or .tpacbak. For more information on this use the `-recovery_instructions` option for this command.

Both the source volume domain and target volume domain should be in a quiet time while performing this function.

All hosts must be at the same version of NetBackup and all must be running NetBackup before this utility will attempt to merge databases.

The intent of this utility is to provide a way for users to centralize their NetBackup Media Manager databases. Having all NetBackup Media Manager databases centralized and merged is preferable to distributing media and device domains for one NetBackup Master Server. For more information see section, "NetBackup Media Manager Best Practices" in the *NetBackup Media Manager System Administrator's Guide*.

EXAMPLES

Example 1

The following command determines what merge conflicts exist between the volume database host "flash" and the Media and Device Management Domain Server "spain"

```
vmdb_merge -preview -source flash -target spain -verbose
```

Example 2

The following command merges volumes from volume database host "spain" into the Media and Device Management Domain Server "flash"

```
vmdb_merge -merge -verbose -time -target flash -source spain
```

Example 3

The following command will print a set of instructions on where to find database files that were saved prior to the merge command.

```
vmdb_merge -recovery_instructions
```

SEE ALSO

tpautoconf(1M)

vmdelete(1M)

NAME

vmdelete - Delete volumes from the volume database

SYNOPSIS

```
/usr/openv/volmgr/bin/vmdelete [-h volume_database_host] [-m
        media_id | -v volume_group]
```

DESCRIPTION

Delete volumes from the volume database.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide* or the *NetBackup Media Manager System Administrator's Guide*.

OPTIONS

`-h` *volume_database_host*

This option is only applicable for NetBackup Enterprise Server.

Name of the host that has the volume database which contains information about the volumes in a robot. If no host is specified, the host where you execute the command is 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

The following command deletes a single volume:

```
vmdelete -m AJS144
```

The following command deletes all volumes with the volume group name of DELETE_ME:

```
vmdelete -v DELETE_ME
```

SEE ALSO

`vmadd(1M), vmchange(1M), vmquery(1M)`

vmoprcmd(1M)

NAME

vmoprcmd - perform operator functions on drives

SYNOPSIS

```
/usr/openv/volmgr/bin/vmoprcmd [-h device_host] -down | -up |
          -upopr | -reset drive_index | -downbyname | -upbyname |
          -upoprbyname | -resetbyname drive_name |
          -crawlreleasebyname drive_name | -comment drive_index
          ["comment"] | -commentbyname drive_name ["comment"] |
          -assign drive_index mount_request_id | -assignbyname
          drive_name mount_request_id | -deny | -resubmit
          mount_request_id | -d [pr | ds | ad] | -help
```

DESCRIPTION

Perform operator functions on drives. The `-h` option is not required, but you must choose one and only one of the other options listed below.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide* or the *NetBackup Media Manager System Administrator's Guide*.

OPTIONS

`-h` *device_host*

Name of the device host where the drives are attached and configured. If no host option is specified, the device host where you execute the command is default.

The following point applies only to NetBackup Server:

The device host is the host where Media Manager is installed.

`-down` | `-up` | `-upopr` | `-reset` *drive_index*

`-down` Sets the drive to the DOWN state, if it is not assigned.

`-up` Sets the drive to UP in Automatic Volume Recognition (AVR) mode. This is the normal mode for all drives.

`-upopr` Sets the drive to UP 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 is up.

`-reset` Resets the specified drive, terminating the drive assignment and taking control away from the assigned user.

Caution Do not reset an assigned drive unless directed by site policy or the system administrator. Terminating an active job can destroy user data.

`-downbyname | -upbyname | -upoprbyname | -resetbyname` *drive_name*
: These options are similar to `-down`, `-up`, `-upopr`, and `-reset` respectively, except the drive is specified by the drive name instead of drive index.

`-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 is specified by the drive name instead of drive index.

`-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 is specified by the drive name instead of 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.

`-d [pr | ds | ad]`
: If none of the following optional display parameters are specified, all information is displayed.

  `pr` Display pending requests.

  `ds` Display the status of drives under control of Media Manager.

  `ad` Display additional status of drives under control of Media Manager.

`-help`
: Display the usage statement for this command.

`-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.

NOTES

Only limited validation of the option parameters is done.

tpconfig -d, tpconfig -l, and vmoprcmd may truncate long drive names. Please use tpconfig -dl to obtain the full drive name.

vmoprcmd may truncate drive names to 20 characters.

