

Veritas NetBackup™ Appliance Commands Reference Guide

Release 3.2 (5250)



Veritas NetBackup™ Appliance Commands Reference Guide

Last updated: 2020-05-04

Legal Notice

Copyright © 2020 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

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

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

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

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

Technical Support

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

<https://www.veritas.com/support>

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

<https://my.veritas.com>

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

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

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

https://www.veritas.com/content/support/en_US/dpp.Appliances.html

Documentation feedback

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

APPL.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1	Overview	11
	About the NetBackup Appliance Shell Menu	11
	Logging on to the NetBackup Appliance Shell Menu	12
	Command limitations on appliances that are not configured	12
	Using the NetBackup Appliance Shell Menu	12
	About the NetBackup Appliance Shell Menu command views	13
	About the commands under the Appliance view	15
	About the commands under the Manage view	16
	About the commands under the Monitor view	23
	About the commands under the Network view	24
	About the commands under the Reports view	27
	About the commands under the Settings view	27
	About the commands under the Support view	30
Appendix A	Main > Appliance commands	34
	Main > Appliance > Master	35
	Main > Appliance > Media	36
	Main > Appliance > Management	37
	Main > Appliance > Remove	38
	Main > Appliance > ShowDedupPassword	39
	Main > Appliance > ShowIdentity	40
	Main > Appliance > Status	41
Appendix B	Main > Manage > FibreChannel commands	43
	Main > Manage > FibreChannel > Clean	44
	Main > Manage > FibreChannel > Configure	46
	Main > Manage > FibreChannel > Reset	50
	Main > Manage > FibreChannel > Scan	51
	Main > Manage > FibreChannel > Show	52
	Main > Manage > FibreChannel > Statistics	55
Appendix C	Main > Manage > HighAvailability commands	57

Manage > HighAvailability > AddNode	58
Main > Manage > HighAvailability > GetAssetTag	59
Manage > HighAvailability > RemoveNode	60
Manage > HighAvailability > Setup	62
Manage > HighAvailability > Status	63
Manage > HighAvailability > Switchover	65

Appendix D	Main > Manage > Libraries commands	66
	Main > Manage > Libraries > Configure	67
	Main > Manage > Libraries > Deny	68
	Main > Manage > Libraries > Down	69
	Main > Manage > Libraries > Inventory	70
	Main > Manage > Libraries > List	71
	Main > Manage > Libraries > Requests	72
	Main > Manage > Libraries > Reset	73
	Main > Manage > Libraries > Resubmit	74
	Main > Manage > Libraries > Up	75

Appendix E	Main > Manage > Libraries > Advanced > ACS commands	76
	Main > Manage > Libraries > Advanced > ACS	77
	Main > Manage > Libraries > Advanced > ACS	78
	Main > Manage > Libraries > Advanced > ACS	79
	Main > Manage > Libraries > Advanced > ACS	80
	Main > Manage > Libraries > Advanced > ACS	81
	Main > Manage > Libraries > Advanced > ACS	82
	Main > Manage > Libraries > Advanced > ACS	83
	Main > Manage > Libraries > Advanced > ACS	84
	Main > Manage > Libraries > Advanced > ACS	85
	Main > Manage > Libraries > Advanced > ACS	86

Appendix F	Main > Manage > License commands	87
	Main > Manage > License > Add	88
	Main > Manage > License > List	89
	Main > Manage > License > ListInfo	90
	Main > Manage > License > Remove	91

Appendix G	Main > Manage > MountPoints commands	92
	Main > Manage > MountPoints > List	93
	Main > Manage > MountPoints > Mount	94

	Main > Manage > MountPoints > Unmount	96
Appendix H	Main > Manage > NetBackup CLI commands	98
	Main > Manage > NetBackupCLI > Create	99
	Main > Manage > NetBackupCLI > Delete	100
	Main > Manage > NetBackupCLI > List	101
	Main > Manage > NetBackupCLI > PasswordExpiry	102
Appendix I	Main > Manage > OpenStorage commands	104
	Main > Manage > OpenStorage > Install	105
	Main > Manage > OpenStorage > List	107
	Main > Manage > OpenStorage > Readme	109
	Main > Manage > OpenStorage > Share	111
	Main > Manage > OpenStorage > Uninstall	112
Appendix J	Main > Manage > Software commands	113
	Main > Manage > Software > Cancel	114
	Main > Manage > Software > Delete	115
	Main > Manage > Software > Download	116
	Main > Manage > Software > DownloadProgress	117
	Main > Manage > Software > Firmware	118
	Main > Manage > Software > Install	119
	Main > Manage > Software > List	120
	Main > Manage > Software > Readme	122
	Main > Manage > Software > Rollback	124
	Main > Manage > Software > Share	125
	Main > Manage > Software > UpgradeStatus	126
	Main > Manage > Software > VxUpdate	127
Appendix K	Main > Manage > Storage commands	129
	Main > Manage > Storage > Add	130
	Main > Manage > Storage > Create	131
	Main > Manage > Storage > Delete	132
	Main > Manage > Storage > Edit	133
	Main > Manage > Storage > Monitor	136
	Main > Manage > Storage > Move	137
	Main > Manage > Storage > Remove	139
	Main > Manage > Storage > Resize	141
	Main > Manage > Storage > Scan	143

	Main > Manage > Storage > Show	145
	Main > Manage > Storage > Erase	147
Appendix L	Main > Manage > Tapes commands	149
	Main > Manage > Tapes > Cleaning	150
	Main > Manage > Tapes > Delete	151
	Main > Manage > Tapes > Eject	152
	Main > Manage > Tapes > Freeze	153
	Main > Manage > Tapes > Inventory	154
	Main > Manage > Tapes > List	155
	Main > Manage > Tapes > ListNetBackupMedia	156
	Main > Manage > Tapes > Suspend	157
	Main > Manage > Tapes > Unfreeze	158
	Main > Manage > Tapes > Unsuspend	159
Appendix M	Main > Manage > Certificates commands	160
	Main > Manage > Certificates > Generate	161
	Main > Manage > Certificates > Delete	162
Appendix N	Main > Monitor commands	163
	Main > Monitor > Beacon	164
	Main > Monitor > MemoryStatus	166
	Main > Monitor > NetBackup	169
	Main > Monitor > NetworkStatus	170
	Main > Monitor > SDCS	171
	Main > Monitor > Top	173
	Main > Monitor > Uptime	174
	Main > Monitor > Who	175
	Main > Monitor > Hardware	176
Appendix O	Main > Network commands	180
	Main > Network > Configure	182
	Main > Network > Date	185
	Main > Network > DNS	186
	Main > Network > Gateway	188
	Main > Network > Hostname	190
	Main > Network > Hosts	191
	Main > Network > IPv4	192
	Main > Network > IPv6	193
	Main > Network > LinkAggregation	194
	Main > Network > NetStat	198

Main > Network > NTPServer	199
Main > Network > Ping	200
Main > Network > SetProperty	201
Main > Network > Show	202
Main > Network > TimeZone	203
Main > Network > TraceRoute	204
Main > Network > Unconfigure	205
Main > Network > VLAN	206
Main > Network > WANOptimization	209

Appendix P Main > Network > Security commands (IPsec)

.....	213
Main > Network > Security > Configure	214
Main > Network > Security > Delete	215
Main > Network > Security > Export	216
Main > Network > Security > Import	217
Main > Network > Security > Provision	218
Main > Network > Security > Refresh	219
Main > Network > Security > Show	220
Main > Network > Security > Unconfigure	221

Appendix Q Main > Reports commands

Main > Reports > Deduplication	223
Main > Reports > Process	224

Appendix R Main > Settings commands

Main > Settings > Cloud	226
Main > Settings > Deduplication	227
Main > Settings > FibreTransport	235
Main > Settings > iSCSI > Initiator	239
Main > Settings > iSCSI > Interface	240
Main > Settings > iSCSI > Target	243
Main > Settings > LogForwarding	247
Main > Settings > LifeCycle	250
Main > Settings > NetBackup	254
Main > Settings > NetBackup DNAT	258
Main > Settings > Password	260
Main > Settings > Share	261
Main > Settings > SNMP polling	262
Main > Settings > Sysctl	263
Main > Settings > SystemLocale	264