EXAMPLES

The following command sets the drive, with a drive index of 0, to UP mode:

```
vmoprcmd -up 0
```

The following command displays the drive status of all drives:

```
vmoprcmd -d ds
```

The following command displays pending requests and the drive status of all drives on the device host named crab:

```
vmoprcmd -h crab
```

SEE ALSO

`tpconfig(1M)`

vmphyinv(1M)

NAME

vmphyinv - Physically inventory the media contents of a robotic library or standalone drive and update the volume database.

SYNOPSIS

```
/usr/openv/volmgr/bin/vmphyinv -rn robot_number] [-rh
         robot_control_host] [-h device_host]

[-pn pool_name] [-v volume_group] [-rc1 robot_coord1 -number
         number]

[-drv_cnt count] [-non_interactive] [-mount_timeout timeout]
         [-verbose]

install_path/volmgr/bin/vmphyinv -rn robot_number] [-rh
         robot_control_host] [-h device_host]

-ml media_id:media_id:...:media_id [-drv_cnt count]

[-non_interactive] [-mount_timeout timeout] [-verbose]

install_path/volmgr/bin/vmphyinv -rn robot_number] [-rh
         robot_control_host] [-h device_host]

[

{ { [-slot_range from to] [-slot_list s1:s2:...:sN] } -d
         density }

{ { [-slot_range from to] [-slot_list s1:s2:...:sN] } -d
         density }

]

[-drv_cnt count] [-non_interactive] [-mount_timeout timeout]
         [-verbose]


install_path/volmgr/bin/vmphyinv {-u drive_number | -n
         drive_name} [-h device_host]

[-non_interactive] [-mount_timeout timeout] [-verbose]
```

DESCRIPTION

Physically inventory the media contents of a robotic library or standalone drive and update the volume database. vmphyinv mounts each media specified by the search criterion, reads the tape header, and updates the volume database based on the information obtained from the tape header. For more information about this command, refer to the NetBackup Media Manager systems administrator's guide.

This command can be executed by authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide* or the *NetBackup Media Manager System Administrator's Guide*.

OPTIONS

`-rn robot_number`
: Specifies the Media Manager robot number whose media will be inventoried. robot_number should correspond to a robot which has drives that have already been configured. vmphyinv inventories each of the media, having 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 hostname`
: Specifies the device host name. This option is used to obtain the global device database host name. If not specified, the current host is used to obtain the global device host name.

`-pn pool_name`
: Specifies the case-sensitive pool name of the volumes, corresponding to robot specified by the -rn option, which need to be inventoried. Valid only when the -rn option is specified.

`-v volume_group`
: Specifies the volume group of the volmes, corresponding to robot specified by the -rn option, which need to be inventoried. Valid only when the -rn option is specified.

`-rc1 robot_coord1`
: Specifies the starting slot of the media which needs to be inventoried. Valid only when the -rn option is specified.

`-number number`
: Specifies the number of slots starting from robot_coord1 which need to be inventoried. Valid only when -rn and -rc1 are also specified.

`-ml media_id1:media_id2: … :media_idN`
Specifies a list of media, which need to be inventoried. Valid only when -rn option is specified. If the media ID specified does not belong to the specified robot, the media will be 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 while inventorying the media by slot range/list.

`-u device_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 Manager device configuration.

`-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 Manager device configuration.

`-non_interactive`
vmphyinv, in the default mode displays a list of recommendation and ask for confirmation before modifying volume database and NetBackup media database (if required). If this option is specified, the changes are applied without any confirmation.

`-mount_timeout`
Specifies the mount timeout in seconds. If the media cannot be mounted within the time specified, the mount request is cancelled. The default value is 15 minutes.

`-drv_cnt`
Specifies the maximum number of drives that can be used simultaneously by vmphyinv. The actual number of drives used by vmphyinv is determined by the total number of drives configured and this value. The number of drives used by vmphyinv is the minimum of the drive count specified and the total number of drives configured. The default is to use all the drives.

`-verbose`

Selects the verbose mode. When specified, more information (for example, the number of available drives, what is found on each tape, and catalog identification if the media is a catalog) is displayed to the caller. For more information about this option and the output it produces, refer to the *NetBackup Media Manager System Administrator's Guide*.