Appendix S	Main > Settings > Alerts commands	266
	Main > Settings > Alerts > CallHome	267
	Main > Settings > Alerts > Email	272
	Main > Settings > Alerts > Hardware	274
	Main > Settings > Alerts > SNMP	275
Appendix T	Main > Settings > Notifications view commands	283
	Main > Settings > Notifications > LoginBanner	284
Appendix U	Main > Settings > Security commands	287
	Main > Settings > Security > Authorization	288
	Main > Settings > Security > Authentication > ActiveDirectory	291
	Main > Settings > Security > Authentication > Kerberos	294
	Main > Settings > Security > Authentication > LDAP	297
	Main > Settings > Security > Authentication > LocalUser	305
	Main > Settings > Security > Certificate	307
	Main > Settings > Security > FIPS	308
	Main > Settings > Security > Ports	310
	Main > Settings > Security > STIG	311
Appendix V	Main > Support commands	312
	Main > Support > Checkpoint	314
	Main > Support > Cleanup > RemoveShelfEntries	317
	Main > Support > Cleanup > ResetDIMMErrors	318
	Main > Support > Collect	320
	Main > Support > DataCollect	321
	Main > Support > Disk	323
	Main > Support > Errors	324
	Main > Support > FactoryReset	325
	Main > Support > FibreTransport	331
	Main > Support > InfraServices	333
	Main > Support > iostat	335
	Main > Support > IPMI	338
	Main > Support > KillRemoteCall	341
	Main > Support > Logs	342
	Main > Support > Maintenance	347
	Main > Support > Messages	348
	Main > Support > NBDNA	349
	Main > Support > nbperfchk	350

Main > Support > NBSU	354
Main > Support > Processes	355
Main > Support > RAID	356
Main > Support > Reboot	358
Main > Support > RecoverStorage	359
Main > Support > Service	360
Main > Support > ServiceAllowed	361
Main > Support > Show	363
Main > Support > Shutdown	367
Main > Support > Storage ClearReservations	368
Main > Support > Storage Reset	369
Main > Support > Storage SanityCheck	371
Main > Support > Test	372

Overview

This chapter includes the following topics:

- [About the NetBackup Appliance Shell Menu](#)
- [Logging on to the NetBackup Appliance Shell Menu](#)
- [Using the NetBackup Appliance Shell Menu](#)
- [About the NetBackup Appliance Shell Menu command views](#)

About the NetBackup Appliance Shell Menu

The NetBackup Appliance Shell Menu is an interactive shell that is available on the appliances through SSH. This menu interface enables you to perform most of the administration functions that are necessary to administer the appliances.

You can use the NetBackup Appliance Shell Menu in place of the NetBackup Appliance Web Console for many operations. In addition, anyone who is limited to only SSH because of firewall restraints should use this shell menu.

The *NetBackup Appliance Commands Reference Guide* contains detailed information about the NetBackup Appliance commands. Each command contains a brief description of the primary function of the command, a synopsis, and descriptions of the options that are listed in the synopsis. Some commands also contain notes and usage examples.

Note: It is possible that changes may occur after the documents have been initially released. The electronic versions of these documents on the Support website contain the most up-to-date information. You should refer to these documents for the latest information about the appliance. The documents are provided so that you can download and print them at any time.

[NetBackup Appliance Documentation page](#)

Logging on to the NetBackup Appliance Shell Menu

The following procedure explains how to log on to the NetBackup Appliance Shell Menu.

To log on to the NetBackup Appliance Shell Menu

- 1 Connect to the NetBackup Appliance Shell Menu.
- 2 Enter the user name and password for the appliance. By default, the user name `admin` has the password, `P@ssw0rd`.

Caution: For security reasons, you should change this password after you have installed the NetBackup appliance.

- 3 After a successful logon, the cursor is alongside the **Main_Menu** prompt.
- 4 Press the `?` key to display the available commands and shell views.

Command limitations on appliances that are not configured

Before an appliance can be managed, it must first be configured. The commands that are used for initial configuration are the only valid commands that can be executed on a new appliance, or a factory reset appliance. Commands other than those used for the initial configuration can exhibit unexpected or undesired behavior. To prevent this situation, Veritas recommends that you avoid using any management commands until after the appliance initial configuration has been completed.

For information on valid commands for appliances that are not configured, refer to the following documents:

NetBackup Appliance Initial Configuration Guide

NetBackup Appliance Commands Reference Guide

Using the NetBackup Appliance Shell Menu

This section details the use, options, and organization of the NetBackup Appliance Shell Menu.

The initial view outlines the various categories of tasks you can perform from the command-line interface.

All the commands are auto-completed. You can press **Tab** or **Enter** to complete a command.

The following is a list of helpful tips on how to use the NetBackup Appliance Shell Menu:

- When you press the `?` key, more information about the commands or sub-views is displayed. If you press `?` after you enter a command, the format and usage of the parameters for that command is displayed.
- When you press the space bar key, the next parameter that needs to be entered is displayed.
- When you press the Enter key, the next "mandatory" parameter that needs to be entered is displayed. A "mandatory" parameter is one that does not have default values.

Note: In the documentation, command variables that are *italicised* or in angular barackets (`<>`) are mandatory variables; whereas command parameters that are in square brackets (`[]`) are optional. For example, in the `Main > Manage > MountPoints > Unmount MountPoint [Force]` command, where *MountPoint* is a mandatory variable and [*Force*] is an optional parameter.

- The Secure Shell(SSH) sessions have a limited idle time due to security limits on the Red Hat Enterprise Linux (RHEL) Operating System. You may experience the following issues:
 - You are logged out automatically if the SSH session remains idle up to the current session time limit.
 - Commands fail to complete if they require more time than the current session time limit. One example where you may experience this issue is when you add a large number of LDAP or AD users and user groups.To help avoid these issues, keep the session alive for a longer duration by increasing the session time limit in the SSH client. For detailed configuration instructions, refer to your SSH client documentation.

About the NetBackup Appliance Shell Menu command views

When you enter the NetBackup Appliance Shell Menu, you enter on the `Main_Menu` view. This view is the starting point from which you can configure, manage, monitor, and support your appliance using the command line. The following table describes the views and commands that are available.

Table 1-1 NetBackup appliance commands and views from the `Main_Menu` view

Command	Explanation
Appliance	Enter the <code>Appliance</code> view to manage your master and media appliances. See “About the commands under the Appliance view” on page 15.
Exit	Exit the current shell and log out.
Manage	Enter the <code>Manage</code> view to manage your appliance. See “About the commands under the Manage view” on page 16.
Monitor	Enter the <code>Monitor</code> view to monitor appliance activities. See “About the commands under the Monitor view” on page 23.
Network	Enter the <code>Network</code> view to administer your network. See “About the commands under the Network view” on page 24.
Reports	Enter the <code>Reports</code> view to examine the running and historical state of the host. See “About the commands under the Reports view” on page 27.
Settings	Enter the <code>Settings</code> view to change the appliance settings. See “About the commands under the Settings view” on page 27.
Shell	<p>This command appears on all of the other command views.</p> <p>Use the following commands to do the following:, command line history information, and to return to the main menu.</p> <ul style="list-style-type: none"> ■ <code>Shell Help</code> Displays the help for using the shell menu. ■ <code>Shell History [Limit]</code> Displays the command-line history of the current session. You can set a limit with this command that defines the size of the history list. A limit of zero means the list has no boundaries. ■ <code>Shell Main</code> Returns to the main menu.
Support	Enter the <code>Support</code> view to enable and administer support capabilities on your appliance. See “About the commands under the Support view” on page 30.

Table 1-1 NetBackup appliance commands and views from the `Main_Menu` view *(continued)*

Command	Explanation
<code>Return</code>	This command is not present on the <code>Main_Menu</code> view, however, it appears on all other views. Use this command to return to the previous menu.

See [“About the NetBackup Appliance Shell Menu”](#) on page 11.

See [“Using the NetBackup Appliance Shell Menu”](#) on page 12.

See [“Logging on to the NetBackup Appliance Shell Menu ”](#) on page 12.

About the commands under the Appliance view

From within the Appliance view you can perform the following functions:

- Set the management role of an appliance.
- Configure the appliance role.
- Check the status of the appliance.
- Decommission an existing media appliance.
- View the identities of the appliance.
- View the NetBackup deduplication password.

The following table summarizes the commands that are available in the Appliance view depending on which appliance role you chose during the initial configuration.

Table 1-2

Command	Explanation
<code>Management</code>	Use this command to set the management role of a NetBackup appliance. See Appliance > Management on page 37.
<code>Master</code>	Use this command to configure your appliance as a NetBackup master appliance. See Appliance > Master on page 35.
<code>Media</code>	Use this command to configure the appliance as NetBackup media server. See Appliance > Media on page 36.

Table 1-2 (continued)

Command	Explanation
Remove	Use this command to decommission an existing media appliance. See Appliance > Remove on page 38.
ShowDedupPassword	Use to display the NetBackup deduplication password of the domain. See Appliance > ShowDedupPassword on page 39.
ShowIdentity	Use this command to display the identities of the current appliance for different authority requirements. See Appliance > ShowIdentity on page 40.
Status	Use this command to display the current appliance status information. See Appliance > Status on page 41.

Note: The commands `Master` and `Media` are only available during appliance initial configuration.

About the commands under the Manage view

From the appliance management view, **Manage**, you can perform the following functions:

- Administer the Fibre Transport HBA cards.
- Manage a high availability (HA) configuration.

Note: NetBackup Appliance models 5240 and 5250 do not support HA.

- Configure and inventory robotic tape libraries.
- Add, remove, and list license keys.
- Manage software updates.
- List and resize Storage Disk Pool Volumes of NetBackup.
- Manage the tape media for the appliance.
- Manage NetBackupCLI user accounts.
- Manage OpenStorage plugins.

- Manage remote mount points.

The following table summarizes the commands that are available in the Main > Manage view.

Table 1-3 Main > Manage view commands

Commands	Explanation
Certificates	<p>Enter the Certificates view. From this view you can do the following:</p> <ul style="list-style-type: none"> ■ <code>Generate</code> - Use the Generate command to generate and download a certificate for a vCenter or SCVMM client. See Manage > Certificates > Generate on page 161. ■ <code>Delete</code> - Use the Delete command to delete an existing certificate. See Manage > Certificates > Delete on page 162.
FibreChannel	<p>Enter the FibreChannel view to administer the Fibre Transport HBA cards. You can perform the following administrative functions:</p> <ul style="list-style-type: none"> ■ <code>Clean</code> - Clean stale SCSI information about unresponsive Fibre Channel devices from the system. See Manage > FibreChannel > Clean on page 44. ■ <code>Configure</code> - Configure supported FC HBA cards. See Manage > FibreChannel > Configure on page 46. ■ <code>Reset</code> - Reset Fibre Channel initiator ports on this appliance. See Manage > FibreChannel > Reset on page 50. ■ <code>Scan</code> - Scan the Fibre Channel HBA initiator ports on this appliance. See Manage > FibreChannel > Scan on page 51. ■ <code>Show</code> - Show the Fibre Channel cards in this appliance and configuration. See Manage > FibreChannel > Show on page 52. ■ <code>Statistics</code> - Display utilization statistics for the Fibre Channel HBA initiator ports on this appliance. See Manage > FibreChannel > Statistics on page 55.

Table 1-3 Main > Manage view commands (continued)

Commands	Explanation
HighAvailability	<p>Use these command options to configure or manage a high availability setup. From the HighAvailability view you can do the following:</p> <ul style="list-style-type: none"> ■ AddNode - Add a new compute node to the high availability setup. See Manage > HighAvailability > AddNode on page 58. ■ GetAssetTag - Display the status and the values of the asset tags on the hardware components in a high availability setup. See Manage > HighAvailability > GetAssetTag on page 59. ■ RemoveNode - Remove a node from the high availability setup. See Manage > HighAvailability > RemoveNode on page 60. ■ Setup - Perform a pre-check and configure the high availability setup. See Manage > HighAvailability > Setup on page 62. ■ Status - Display the high availability setup and the status of all related services. See Manage > HighAvailability > Status on page 63. ■ Switchover - Switch the services between the two nodes. See Manage > HighAvailability > Switchover on page 65. <p>Note: These commands can only be used on appliance model 53xx media servers. Appliance model 52xx master or media servers cannot be used to run these commands.</p>

Table 1-3 Main > Manage view commands (continued)

Commands	Explanation
Libraries	<p>Enter the NetBackup Library view. From the Libraries view you can configure and inventory robotic tape libraries. You can also perform the following functions:</p> <ul style="list-style-type: none"> ■ Advanced > ACS - Configure or edit the ACSLS network configuration entries in the <code>vm.conf</code> file. ■ Configure - Configure attached libraries for a media server. See Manage > Libraries > Configure on page 67. ■ Deny - Deny a pending tape request. See Manage > Libraries > Deny on page 68. ■ Down - Take drive offline. See Manage > Libraries > Down on page 69. ■ Inventory - Inventory libraries for volumes. See Manage > Libraries > Inventory on page 70. ■ List - List the attached libraries and tape drives for a media server. See Manage > Libraries > List on page 71. ■ Requests - List any pending tape requests. See Manage > Libraries > Requests on page 72. ■ Reset - Reset a drive. See Manage > Libraries > Reset on page 73. ■ Resubmit - Resubmit a pending tape request. See Manage > Libraries > Resubmit on page 74. ■ Up - Bring a drive online. See Manage > Libraries > Up on page 75.
License	<p>Enter the License administration view, where you can add, remove, and list license keys.</p> <ul style="list-style-type: none"> ■ Add - Add a license key. See Manage > License > Add on page 88. ■ List - List the currently installed licenses. See Manage > License > List on page 89. ■ ListInfo - List the detailed information of the installed licenses. See Manage > License > ListInfo on page 90. ■ Remove - Remove a license key. See Manage > License > Remove on page 91.

Table 1-3 Main > Manage view commands (continued)

Commands	Explanation
MountPoints	<p>Enter the MountPoints view.</p> <ul style="list-style-type: none"> List - List existing mount points on the appliance. See Manage > MountPoints > List on page 93. Mount - Mount a remote NFS drive. See Manage > MountPoints > Mount on page 94. Unmount - Unmount a mounted NFS drive See Manage > MountPoints > Unmount on page 96.
NetBackupCLI	<p>Enter the NetBackupCLI view.</p> <ul style="list-style-type: none"> Create - Create a NetBackup user account. See Manage > NetBackupCLI > Create on page 99. Delete - Delete a NetBackup user account. See Manage > NetBackupCLI > Delete on page 100. List - View a list of NetBackup users. See Manage > NetBackupCLI > List on page 101. PasswordExpiry - Use to manage the NetBackup command-line password. See Manage > NetBackupCLI > PasswordExpiry on page 102.
OpenStorage	<ul style="list-style-type: none"> Install - Install an OpenStorage plug-in. See Manage > OpenStorage > Install on page 105. List - View list of available or installed OpenStorage plug-ins. See Manage > OpenStorage > List on page 107. Share - Share or unshare directory for uploading a plug-in See Manage > OpenStorage > Share on page 111. Uninstall - Uninstall the OpenStorage plug-in. See Manage > OpenStorage > Uninstall on page 112.

Table 1-3 Main > Manage view commands (continued)

Commands	Explanation
Software	<p>Enter the Software view. From this view you can do the following:</p> <ul style="list-style-type: none"> ■ Cancel - Cancel the download of a software patch. See Manage > Software > Cancel on page 114. ■ Delete - Delete a software update. See Manage > Software > Delete on page 115. ■ Download - Download a software update. See Manage > Software > Download on page 116. ■ DownloadProgress - View the progress of an online patch download. See Manage > Software > DownloadProgress on page 117. ■ Install - Install a release update. See Manage > Software > Install on page 119. ■ List - List the available software information. See Manage > Software > List on page 120. ■ Readme - View the Readme to obtain the event sequence for installing a release update. See Manage > Software > Readme on page 122. ■ Rollback - Roll back the last installed release update. See Manage > Software > Rollback on page 124. ■ Share - Share or unshare a directory for uploading a software update. See Manage > Software > Share on page 125. ■ UpgradeStatus - View the version of your appliance. See Manage > Software > UpgradeStatus on page 126.

Table 1-3 Main > Manage view commands (continued)

Commands	Explanation
Storage	<p>Enter the Storage view. From this view you can do the following:</p> <ul style="list-style-type: none"> ■ Add - Add new storage expansion unit. See Manage > Storage > Add on page 130. ■ Create - Create a share. See Manage > Storage > Create on page 131. ■ Delete - Delete a share. See Manage > Storage > Delete on page 132. ■ Edit - Edit a share. See Manage > Storage > Edit on page 133. ■ Monitor - Monitor storage tasks. See Manage > Storage > Monitor on page 136. ■ Move - Move storage partition from one device to another. See Manage > Storage > Move on page 137. ■ Remove - Remove a storage expansion unit. See Manage > Storage > Remove on page 139. ■ Resize - Resize NetBackup storage partitions. See Manage > Storage > Resize on page 141. ■ Scan - Refresh the storage disks and devices information. See Manage > Storage > Scan on page 143. ■ Show - View NetBackup storage information. See Manage > Storage > Show on page 145.