EXAMPLES

The following command updates the volume database of robot 1 connected to host shark:

```
vmphyinv -rn 1 -rh shark
```

The following command updates the volume database of robot 7 connected to host whale. Only the media belonging to the pool name "some_pool" will be inventoried:

```
vmphyinv -rn 7 -rh whale -pn some_pool
```

The following command updates the volume database of robot 3 connected to host dolphin. Only the media A00001, A00002, A00003 will be inventoried.

```
vmphyinv -rn 3 -rh dolphin -ml A00001:A00002:A00003
```

The following command updates the volume database of robot 2 of type TLD connected to host phantom. Only the media in slots 3 to 8 will be inventoried.

```
vmphyinv -rn 2 -rh phantom -slot_range 3 8 -d dlt
```

The following command updates the volume database of standalone drive (drive index 3) attached to host tigerfish:

```
vmphyinv -u 0 -h tigerfish
```

SEE ALSO

vmupdate`(1M)`, vmcheckxxx`(1M)`, vmoprcmd`(1M)`

vmpool(1M)

NAME

vmpool - Manage volume pools

SYNOPSIS

```
/usr/openv/volmgr/bin/vmpool [-h volume_database_host] -listall
        [-b] | -listscratch | -add pool_name "description" host uid
        gid | -change pool_name "description" host uid gid | -delete
        pool_name | -set_scratch pool_name | -unset_scratch
        pool_name
```

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, `-listscratch`).

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide* or the *NetBackup Media Manager System Administrator's Guide*.

OPTIONS

`-h` *volume_database_host*

This option is only applicable for NetBackup Enterprise Server.

Name of the host that has the volume database which keeps information about the media in a robot. If no host is specified, the host where you execute the command is default.

`-listall [-b]`

List information about all volume pools. You can use the `-b` option to specify a brief format for volume pool information.

`-listscratch`

List all configured scratch pools.

`-add` *pool_name* "*description*" *host uid gid*

Add a new volume pool.

`-change` *pool_name* "*description*" *host uid gid*

Change an existing volume pool.

`-delete` *pool_name*

Delete a volume pool.

"description"

Description of the volume pool. The double quote marks are required if the description contains any spaces.

host

Name of the host that will be permitted to request and use volumes in this volume pool.

The following applies only to NetBackup Enterprise Server:

To permit only a specific host to access the volume pool, enter the name of that host. To permit any host to access the volume pool, enter ANYHOST. Using the value ANYHOST is recommended.

The following applies only to NetBackup Server:

You can only specify the value ANYHOST.

uid

Specifies the user id of the user that is permitted to request and use volumes in the volume pool. Enter a specific user id to permit only processes running at that user id, to access the volume pool.

Enter the default value, -1 (ANY), to permit any user id to access the pool.

For a NetBackup or Storage Migrator volume pool, always enter the user id for root.

If you specify a specific user id and a different user id requests the pool, then Media Manager verifies the group id (see *gid*).

gid

Enter the group id of the group that is permitted to request and use volumes in this volume pool.

Enter a specific group id to permit only processes running as that group id, to access the volume pool.

Enter the default value, -2 (NONE), to permit only the user id specified by *uid* to request or access the volume pool.

`-set_scratch` *pool_name*

If *pool_name* is a previously defined volume pool, *pool_name* will become the scratch pool and its description will not be changed. The NetBackup, DataStore, and None volume pools cannot be changed to scratch pools.

If *pool_name* is a new volume pool, a new pool will be 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 using `vmpool -delete` *pool_name*.

NOTES

Only limited validation of the option parameters is done.

uid and *gid* should only be used for restricting access to volumes by user or by group on UNIX hosts.

EXAMPLES

The following command adds a new pool named MyPool on the host named llama with the default host, user id, and group id permissions:

```
vmpool -h llama -add MyPool "my description with spaces" ANYHOST -1
-2
```

The following command lists all pools configured on the host where the command is executed:

```
vmpool -listall -b
```

vmquery(1M)

NAME

vmquery - Query the volume database, or assign and unassign volumes

SYNOPSIS

```
/usr/openv/volmgr/bin/vmquery [-h volume_database_host, ... -h
          volume_database_host] [-vltcid vault_container_id] [-W]
          [-b | -w] -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_host rob_slot rob_side | -assignbyid media_id media_type
          pool_number stat asg_time | -deassignbyid media_id
          pool_number stat
```

DESCRIPTION

Query the volume database for volume information. The `-h`, `-b`, and `-w` options are not required, but you must choose only one of the other (eleven) options.

The `-b` or `-w` option can be used in conjunction with any of the other eleven options, but the `-b` or `-w` options cannot be specified together.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide* or the *NetBackup Media Manager System Administrator's Guide*.

OPTIONS

`-h` *volume_database_host*

This option is only applicable for NetBackup Enterprise Server.