Table 1-3 Main > Manage view commands (continued)

Commands	Explanation
Tapes	<p>Enter the Tapes view. The Tapes view contains the following commands that enable you administer the media that is configured to your appliance:</p> <ul style="list-style-type: none"> ■ Cleaning - Designate which tape is the cleaning tape See Manage > Tapes > Cleaning on page 150. ■ Delete - Delete media from a NetBackup database See Manage > Tapes > Delete on page 151. ■ Eject - Eject media from a tape library See Manage > Tapes > Eject on page 152. ■ Freeze - Freeze media in a NetBackup database See Manage > Tapes > Freeze on page 153. ■ Inventory - Inventory all of the libraries for the volumes that have been added or removed See Manage > Tapes > Inventory on page 154. ■ List - Show a list of the available media See Manage > Tapes > List on page 155. ■ ListNetBackupMedia - Show a list of the media that NetBackup uses See Manage > Tapes > ListNetBackupMedia on page 156. ■ Suspend - Suspend media in a NetBackup database See Manage > Tapes > Suspend on page 157. ■ Unfreeze - Unfreeze the media that has been frozen in a NetBackup database See Manage > Tapes > Unfreeze on page 158. ■ Unsuspend - Unsuspend the media that has been suspended in a NetBackup database See Manage > Tapes > Unsuspend on page 159.

About the commands under the Monitor view

From the Monitor view, you can perform the following functions:

- Monitor the appliance.
- Display backup jobs and network statistics.
- Display top process information and uptime statistics for the host.
- Display current logon sessions.

The following table summarizes the commands that are available in the Monitor view.

Table 1-4 Main > Monitor view commands

Command	Explanation
Beacon	Flash lights on storage expansion unit disk drives. See Monitor > Beacon on page 164.
Hardware	Monitors various components of the appliance. See Monitor > Hardware on page 176. The 52xx and 53xx appliances have additional options for the Monitor > Hardware commands.
MemoryStatus	Displays the memory usage statistics of the appliance in KB. See Monitor > MemoryStatus on page 166.
NetBackup	Displays and controls backup jobs. This command is available only for a master appliance. See Monitor > NetBackup on page 169.
NetworkStatus	Displays the network statistics for the appliance. See Monitor > NetworkStatus on page 170.
SDCS	Monitors the connection to Symantec Data Center Security (SDCS). See Monitor > SDCS on page 171.
Top	Display the top process information. See Monitor > Top on page 173.
Uptime	Display the uptime statistics for the current host. See Monitor > Uptime on page 174.
Who	Display current logon sessions on the current host. See Monitor > Who on page 175.

About the commands under the Network view

From the Network administration view, you can perform the following operations:

- Administer the network settings and link aggregation of the appliance.
- Set the time zone and the system time.

- Display the uptime statistics for the appliance.

The following table summarizes the commands that are available for you to use in the Network view.

Table 1-5 Main > Network view commands

Command	Explanation
Configure	Configure the IPv4 or IPv6 address of a network interface with the default gateway. See Network > Configure on page 182.
Date	Use to set or show the computer system time. See Network > Date on page 185.
DNS	Configure the DNS information. See Network > DNS on page 186.
Gateway	Add a new default gateway or delete an existing one for an interface. See Network > Gateway on page 188.
Hostname	Set or get the host name of an appliance. See Network > Hostname on page 190.
Hosts	Add or delete a host entry from the hosts' file or view the hosts configuration information. See Network > Hosts on page 191.
IPv4	Change the IPv4 address of a network interface. See Network > IPv4 on page 192.
IPv6	Change the IPv6 address of a network interface. See Network > IPv6 on page 193.

Table 1-5 Main > Network view commands (*continued*)

Command	Explanation
LinkAggregation	<p>LinkAggregation - The LinkAggregation command provides you with the following commands options.</p> <ul style="list-style-type: none"> ■ Create - Create a bond with or without assigning an IP to it. ■ Delete - Delete a bond. ■ Disable - Disable link aggregation. ■ Enable - Enable link aggregation and select a bonding mode. ■ Show - Show the status of link aggregation. ■ Status - Check the status of the link aggregation. <p>See Network > LinkAggregation on page 194.</p>
NetStat	<p>Examine network statistical information.</p> <p>See Network > NetStat on page 198.</p>
NTPServer	<p>Use this command to manage the NTP servers. You can add, delete, and show current NTP servers.</p> <p>See Network > NTPServer on page 199.</p>
Ping	<p>An attempt to reach a host or IP address with ICMP ECHO_REQUESTs</p> <p>See Network > Ping on page 200.</p>
Security	<p>Use the commands in this view to manage IPsec policies.</p>
SetProperty	<p>Use to set the Ethernet interface property.</p> <p>See Network > SetProperty on page 201.</p>
Show	<p>You can use this command to show the network properties.</p> <p>See Network > Show on page 202.</p>
Timezone	<p>Use to set or reset the time zone.</p> <p>See Network > TimeZone on page 203.</p>
TraceRoute	<p>Displays the network packet route.</p> <p>See Network > TraceRoute on page 204.</p>
Unconfigure	<p>Removes the IP address and shuts down the interface.</p> <p>See Network > Unconfigure on page 205.</p>

Table 1-5 Main > Network view commands *(continued)*

Command	Explanation
VLAN	<p>Manages VLAN operations</p> <p>The VLAN command provides you with the following options.</p> <ul style="list-style-type: none"> ■ Delete - Deletes a VLAN interface. ■ Show - Displays properties and status of VLAN interfaces. ■ Tag - Tags a VLAN over a physical or bonded interface. <p>See Network > VLAN on page 206.</p>
WANOptimization	<p>Manages WANOptimization.</p> <p>See Network > WANOptimization on page 209.</p>

See “[About the NetBackup Appliance Shell Menu command views](#)” on page 13.

About the commands under the Reports view

From the Reports view, you can perform the following functions:

- View deduplication statistics.
- View the status of a current process.

The following table summarizes the commands that are available in the Reports view.

Table 1-6 Main > Reports view commands

Command	Explanation
Deduplication	<p>Display deduplication statistics for the appliance.</p> <p>See Reports > Deduplication on page 223.</p>
Process	<p>View the status of the current processes on the appliance.</p> <p>See Reports > Process on page 224.</p>

About the commands under the Settings view

From the Main > Settings view you can perform the following functions:

- Enable or disable Call Home.
- Adjust deduplication parameters.
- Mange alert settings and email accounts.

- Administer the Fibre Transport features.
- Configure iSCSI
- Change backup image life cycle parameters settings.
- Change your user password.
- Manage user authorization and authentication.
- Administer the SNMP-related settings.
- Adjust NetBackup settings.
- Configure a media share.
- Modify sysctl parameters.
- Change the system locale.

The following table summarizes the commands that are available for you to use in the Main > Settings view.

Table 1-7 Main > Settings view commands

Command	Explanation
Alerts	<p>Enter the <code>Alert</code> view. The <code>Alerts</code> commands let you manage your alerts for Call Home, SNMP, and email notification settings. The following commands are available under the <code>Alerts</code> submenu:</p> <ul style="list-style-type: none"> ■ <code>CallHome</code> See Settings > Alerts > CallHome on page 267. ■ <code>Email</code> See Settings > Alerts > Email on page 272. ■ <code>Hardware</code> See Settings > Alerts > Hardware on page 274. ■ <code>SNMP</code> See Settings > Alerts > SNMP on page 275.
Deduplication	<p>Adjust deduplication parameters.</p> <p>See Settings > Deduplication on page 227.</p>
FibreTransport	<p>Administer Fibre Transport settings. This command is available only for a master appliance.</p> <p>See Settings > FibreTransport on page 235.</p>
iSCSI	<p>Configure the iSCSI settings. This applies to configuration H of the NetBackup 5240 appliance.</p> <p>See Settings > iSCSI > Initiator on page 239.</p>

Table 1-7 Main > Settings view commands (continued)

Command	Explanation
LifeCycle	<p>Change backup image life cycle parameters settings. This command is available only for a master appliance.</p> <p>See Settings > LifeCycle on page 250.</p>
NetBackup	<p>Use this command to do the following:</p> <ul style="list-style-type: none"> ■ Add/delete/show additional servers to the server list. ■ Tune NetBackup data buffers. ■ Show the NetBackup additional server list. <p>See Settings > NetBackup on page 254.</p>
Notifications	<p>Set and manage a text banner that appears before a user logs on to the appliance.</p> <p>See Settings > Notifications > LoginBanner on page 284.</p>
Password	<p>Change the administrator's user password on the current host.</p> <p>See Settings > Password on page 260.</p>
Security	<p>Enter into the Security view. From this view you can do the following:</p> <ul style="list-style-type: none"> ■ <i>Authentication</i> - authorize users to access the appliance by assigning them various roles (permissions). See Settings > Security > Authentication > LDAP on page 297. See Settings > Security > Authentication > ActiveDirectory on page 291. See Settings > Security > Authentication > Kerberos on page 294. See Settings > Security > Authentication > LocalUser on page 305. ■ <i>Authorization</i> - configure and manage user registration and authentication on the appliance. See Settings > Security > Authorization on page 288.
Share	<p>Configure a media share.</p> <p>See Settings > Share on page 261.</p>
Sysctl	<p>Modify your sysctl parameters.</p> <p>See Settings > Sysctl on page 263.</p>
SystemLocale	<p>Change the system locale of the NetBackup appliance to correctly display, backup, and restore the files and the folders that are named with non-7-bit ASCII characters. For example, Chinese, Japanese, Korean, German Umlaut, or French accents.</p> <p>See Settings > SystemLocale on page 264.</p>

About the commands under the Support view

From the Main > Support view you can perform the following functions:

- Collect appliance logs and data for support interactions through the `DataCollect` command.
- Manage system checkpoints and IPMI operations.
- Gather disk information.
- Display NetBackup errors.
- Create and Manage checkpoints.
- Reset the appliance to factory default settings.
- Show the appliance logs.
- Display the messages file.
- Restart your appliance.
- Turn off your appliance.
- Share, unshare, and set the level of debug logs.
- Display debugging information from the Vxlog files.
- Restart a service on a host.
- Upload a set of log files that are based on a timed duration of four hours.
- Create and send a .tar file of the logs based on the job ID.
- Create and send a .tar file of the logs based on the time the log files were created.
- Test the current status of the various appliance components.