Name of the host that has the volume database maintaining information about the volumes in a robot. If no host is specified, the host where you execute the command is default. Up to 100 volume database hosts can be queried.

`-b`

Specifies the brief output format for volume information. This option can be used in conjunction with any of the other eleven options.

`-w`

Specifies the wide output format for volume information. This option includes additional information not shown by the `-b` option and can be used in conjunction with any of the other eleven options.

`-a`
Show all volumes.

`-m` *media_id*
Query volumes by media id. The media id is a maximum of 6 ASCII characters.

`-v` *volume_group*
Query 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*
Query volumes by robot number. A robot number is a unique, logical identification number for the robot where the volume is located.

`-rt` *robot_type*
Query volumes by the type of the robot where the volume is located.

Valid robot types for NetBackup Enterprise Server follow:

none, acs, lmf, odl, rsm, tl4, tl8, tld, tlh, tlm, ts8, tsd, tsh.

Valid robot types for NetBackup Server follow:

none, rsm, tl4, tl8, tld, ts8, tsd.

`-mt` *media_type*
Query volumes by media type.

Valid media types for NetBackup Enterprise Server follow:

4mm, 8mm, 8mm2, 8mm3, dlt, dlt2, dlt3, dtf, hcart, hcart2, hcart3, odiskwm, odiskwo, 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*
Query 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*
Query volumes by pool name.

`-res` *robot_type robot_number robot_host rob_slot rob_side*
Query volumes by residence.

robot_host
Name of the host which controls the robot, where the volume is located.

rob_slot

This is the slot number in the robot (robot coordinate 1) where the volume resides.

rob_side

This is the platter side (robot coordinate 2) for optical disks (A or B). If the volume is not an optical disk, specify zero for *rob_side*.

`-assignbyid` *media_id media_type pool_number stat asg_time*

Assign volume by media id, pool, and status.

stat

Status applies only to volumes that are assigned to NetBackup or Storage Migrator.

A status of 0 means the volume is assigned to NetBackup regular backups.

A status of 1 means the volume is assigned to NetBackup catalog backups.

A status of 2 means the volume is assigned to Storage Migrator.

A status of 3 means the volume is assigned to Storage Migrator for Microsoft Exchange or Storage Migrator for Windows 2000.

asg_time

Applies only to volumes assigned to NetBackup or Storage Migrator.

asg_time is the time when the volume was assigned and is the number of seconds since 00:00:00 UTC, January 1, 1970. *asg_time* was originally created using the time() call.

`-deassignbyid` *media_id pool_number stat*

Unassign volume by media id, pool, and status.

Caution Unassigning volumes may cause inconsistencies between the application media database and the volume database, leading to possible data loss. You *must* use a NetBackup application interface (for example, NetBackup Console) to expire the media after unassigning volumes.

`-vltcid` *`vault_container_id`*

List the volumes that are stored in the container. *`vault_container_id`* can be a string of up to 29 alphanumeric characters.

`-W`

Specifies parsable output format for volume information. The output data lines are space separated fields except: the MediaID field is padded to 6 characters by adding spaces to the end of the string, the MediaType field is padded to 8 characters by adding spaces to the end of the string, and 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

The following command lists all volume information, in brief format from the volume database on the host named llama:

```
vmquery -h llama -b -a
```

The following command assigns volume A23456, which is in pool 1 (NetBackup), and sets the status to 0 and the assign time to 12/31/98 15:50:22:

```
vmquery -assignbyid A23456 8mm 1 0 915141022
```

The following command unassigns volume A23456, which is in pool 1 (NetBackup), with a status of 0:

```
vmquery -deassignbyid A23456 1 0
```

SEE ALSO

`vmadd(1M), vmchange(1M), vmdelete(1M), vmpool(1M)`

vmrule(1M)

NAME

vmrule - Manage barcode rules

SYNOPSIS

`/usr/openv/volmgr/bin/vmrule [-h` *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*

DESCRIPTION

Use this command to add, change, delete, or list barcode rules. The `-h` option is not required, but you must chose one and only one of the other four options.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide* or the *NetBackup Media Manager System Administrator's Guide*.

OPTIONS

`-h` *volume_database_host*

This option is only applicable for NetBackup Enterprise Server.

Name of the host that has the volume database which contains information about the volumes in a robot. If no host is specified, the host where you execute the command is default.

`-listall [-b]`

List information about all barcode rules. You can use the `-b` option to specify a brief format for the barcode rule information that is displayed.

`-add` *barcode_tag media_type pool_name max_mounts "description"*

Add a new barcode rule.