The following table summarizes all of the commands that are available in the NetBackup Support view.

Table 1-8 Main > Support view commands

Command	Explanation
<code>CheckPoint</code>	Manage system checkpoints. See Support > Checkpoint on page 314.
<code>Cleanup</code>	Clean or reset specific appliance monitoring data. See Support > Cleanup > RemoveShelfEntries on page 317.

Table 1-8 Main > Support view commands (*continued*)

Command	Explanation
DataCollect	Gather the device logs. See Support > DataCollect on page 321.
Disk	Gather and displays information about the local disk layout and usage. See Support > Disk on page 323.
Errors	Display the problem entries from the previous day in the NetBackup logs. See Support > Errors on page 324.
FactoryReset	Reset the appliance to factory default settings. See Support > FactoryReset on page 325.
InfraServices	Display and control the infrastructure services. See Support > InfraServices on page 333.
iostat	Monitor the system input and output device loading See Support > iostat on page 335.
IPMI	Manage the IPMI operations. See Support > IPMI on page 338.
KillRemoteCall	Terminate remote calls on peer compute nodes. See Support > KillRemoteCall on page 341.
Logs	From this command you can perform the following tasks: <ul style="list-style-type: none"> ■ Browse the different appliance logs. ■ Set the level of debug logs ■ Export or remove CIFS and NFS shares for the logs. ■ Upload the NetBackup log files for your appliance to Support. The files that you send can be based on the job ID, the time that the log files were taken, or the default-based duration. ■ Display debugging information from the VXlog files. See Support > Logs on page 342.
Maintenance	Enable you to open an interactive shell menu that you can use to troubleshoot or manage underlying operating system tasks. See Support > Maintenance on page 347.

Table 1-8
Main > Support view commands *(continued)*

Command	Explanation
Messages	Display the message file. See Support > Messages on page 348.
NBDNA	Create and remove network traces with the NetBackup Domain Network Analyzer (NBDNA) utility. See Support > NBDNA on page 349.
Nbperfchk	Measure the read and write speeds of a disk array. See Support > nbperfchk on page 350.
NBSU	Manage NetBackup supported data files. See Support > NBSU on page 354.
Processes	Display the status of the current processes. See Support > Processes on page 355.
Reboot	Restart the system. See Support > Reboot on page 358.
RecoverStorage	View or purge any storage recovered during a reimage. See Support > RecoverStorage on page 359.
Service	Stop or restarts a service on an appliance Linux host. See Support > Service on page 360.
ServiceAllowed	Set specific components of a Primary or an Expansion Storage Shelf to the Service Allowed mode so that service can be performed on those units. See Support > ServiceAllowed on page 361.
Shutdown	Power the system off. See Support > Shutdown on page 367.

Table 1-8
Main > Support view commands (*continued*)

Command	Explanation
Storage	<p>Use this command to perform the following tasks:</p> <ul style="list-style-type: none"> Storage Reset - Delete the backup data and partitions from the appliance, and configure the disk status for all the disks as New Available. See Support > Storage Reset on page 369. Storage SanityCheck- Enable or disable storage sanity checks. See Support > Storage SanityCheck on page 371. Storage ClearReservations - Clear the existing storage reservations on the storage disks. See Support > Storage ClearReservations on page 368.
Test	<p>Test the current status of the various appliance components.</p> <p>See Support > Test on page 372.</p>

Main > Appliance commands

This appendix includes the following topics:

- [Appliance > Master](#)
- [Appliance > Media](#)
- [Appliance > Management](#)
- [Appliance > Remove](#)
- [Appliance > ShowDedupPassword](#)
- [Appliance > ShowIdentity](#)
- [Appliance > Status](#)

Appliance > Master

Appliance > Master – Configure the appliance as a NetBackup master appliance

SYNOPSIS

Master

DESCRIPTION

This command configures your appliance as a NetBackup master appliance. You can also configure your appliance as a master appliance during the initial configuration of the appliance from the NetBackup Appliance Web Console.

Note: This command is available only when the appliance is in a factory-install mode. The command is not available after the appliance is configured.

OPTIONS

Master

Configure your appliance as a NetBackup master server.

Appliance > Media

Appliance > Media – Configure an appliance as a media server.

SYNOPSIS

Media *MasterServer*

DESCRIPTION

This command is used to configure the appliance as a media server to an existing NetBackup master server. If the master server is in a clustered environment, Veritas recommends that you enter the cluster name first, followed by the names of the nodes within the master server cluster. You should use the comma character as a delimiter between the node names.

This command is available on the following types of appliances:

Note: This command is available only during the initial configuration of the appliance. After the appliance is configured, the `Appliance > Media` command is not available.

OPTIONS

Media *MasterServer*

Use to configure the appliance as a media server to an existing NetBackup master server.

MasterServer is the master server host name. You can provide the following information in this field:

- If the master server is a multi-homed server, make sure that the appliance and the host name are on the same network.
- If the master server is a clustered environment, enter the cluster name first followed by the names of the nodes within the master server cluster. You should use the comma character as a delimiter between the node names.

Appliance > Management

Appliance > Management – Set the management role of a NetBackup appliance

SYNOPSIS

```
Management Agent Register Hostname Access Key
```

```
Management Server
```

DESCRIPTION

You can use this command to set the management role of a NetBackup appliance. An appliance can be set as an Appliance Management Server (AMS) or an agent. If you want to centrally manage multiple NetBackup appliances in your environment from the Appliance Management Console, you must set the appliances as AMS and agents. See the *Appliance Management Guide* for details.

OPTIONS

```
Management Agent Register Hostname Access Key
```

Use the command to register this appliance as an agent. The appliance must be version 3.1 or later and must be configured as a master or a media server. Note that the AMS must already be configured before you can register an appliance as an AMA.

The hostname can be a Fully Qualified Domain name or an IPv4 and IPv6 address.

In order to register an appliance as an agent, you must enter an access key. You can generate the access key from the Appliance Management Console on the AMS and paste it here. The access key is 32 digits in length.

```
Management Server
```

Use this command to set this appliance as an AMS. The appliance must be version 3.1 or later and configured as a master or a media server.

Appliance > Remove

Appliance > Remove – Decommission an existing media server.

SYNOPSIS

```
Remove MediaServer TargetMediaServer
```

DESCRIPTION

You can use the `Remove` command to decommission a media appliance from your configuration. When you go through the process of decommissioning an appliance you can move your tape media to another appliance.

Note: This command only exists on a master appliance. You must use the master appliance to decommission a media appliance. To safely decommission an appliance, see the *NetBackup Appliance Decommissioning and Reconfiguration Guide*.

OPTIONS

```
Remove MediaServer TargetMediaServer
```

Decommission a media appliance. The *MediaServer* variable is the name of the appliance that you want to decommission. The *TargetMediaServer* variable is the name of the new appliance where the tapes are moved during the decommissioning of the original media server. If you do not want to move tape media, then specify **NONE** for this variable.

Appliance > ShowDedupPassword

Appliance > ShowDedupPassword – Display the NetBackup deduplication password of the domain.

SYNOPSIS

ShowDedupPassword

DESCRIPTION

You can use this command to display the NetBackup deduplication password of the domain. Simply type `ShowDedupPassword` at the command prompt to see the password.

Note: If you change the password for MSDP, the NetBackup Appliance Shell Menu does not display the new password. The `ShowDedupPassword` option displays the original password that was created during the installation process.

OPTIONS

ShowDedupPassword

Display the NetBackup deduplication password of the domain.

Appliance > ShowIdentity

Appliance > ShowIdentity – Display the identities of the appliance for different authority requirements.