`-change` *barcode_tag media_type pool_name max_mounts "description"*

Change a barcode rule.

`-delete` *barcode_tag*

Delete a barcode rule.

barcode_tag

Specifies the barcode prefix which will invoke the barcode rule.

media_type

Specifies the media type of the volume, a barcode rule attribute. This affects whether the rule will be used and also affects the media type for volumes added using a robot inventory update.

Valid media types for NetBackup Enterprise Server follow:

4mm, 8mm, 8mm2, 8mm3, dlt, dlt2, dlt3, dtf, hcart, hcart2, hcart3, odiskwm, odiskwo, 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 will be added.

max_mounts

Maximum number of mounts 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.

"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

The following command creates a rule that defines any tape with a barcode starting 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"
```

SEE ALSO

`vmupdate(1M)`

vmupdate(1M)

NAME

vmupdate - Inventory the media contents of a robotic library and update the volume database

SYNOPSIS

```
/usr/openv/volmgr/bin/vmupdate -rt robot_type -rn robot_number [-rh
        robot_host] [-h volume_database_host] [[-if
        inventory_filter_value] [-if inventory_filter_value] ...] [-full]
        [-recommend] [-interactive] [-involgrp volume_group]
        [-outvolgrp volume_group] [-mt media_type] [-p pool_name]
        [-use_barcode_rules] [-use_seed] [-mp media_id_prefix]
        [-no_sides] [-no_format_optical] [-overwrite_labels]
        [-empty_map]
```

DESCRIPTION

Inventory the media contents of a robotic library and update the volume database. If no options are specified, the volume configuration is updated to match the robot contents.

This command can be executed by any authorized users. For more information about NetBackup authorization, refer to "Enhanced Authorization and Authentication" in the *NetBackup System Administrator's Guide* or the *NetBackup Media Manager System Administrator's Guide*.

OPTIONS

`-rt` *robot_type*

Specifies the robot type of the robot to inventory.

Valid robot types for NetBackup Enterprise Server follow:

none, acs, lmf, odl, rsm, tl4, tl8, tld, tlh, tlm, ts8, tsd, tsh.

Valid robot types for NetBackup Server follow:

none, rsm, tl4, tl8, tld, ts8, tsd.

`-rn` *robot_number*

Unique, logical identification number for the robot to inventory.

`-rh` *robot_host*

Name of the host which controls the robot. If no host is specified, the host where you execute this command is assumed.

`-h` *volume_database_host*

This option is only applicable for NetBackup Enterprise Server.

Name of the host that has the volume database which contains information about the volumes in a robot. If no host is specified, the host where you execute this command is assumed.

`-if` *inventory_filter_value*

This option is only applicable for NetBackup Enterprise Server.

Specifies inventory filter values. Multiple `-if` options may be specified. The inventory filter value is an ACS scratch pool ID, a TLH volume category, or an LMF barcode prefix.

The `-if` and `-full` options cannot be specified together.

`-full`

Specifies full inventory. The `-full` and `-if` options cannot be specified together.

`-recommend`

Lists changes required to update the volume configuration.

`-interactive`

Prompts you before updating the volume configuration.

`-involgrp` *volume_group*

Specifies the volume group for media moved into the robot.

`-outvolgrp` *volume_group*

Specifies the volume group for media moved out of the robot.

`-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, dtf, hcart, hcart2, hcart3, odiskwm, odiskwo, 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_name*

Specifies the name of the volume pool to which new media will be assigned.

`-use_barcode_rules`

Specifies that barcode rules will be used for assigning attributes to new media.

`-use_seed`

Specifies automatic generation of media IDs for media with no barcodes.

`-mp` *media_id_prefix*
: Specifies the prefix that is used as a seed to generate new media IDs for media with no barcodes.

`-no_sides`
: Specifies that any new optical media IDs will not always contain platter side A or B.

`-no_format_optical`
: Specifies to NOT format new optical media.

`-overwrite_labels`
: Specifies that existing labels will be overwritten when formatting optical media.

`-empty_map`
: Specifies that volumes in the media access port (map) will be moved into the robot before the robot inventory is started. This option is only valid for TL8, TLD, or TLM robot types.

NOTES

Only limited validation of the option parameters is done.

EXAMPLES

The following command updates the volume configuration on the host 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

`vmcheckxxx(1M)`

vopie_util(1M)

NAME

`vopie_util` - Manage local vopie authentication files

SYNOPSIS

```
/usr/openv/bin/vopie_util [-log_dir path] [-severity mask]
        [-debug] [-local_name name] [-always_write] [-hashed |
        -unhashed] remote_name [sequence seed hash]
```

DESCRIPTION

The `vopie_util` program is available on Windows and UNIX NetBackup servers and clients. It updates the hashed (public) and unhashed (secret) key files for the vopie authentication method on the local system. Typically, `vopie_util` is used to synchronize the vopie key files between two systems.

OPTIONS

`-log_dir` *path*

Specifies the directory where the `vopie_util` log directory resides. The default is:

install_path`\NetBackup\logs` (Windows)

`/usr/openv/logs` (UNIX)

To enable logging, create a `vopie_util` directory in the *path* directory before starting `vopie_util`. For example:

`/usr/openv/logs/vopie_util`

`-severity` *mask*

Specifies the type of messages to be logged. *mask* is the sum of zero or more of these values:

`1` Unknown

`2` Debug

`4` Information

`8` Warning

`16` Error

32 Critical

The default is 48 decimal (0x30 hexadecimal or 060 octal), which specifies critical and error.

`-debug`

Specifies that additional information is logged to standard error.

`-local_name` *name*
: Specifies the name of the local system. The default is the network host name of the system. We recommend that this name match the NetBackup client name for the system.

`-always_write`
: Always update the file even if it already exists. The default is to not overwrite existing files.

`-hashed`
: Updates the hashed (public) key file. This file contains the challenges that this system presents to other systems during authentication. If the *sequence, seed,* and *hash* options described below are not specified, the hashed-key file data matches any secret key.

`-unhashed`
: Updates the unhashed (secret) key file. A secret key is randomly generated and written to the unhashed key file. The unhashed file contains the responses that the system returns when challenged by another system.

  The corresponding hashed-key file data is displayed after running the command with this option.

remote_name
: Specifies the name of the remote system with which this one is being synchonized.

sequence seed hash
: Can be used with the `-hashed` option and specifies data that is written in the hashed (public) key file:

  sequence is a decimal number between 10 and 499.

  seed is a 6 to 20 character string.

  hash is a 16 digit hexadecimal number.

EXAMPLES

Example 1

In this example, the vopie key files are set up so the first connection between systems red and blue is not fully authenticated. After the connection, the key files are updated so full authentication is required. This is the easiest way to synchronize the key files but it leaves a small window of insecurity.

1. On system red:

   a. Create a secret key file on red by running the following command:

   ```
   vopie_util -local_name red -unhashed blue
   ```

The public key (hashed) file information for red is displayed:

```
red 0167 jp0167 0aa47eae2d86231d
```

This information can be ignored in this example.

b. Create a public key file on red that will match any secret key on blue:

```
vopie_util -local_name red -hashed blue
```

2. On system blue:

a. Create a secret-key file on blue by running the following command:

```
vopie_util -local_name blue -unhashed red
```

The public key (hashed) file information for blue is displayed:

```
blue 0431 gw3251 0aa47eae2d86231d
```

This information can be ignored in this example.

b. Create a public key file on blue that will match any secret key on red by running the following command:

```
vopie_util -local_name blue -hashed red
```

Example 2

In this example, the vopie key files on systems green and yellow are synchronized. Full authentication is required immediately. This is a more secure method than in example 1.

1. On system green, create a secret key file on green by running the following command:

```
vopie_util -local_name green -unhashed yellow
```

The public key (hashed) file information for green is displayed:

```
green 0209 fz9365 f852019bde05e92f
```

yellow uses this key when it issues challenges.

2. On system yellow:

a. Create a public key file on yellow that matches the secret key file on green by running the following (all on one line):

```
vopie_util -local_name yellow -hashed green 0209 fz9365
f852019bde05e92f
```

b. Create a secret key file on yellow by running the following by command:

```
vopie_util -local_name yellow -unhashed green
```

The public key (hashed) file information for yellow is displayed:

```
yellow 0468 yq0860 82723984b43bf474
```

green uses this key when it issues challenges.

3. On system green, create a public key file on green that matches the secret key file on yellow by running the following (all on one line):

```
vopie_util -local_name green -hashed yellow 0468 yq0860
82723984b43bf474
```

SEE ALSO

bpauthsync(1M),vopied(1M)

vopied(1M)

NAME

`vopied` - Daemon to provide VERITAS One-time Password user authentication

SYNOPSIS