SYNOPSIS

ShowIdentity

DESCRIPTION

This command displays the identity values of the current appliance from different aspects, such as the SSH fingerprint, and the certificates fingerprints.

Currently, it only shows the SSH fingerprint value of the appliance. You can check the SSH fingerprint of an appliance through the network first and note down the value. Then, log in to the appliance and use this command to get the SSH fingerprint. If the two values match, the network is safe for use.

For a NetBackup 53xx high availability (HA) configuration, before you add the partner node, it is mandatory to make sure that the network is safe.

OPTIONS

ShowIdentity

Use this command to get the identities of the appliance.

Appliance > Status

Appliance > Status – Show status information about the appliance.

SYNOPSIS

Status

DESCRIPTION

Use this command to show status information about the appliance.

OPTIONS

Status

Show the status information about the appliance, such as appliance model, software release version, roles, and network settings.

EXAMPLES

The following is an example output of the Main > Appliance > Status command

```
abc123.Appliance> Status
```

```
Wed Jul 10 04:43:00 UTC 2020
```

```
=====
```

```
Appliance Model is NetBackup Appliance 52xx.
```

```
Appliance Version is 3.x.
```

```
Appliance is configured as master appliance.
```

```
All storage partitions are below watermark.
```

```
-----
```

```
Network Settings
```

```
-----
```

```
BONDING [Disabled]
```

```
-----
```

```
PHYSICAL DEVICE STATUS
```

```
-----
```

eth0	:	1Gb/s	TP	UNPLUGGED UP	192.168.229.233	--	None	--
eth1	:	1Gb/s	TP	UNPLUGGED UP	--	None	--	--
eth2	:	1Gb/s	TP	PLUGGED UP	10.182.20.242	--	None	--
eth3	:	1Gb/s	TP	UNPLUGGED UP	--	None	--	--
eth4	:	10Gb/s	FC	UNPLUGGED UP	--	None	--	--
eth5	:	10Gb/s	FC	UNPLUGGED UP	--	None	--	--
eth6	:	10Gb/s	FC	UNPLUGGED UP	--	None	--	--
eth7	:	10Gb/s	FC	UNPLUGGED UP	--	None	--	--

ROUTING STATUS

default 10.182.1.1 eth2

**VNIC=Virtual Interface TP=Twisted Pair FC=Fibre channel 1G/10G=1/10 Gigabit Ethernet
INFO:Only a single cabled network card detected. Cabling other ports is recommended to
make use of Link aggregation.

Main > Manage > FibreChannel commands

This appendix includes the following topics:

- [Manage > FibreChannel > Clean](#)
- [Manage > FibreChannel > Configure](#)
- [Manage > FibreChannel > Reset](#)
- [Manage > FibreChannel > Scan](#)
- [Manage > FibreChannel > Show](#)
- [Manage > FibreChannel > Statistics](#)

Manage > FibreChannel > Clean

Manage > FibreChannel > Clean – Use this command to clean stale SCSI information about unresponsive Fibre Channel devices from the system.

SYNOPSIS

Clean

DESCRIPTION

SCSI devices may become unresponsive because these devices might have been removed from the system while the operating system keeps a stale reference to these SCSI devices. This command is used to remove the operating system references to these devices that are not relevant anymore.

Note: The `Clean` operation may fail the currently running duplication jobs over FC. The duplication jobs failover to other FT paths if they exist. If no other FT paths are available, they failover to the Ethernet network. If no FT connection or IP connection exists, the jobs fail.

OPTIONS

Clean

Remove the stale operating system references to the SCSI devices that have been removed.

EXAMPLES

The following is an example of information when you run the `Main > Manage> FibreChannel > Clean` command.

```
nbu-appliance.FC> Clean
- [Info] FTMS mode: Fibre Transport server installed and running.
- [Info] Fibre Transport Deduplication state: enabled
**** FC HBA Cards ****
18:00.0 Fibre Channel: QLogic Corp. ISP2722-based 16/32Gb Fibre Channel to PCIe Adapter (rev 01)
18:00.1 Fibre Channel: QLogic Corp. ISP2722-based 16/32Gb Fibre Channel to PCIe Adapter (rev 01)
19:00.0 Fibre Channel: QLogic Corp. ISP2722-based 16/32Gb Fibre Channel to PCIe Adapter (rev 01)
19:00.1 Fibre Channel: QLogic Corp. ISP2722-based 16/32Gb Fibre Channel to PCIe Adapter (rev 01)

**** Drivers ****
```

```
qla2xxx      is loaded
windrvr6     is loaded
qla2x00tgt   is loaded
scst         is loaded
scst_user    is loaded
```

**** Ports ****

Bus ID	Slot	Port	PortWWN	Status	PhysicalState	ConfigurationType	Speed	RemotePort
07:00.0	Slot5	1	21:00:00:24:FF:46:8A:12	Disconnected	Target	Target (FTMS)	0 gbit/s	-----
07:00.1	Slot5	2	21:00:00:24:FF:46:8A:13	Fabric	Target	Target (FTMS)	8 gbit/s	-----
08:00.0	Slot6	1	21:00:00:24:FF:8E:E4:0F	Disconnected	Target	Target (FTMS)	0 gbit/s	-----
08:00.1	Slot6	2	21:00:00:24:FF:8E:E4:0E	Disconnected	Target	Target (FTMS)	0 gbit/s	-----
81:00.0	Slot4	1	21:00:00:24:FF:8E:E4:14	Online	Initiator	Initiator	8 gbit/s	
81:00.1	Slot4	2	21:00:00:24:FF:8E:E4:15	Online	Target	Target (MSDP)	8 gbit/s	
82:00.0	Slot2	1	21:00:00:24:FF:8E:E5:B2	Linkdown	Initiator	Initiator	8 gbit/s	
82:00.1	Slot2	2	21:00:00:24:FF:8E:E5:B3	Online	Target	Target (MSDP)	8 gbit/s	

**** Devices ****

Device	Vendor	ID	Type	Remote Port
--------	--------	----	------	-------------

**** Remote Appliances over FC ****

Please scan for remote appliances over FC first

Manage > FibreChannel > Configure

Manage > FibreChannel > Configure – Use this command to configure the QLogic Fibre Channel HBA ports.

SYNOPSIS

Configure *NumberPorts*

Configure Deduplication Initiator *HBAportid*

Configure Deduplication Target *HBAportid*

DESCRIPTION

You can use the `configure` command to do the following:

- Configure the number of QLogic Fibre Channel HBA ports for use by SAN Client (if the SAN Client feature is enabled). You can configure the appliance Fibre Transport Media Server (FTMS) to use the 2 target port configuration or the 4 target port configuration.
- Configure the FC HBA ports on this appliance as target ports for Fibre Transport Deduplication. Fibre Transport Deduplication is a feature that enables you to use an appliance as a target host for optimized duplication and Auto Image Replication.

Note: You must restart the appliances in the FC zone where a port mode change has occurred. A port mode change occurs when you change and save the port mode configuration, or enable/disable the feature. Veritas recommends that you complete all the port mode changes before you restart the appliances.

OPTIONS

Configure *NumberPorts*

Configure the number of FC HBA target ports for use with the SAN Client feature. The available *NumberPorts* is 2 and 4.

For new appliances or for appliances that have been factory reset, the configuration default is 2.

The available options are as follows:

- `Configure 2`

Sets Port 1 to the target mode on the following FC HBA cards:

- NetBackup 5230 and 5330 - cards in slots 5 and 6
- NetBackup 5240 - cards in slots 5 and 6
- NetBackup 5250 - cards in slots 5 and 6
- NetBackup 5340 - cards in slots 5 and 6

■ `Configure 4`

Sets Ports 1 and 2 to the target mode on the following FC HBA cards:

- NetBackup 5230 and 5330 - cards in slots 5 and 6
- NetBackup 5240 - cards in slots 5 and 6
- NetBackup 5250 - cards in slots 5 and 6
- NetBackup 5340 - cards in slots 5 and 6

Changing this option restarts the appliance, but it does not change the state of the SAN Client feature.

By default, the SAN Client feature is disabled on new appliances or on appliances that have been factory reset. If the SAN Client feature is disabled, changes to this setting only mark the ports as ready for target mode use. To enable the SAN Client feature, go to the `Settings` view and run the `FibreTransport SANClient Enable` command.

`Configure Deduplication Initiator HBAportid`

Configure a port as an FC initiator port.

The *HBAportid* is the slot number(1-6) and port number(1-2) of the HBA port. The format is *Slot:Port*.

Note: You can check the current state of the available ports by using the `Main> Manage> FibreChannel> Show Ports` command before you configure a port.