```
/usr/openv/bin/vopied [-standalone] [-debug] [-portnum number]
          [-max_time seconds] [-log_dir path] [-severity mask]
```

DESCRIPTION

This program is available on Windows and UNIX NetBackup clients. It accepts connections from remote NetBackup servers and clients that are attempting to verify the identity of requests from the local NetBackup system. The authentication method is VERITAS One-time Password (vopie). Normally, `vopied` is started by the NetBackup Client service on Windows and `inetd` on UNIX.

When you install NetBackup on a Windows client or UNIX client, the installation process adds entries for `vopied` to `C:\WINNT\system32\drivers\etc\services` on Windows and `/etc/services` and `/etc/inetd.conf` on UNIX.

The `services` entry looks like this:

```
vopied  13783/tcp       vopied
```

The `inetd.conf` entry on UNIX looks like this:

```
vopied  stream  tcp     nowait  root    /usr/openv/bin/vopied vopied
```

OPTIONS

`-standalone`
: Available only on UNIX clients and specifies that `vopied` will run continuously rather than being started by `inetd`.

`-debug`
: Available only on UNIX clients and implies `-standalone` (that is, `vopied` runs continuously). This option prevents `vopied` from forking and does not disconnect it from standard input, output, and error.

`-portnum` *number*
: Available only on UNIX clients and implies `-standalone` (that is, `vopied` runs continuously). Specifies the port number where `vopied` listens for requests. The default is the `vopied` entry in:

  `/etc/services`

`-max_time` *seconds*
Specifies a time out value for network connections. The default is 60 seconds.

`-log_dir` *path*
Specifies the directory where the `vopied` log directory resides. The default is:

install_path`\NetBackup\logs` (Windows)

`/usr/openv/logs` (UNIX)

To enable logging, create a `vopied` directory in the *path* directory before starting `vopied`. For example:

`/usr/openv/logs/vopied`

`-severity` *mask*
Specifies the type of messages to be logged. *mask* is the sum of zero or more of these values:

`1` Unknown

`2` Debug

`4` Information

`8` Warning

`16` Error

`32` Critical

The default is 48 decimal (0x30 hexadecimal), which specifies critical and error.

SEE ALSO

`bpauthsync(1M),vopie_util(1M)`

xbp(1)

NAME

xbp - Start the X Windows based interface for NetBackup users

SYNOPSIS