The following HBA ports may be available:

- NetBackup 5230 - ports in slots 2, 3, 4
- NetBackup 5330 - ports in slots 2, 3, 6
- NetBackup 5240 - ports in slots 2, 4, 6
- NetBackup 5250 - ports in slots 2, 4, 6
- NetBackup 5340 - ports in slots 2, 3, 6

FC feature support depends on the particular HBA card configuration of each appliance. For complete information about available ports on your HBA configuration, see the *NetBackup Appliance Fibre Channel Guide*.

Note: This command restarts the Deduplication service if the port mode is changed. The service restart causes the ongoing jobs to fail, and then failover to LAN. It is recommended that you cancel or suspend all jobs before you change the port mode.

Configure Deduplication Target *HBAportid*

Configures a port as an FC target port for Optimized Duplication and Auto Image Replication(AIR).

The *HBAportid* is the slot number(1-6) and port number(1-2) of the HBA port. The format is *Slot:Port*.

Note: You can check the current state of the available ports by using the `Main> Manage> FibreChannel> Show Ports` command before you configure a port.

The following HBA ports may be available:

- NetBackup 5230 - ports in slots 2, 3, 4
- NetBackup 5330 - ports in slots 2, 3, 6
- NetBackup 5240 - ports in slots 2, 4, 6
- NetBackup 5250 - ports in slots 2, 4, 6
- NetBackup 5340 - ports in slots 2, 3, 6

FC feature support depends on the particular HBA card configuration of each appliance. For complete information about available ports on your HBA configuration, see the *NetBackup Appliance Fibre Channel Guide*.

Note: This command restarts the Deduplication service if the port mode is changed. The service restart causes the ongoing jobs fail, and then failover to LAN. It is recommended that you cancel or suspend all jobs before you change the port mode.

EXAMPLES

The following is an example of information when you run the `Configure Deduplicaton Initiator` command.


```
appliance.FC> Configure Deduplication Initiator 2:2
[Info] Checking the port state...
[Info] This port is currently configured as an FC target port for optimized duplication
and replication.
Are you sure that you want to change it to an FC initiator port? [yes, no] (no) yes
[Info] Configuring the port state...
[Info] Restarting the optimized duplication service to complete the change. This may take
1 - 2 minutes...
[Info] Port configured successfully as an FC initiator port for optimized duplication.
```

The following is an example of information when you run the `Configure Deduplication Target` command.

```
appliance.FC> Configure Deduplication Target 2:2
[Info] Checking the port state...
[Info] This port is currently configured as an FC initiator port.
Are you sure that you want to change it to an FC Target port for optimized duplication
and replication? [yes, no] (no) yes
[Info] Configuring the port state...
[Info] Restarting the optimized duplication service to complete the change. This may take
1 - 2 minutes...
[Info] Port configured successfully as an FC Target port for optimized duplication
and replication.
```

Manage > FibreChannel > Reset

Manage > FibreChannel > Reset – Use to reset the links between the appliance FC HBA ports that are in initiator mode and any ports connected to its initiator mode ports.

SYNOPSIS

Reset

DESCRIPTION

Use this command to reset the links between the appliance FC HBA ports that are in initiator mode and any ports that are connected to its initiator mode ports.

This command is most useful when the FC links are not up as expected. Link status can change because of SAN zoning changes. If a reset does not reset the links, use the `Main> Support> Reboot` command to restart the appliance.

OPTIONS

Reset

Reset the Fibre Channel card ports that are in the initiator mode. This option re-initializes the ports by issuing a Link Initialization Protocol reset.

EXAMPLES

The following is an example of information when you run the `Main > Manage> FibreChannel > Reset` command.

```
nbu-appliance.FC> reset
- [Info] Resetting HBA ports involves restarting the Deduplication service. It is recommended
that you cancel all running jobs before the reset. It may take 2-3 minutes before the ports are
available again.
Do you want to proceed? [yes, no] (no) yes
- [Info] FTMS mode: Fibre Transport server installed and running.
- [Info] Fibre Transport Deduplication state: enabled
- [Info] Initiating reset of port at 81:00.0
- [Info] Initiating reset of port at 81:00.1
- [Info] Initiating reset of port at 82:00.0
- [Info] Initiating reset of port at 82:00.1
```

Manage > FibreChannel > Scan

Manage > FibreChannel > Scan – Use to scan the devices that are visible from the FC card initiator ports on the appliance.

SYNOPSIS

Scan

DESCRIPTION

Use this command to scan the devices that are visible from the FC card initiator ports on the appliance.

By default, the operating system should automatically detect the devices that are connected to the appliance HBA initiator mode ports. If the OS does not detect the devices, use this command to try to detect them. If that fails, test the FC links by using the `Reset` command.

This command is most useful during zoning changes.

OPTIONS

Scan

Scan for target mode drivers that are visible from the FC card initiator ports on the appliance.

EXAMPLES

```
nbu-appliance.FC> SCAN
- [Info] FTMS mode: Fibre Transport server installed and running.
- [Info] Fibre Transport Deduplication state: enabled
- [Info] Initiating scan of port at 81:00.0
- [Info] Initiating scan of port at 82:00.0
- [Info] Scanning for remote appliances over FC
```

Manage > FibreChannel > Show

Manage > FibreChannel > Show – Use to view the FC HBA card port and device configuration.

SYNOPSIS

Show [Ports]

DESCRIPTION

Use this command to view the FC HBA card port and device configuration for this appliance.

OPTIONS

Show Ports

Use this command to view only the port information of the FC HBA cards for this appliance.

Port Information includes the following:

- Bus ID
- Slot location (1-6)
- Port location (1-2)
- Port World Wide Name (WWN)
- Status
 - Online
 - Offline
 - Fabric
 - Disconnected
 - Linkdown
 - Loop
 - Ptp
- Physical State (Initiator or Target)
- Configuration Type
 - Initiator - marked as a standard initiator port.

- Target (FTMS) - marked as a target port for SAN Client FTMS.
- Target (MSDP) - marked as a target port for duplicating data from another NetBackup 52xx or 53xx appliance.
- Speed
- Remote Ports

The `Physical State` column shows the actual state of the HBA ports.

The `Configuration Type` column shows the port mode that a user has specified. The default port type configuration is shown if the user has not changed it.

When you enable an FC feature, the port that has been marked as a target port for that feature then enters the target mode. Before the enabling operation, the port stays in the standard initiator mode, and it shows an actual physical state of Initiator.

By comparing the `Configuration Type` and the `Physical State` columns, you can know if a related FC feature is enabled.

Show

Use this command to view the following FC HBA card port and device configuration for this appliance:

- Configuration state of the Fibre Transport media server (FTMS)
- Configuration state of the HBA cards and the card names
- Whether the drivers are loaded
- Port information
- Device information
- Remote appliances over FC

Note: If you cannot see any target appliance that you have configured for this appliance, scan for remote appliances over FC by using the `Main> Manage> FibreChannel> Scan` and then run the `Show` command again.

EXAMPLES

The following is an example of information when you run the `Main > Manage> FibreChannel > Show` command.

```
appliance.FC> Show
- [Info] FTMS mode: none
```

- [Info] Fibre Transport Deduplication state: disabled

**** FC HBA Cards ****

18:00.0 Fibre Channel: QLogic Corp. ISP2722-based 16/32Gb Fibre Channel to PCIe Adapter (rev 01)

18:00.1 Fibre Channel: QLogic Corp. ISP2722-based 16/32Gb Fibre Channel to PCIe Adapter (rev 01)

**** Drivers ****

qla2xxx is loaded

windrvr6 is not loaded

qla2x00tgt is loaded

scst is loaded

scst_user is loaded

**** Ports ****

BusID	Slot	Port	Port WWN	Status	PhysicalState	ConfigurationType	Speed	Remote Ports
08:00.0	Slot6 1	21:00:00:24:FF:88:1E:52	Online	Initiator	Initiator	8 gbit/s	0x21000024ff8cd275	0x21000024ff8cd275
08:00.1	Slot6 2	21:00:00:24:FF:88:1E:53	Online	Initiator	Target(MSDP)	8 gbit/s	0x21000024ff8cd275	0x21000024ff8cd275

**** Devices ****

Device	Vendor	ID	Type	Remote Port
/dev/sg11	VERITAS	TEST-NET-2	FCPIPE (Dedup Target)	0x21000024ff8cd265
/dev/sg12	VERITAS	TEST-NET-2	FCPIPE (Dedup Target)	0x21000024ff8cd275

**** Remote Appliances over FC ****

The result is based on the scan at December 28 2015 Monday 06:01:35 PST

/dev/sg11	203.0.113.0
	98.51.100.0 (TEST-NET-2.veritas.com)
/dev/sg12	203.0.113.0
	98.51.100.0 (TEST-NET-2.veritas.com)

Manage > FibreChannel > Statistics

Manage > FibreChannel > Statistics – Use to display usage statistics for the FC card ports that are in the standard initiator mode.