```
/usr/openv/netbackup/bin/xbp [-r] [-ra] [-rr]
         [-nl][-browselimit files] [X options]
```

DESCRIPTION

The xbp command starts a graphical user interface that lets users archive, back up, and restore files, directories, or raw partitions from their client workstations. You can use xbp only from an X terminal or X server that is compatible with MIT release X11.R4 (or later) of the X Window system.

The xbp interface follows OSF/Motif conventions. If you are unfamiliar with these conventions, see the *OSF/Motif User's Guide*, authored by the Open Software Foundation and published by Prentice-Hall, Inc., ISBN 0-130640509-6.

The xbp online help provides detailed operating instructions.

OPTIONS

xbp has separate modes for backups, archives, and restores. The backup and archive modes display the file system. By default, xbp starts in filesystem mode. The following options allow you to directly control the startup mode:

-r
: Start with display of backups for possible restore.

-ra
: Start with display of archives for possible restore.

-rr
: Start with display of raw-partition backups for possible restore.

-nl
: Specifies that xbp does not resolve links during the search. The default is to resolve links.

-browselimit *files*
: Specifies the limit for implicit searching.

  When switching to restore mode, if the number of files and directories that were backed up during the specified date range is large (10000 by default), xbp pops up a warning dialog saying that searching is delayed until the user explicitly selects Update Display from the Edit menu.

By using the -browselimit parameter when invoking xbp, a user can increase this limit beyond 10000 files.

Also, xbp supports the standard command-line options for X programs. One of these is the -d option, which forces the name of the X terminal or server. Most users already have their DISPLAY environment variable defined and can routinely ignore the -d option.

Other useful X options are:

-bg *color*
: Specifies the color to use for the background of the window. The default is white.

-fg *color*
: Specifies the color to use for displaying text. The default is black.

-font
: Allows you to enlarge text for visibility. It is best to use fixed-pitch fonts because xbp formats some text into columns. These columns can appear uneven with proportional fonts.

-geometry
: Allows you to control the initial size and position of the xbp window.

-title
: Controls the window manager title bar and is useful if you run several instances of xbp at once.

FILES

/usr/openv/netbackup/help/xbp/*

/usr/openv/netbackup/bp.conf

SEE ALSO

bp(1),bparchive(1),bpbackup(1),bplist(1),bprestore(1)

Index

Numerics

3pc.conf file
  sending output to screen 167, 254, 293

A

accessibility features xi
acsd command 1

B

Backup Exec
  listing files 146
backupdbtrace command 3
backuptrace command 5
bp command 7
bpadm command 9
bparchive command 10
bpauthorize command 15
bpauthsync command 18
bpbackup command 21
bpbackupdb command 27
bpcatarc command 32
bpcatlist command 33
bpcatres command 36
bpcatrm command 37
bpcd command 38
bpchangeprimary command 40
bpclassnew command 232
bpclclients command 190
bpclient command 45
bpclinclude command 198
bpclinfo command 203
bpclsched command 214
bpclschedrep command 225
bpconfig command 48
bpdbjobs command 58
bpdbm command 65
bpdgclone command 67
bpduplicate command 69
bperror command 77
bpexpdate command 88
bpgetconfig commnad 97
bpgetdebuglog commnad 100, 267
bpimagelist command 101, 106
bpimmedia command 113
bpimport command 123
bpinst command
  examples 135
  man page 129
  recreate a key file 134
bpkeyfile command
  man page 137
bpkeyutil command
  man page 139
bplabel command 141
bplist command 144
bpmedia command 151
bpmedialist command 154
bpminlicense command 165
bpmoverinfo command 167
bpnbat command 168
bpnbaz command 173
bppficorr command 188
bpplclients command 190
bppldelete command 197
bpplinclude command 198
bpplinfo command 203
bppllist command 212
bpplsched command 214
bpplschedrep command 225
bppolicynew command 232
bprd command 238
bprecover command 240
bprestore command 245
bpschedule command 256
bpschedulerep command 262
bpsetconfig 267
bpstuadd command 269

bpstudel command 276
bpstulist command 278
bpsturep command 283
bpsynth command 289
bptpcinfo command 254, 291
bpverify command 296

C

cat_convert utility 303
change_key_file_pass_phrase option 137
change_netbackup_pass_phrase option 137
configuring
    encryption, using bpinst command 129
crypt_option 131
crypt_strength option 131

D

DES
    keys, generating from bpkeyfile 137
disaster recovery 134
display option 137
drive
    reset 422
drive_mount_notify script 363, 366

F

force_install option 130

G

generating DES encryption keys 137
Glossary. *See* NetBackup Help.

I

importtrace command 308
Inline Tape Copy option 73
installation
    using bpinst command 129

J

jnbSA 311, 313

K

key file 134
    pass phrase 133

L

LEGACY_CRYPT option 131
Licenses
    managing with bpminlicense command 165
lmfcd command 315
lmfd command 315
lmftest 316
ltid command 319

M

Media Manager commands
    acsd 1
MySQL
    passwords 322

N

nbdbsetport command 321
nbdbsetpw command 322
ndmpmoveragent.start 323
ndmpmoveragent.stop 323
NetBackup troubleshooting commands
    backupdbtrace 3
    backuptrace 5
NetBackup Vault 73

O

-o - (on bptpcinfo command) 167, 254, 293
odld command 325
output options (on bptpcinfo) 167, 254, 293

P

pass phrase 133
    restrictions 138
passphrase_prompt option 132
passphrase_stdin option 132
passwords
    using nbdbsetpw to change password
    for nbdbd database service 322
policy_encrypt option 132
policy_names option 130, 133

R

recovery (disaster) 134
reset drive 422
restoretrace command 327
robtest 316, 342, 344

S

scripts
    drive_mount_notify 363, 366
set_ndmp_attr command 329
stdin option 137
stopltid command 319

T

tl4d command 332
tl8cd command 334
tl8d command 334
tldcd command 338
tldd command 338

tlhcd command 341
tlhd command 341
tlhtest 342
tlmd command 344
tlmtest 344
tpautoconf command 346
tpclean command 350
tpconfig command 353
tpformat command 360
tpreq command 363
tpunmount command 366
ts8d command 368
tsdd command 370
tshd command 372

U

update_libraries option 131

V

verbose option 131, 132
vlteject 383
vltinject 387
vltoffsitemedia 389
vltopmenu 393
vltrun 394
vmadd command 398
vmadm command 401
vmchange command 403
vmcheckxxx command 411
vmd command 413
vmdb_merge command 416
vmdelete command 419
vmoprcmd command 421
vmphyinv command 424
vmpool command 428
vmquery command 431
vmrule command 435
vmupdate command 437
vopie_util command 440
vopied command 444

X

xbp command 446