SYNOPSIS

```
Statistics [Interval] [Count]
```

DESCRIPTION

Use this command to display usage statistics for the FC card ports that are in the standard initiator mode.

OPTIONS

```
Statistics [Interval] [Count]
```

Display usage statistics for the FC card ports that are in the standard initiator mode. The [Interval] and [Count] parameters are optional. The [Interval] parameter can be used to specify the time interval in seconds between updates. The default value of this parameter is one second. The [Count] parameter can be used to specify the number of times to display statistics. The default value of this parameter is 3.

EXAMPLES

The following is an example of information when you run the Main > Manage> FibreChannel > Statistics command.

```
nbu-appliance.FC> Statistics
```

Slot	Port	I/O R (count/s)	I/O W (count/s)	I/O R(KB /s)	I/O W(KB /s)	Target I/O R (KB/s)	Target I/O W (KB/s)
2	1	0	0	0	0	-	-
2	2	0	0	0	0	0	0
4	1	0	0	0	0	-	-
4	2	0	0	0	0	0	0

Slot	Port	I/O R	I/O W	I/O R(KB	I/O W(KB	Target I/O R	Target I/O W
		(count/s)	(count/s)	/s)	/s)	(KB/s)	(KB/s)
2	1	0	0	0	0	-	-
2	2	0	0	0	0	0	0
4	1	0	0	0	0	-	-
4	2	0	0	0	0	0	0

Slot	Port	I/O R	I/O W	I/O R(KB	I/O W(KB	Target I/O R	Target I/O W
		(count/s)	(count/s)	/s)	/s)	(KB/s)	(KB/s)
2	1	0	0	0	0	-	-
2	2	0	0	0	0	0	0
4	1	0	0	0	0	-	-
4	2	0	0	0	0	0	0

Main > Manage > HighAvailability commands

This appendix includes the following topics:

- [Manage > HighAvailability > AddNode](#)
- [Manage > HighAvailability > GetAssetTag](#)
- [Manage > HighAvailability > RemoveNode](#)
- [Manage > HighAvailability > Setup](#)
- [Manage > HighAvailability > Status](#)
- [Manage > HighAvailability > Switchover](#)

Manage > HighAvailability > AddNode

Manage > HighAvailability > AddNode – Add a new compute node to a high availability (HA) setup.

SYNOPSIS

AddNode *hostname*

DESCRIPTION

This command adds a new compute node (partner node) to an HA setup by adding the host name of the new node.

This command is only available before the HA setup is complete.

Note: This command can only be used on appliance model 53xx media servers. Appliance model 52xx master or media servers cannot be used to run this command.

Before using this command, make sure that the following requirements are met:

- The model and the hardware configuration of the node you want to add are identical to the existing node.
- The two nodes use the same software version.
- The HA setup has been created using the first configured node.
- The hostname, the IP address, and the network details are configured on the node you want to add.

OPTIONS

AddNode *hostname*

Use this command to add the host name of the new compute node to an HA setup.

Manage > HighAvailability > GetAssetTag

Manage > HighAvailability > GetAssetTag – Display the status and the values of the asset tags on the hardware components in a high availability (HA) configuration.

SYNOPSIS

```
GetAssetTag
```

DESCRIPTION

This command shows the comparison result and each of the asset tag values on the hardware components in an HA setup. The asset tag values on the hardware components in a same HA setupn should be identical.

If the comparison result is `Not OK`, you need to restart the node or nodes with the different value from the shared Primary Storage Shelf.

Note: This command can only be used on appliance model 53xx media servers. Appliance model 52xx master or media servers cannot be used to run this command.

OPTIONS

```
GetAssetTag
```

EXAMPLES

The following is an example of the information that is displayed when you run the `Main > Manage > HighAvailability >GetAssetTag` command:

```
Status: NotOK
      abcnode1:0000111122223333
      efgnode2:0000111122224444
      Storage Shelf:0000111122223333
- [warning] The values of the AssetTag are not identical in the current high
availability configuration.
      Restart the node(s) with the different value from the Storage
shelf, and check the AssetTag value again. If the problem persists, contact
Veritas Technical Support.
```

Manage > HighAvailability > RemoveNode

Manage > HighAvailability > RemoveNode – Remove a node from a high availability (HA) setup.

SYNOPSIS

```
RemoveNode HostName
```

DESCRIPTION

This command removes a configured compute node from an HA setup for maintenance, replacement, or re-purposing. When you remove a node, the data that was backed up with that node remains available from the other node in the HA setup

If you remove a node from the HA setup, it cannot be upgraded. HA nodes must be upgraded from within the HA setup.

Note: This command can only be used on appliance model 53xx media servers. Appliance model 52xx master or media servers cannot be used to run this command.

OPTIONS

```
RemoveNode HostName
```

Use this command to remove a node from an HA setup. The *HostName* is the physical host name of the node. This command can only be run on the node that is not to be removed from the setup.

Note: You cannot perform this operation with the virtual host name or the virtual IP address. You must use the physical host name or the physical IP address of the specific node.

You can only revert the partner node to be a non-HA node by running the `RemoveNode` command. If you attempt to run a factory reset or initiate a rollback to a non-HA checkpoint on a node in an HA setup, the HA setup can malfunction.

If you need to add the node back to the HA setup, perform the following tasks in the order as they appear:

- Refer to the `FactoryReset` command to reset the node to the factory default settings.

Note: Before you perform the factory reset, make sure that you first perform the following tasks:

Remove the node from the HA setup with this command.

Remove the Ethernet cables between the two nodes and the FC cables between the node and the Primary Storage Shelf.

- Refer to the `Manage > High Availability > AddNode` command.

To replace the removed node with a different node, refer to the *NetBackup Appliance High Availability Reference Guide*.

Manage > HighAvailability > Setup

Manage > HighAvailability > Setup – Set up an appliance for a high availability (HA) setup.

SYNOPSIS

```
Setup NewHostName NewIPAddress
```

DESCRIPTION

This command is used on a configured media server to configure the HA setup and to include this media server as the first HA node in the setup. During this procedure, the host name and the IP address of the node are elevated as the virtual host name and the virtual IP address. Because of the elevation, you need to assign a new host name and a new IP address to the node.

The virtual host name and the virtual IP address work as the floating pointers in the HA configuration. With this mechanism, you can also access the HA setup with the virtual IP address or the virtual hostname.

After you set up HA with the first appliance, the HA configuration is partially complete. To complete the HA configuration, perform the initial configuration on the partner node and add it to the HA setup. Refer to *NetBackup Appliance Initial Configuration Guide* for more information.

Note: This command can only be used on appliance model 53xx media servers. Appliance model 52xx master or media servers cannot be used to run this command.

OPTIONS

```
Setup NewHostName NewIPAddress
```

Use this command to configure an appliance to be an HA node.

The mandatory options are as follows:

- **NewHostName**
The hostname of the node after the setup procedure
- **NewIPAddress**
The IP address of the node after the setup procedure

Manage > HighAvailability > Status

Manage > HighAvailability > Status – Display the high availability (HA) setup and the status of all related services.

SYNOPSIS

Status

DESCRIPTION

This command displays the status of the HA setup and the status of the relevant services that are running on the two nodes.

Note: This command can only be used on appliance model 53xx media servers. Appliance model 52xx master or media servers cannot be used to run this command.

OPTIONS

Status

Use this command to see the status of your HA setup and the status of the relevant services.

EXAMPLES

The following is an example of the information that is displayed when you run the Main > Manage > HighAvailability > Status command:

High Availability status: OK

Virtual hostname: veritastest

Virtual IP address: 00.000.000.000

Media Server	Status	Heartbeat Link	Service	Service Status
veritast1	Running	OK	AdvancedDisk	Online
			Fingerprint Calculation	Online
			MSDP	Online
			Virtual IP	Online
			Share	Online

veritast2	Running	OK	AdvancedDisk	Online
			Fingerprint Calculation	Online
			MSDP	Offline
			Virtual IP	Offline
			Share	Online

- [Info] MSDP service can be online only on one media server. The Fingerprinting service runs on all running media servers.
- [Info] AdvancedDisk service can be online on all running media servers.
- [Info] Share service can be online only on the node where the virtual IP address is assigned in the high availability configuration.

Manage > HighAvailability > Switchover

Manage > HighAvailability > Switchover – Switch the services between the two nodes in a high availability (HA) setup.

SYNOPSIS

```
Switchover hostname
```

DESCRIPTION

This command switches the services from one node to the target node in an HA setup. Use this command for a planned upgrade or maintenance, because such operations need to be performed on the node where the MSDP service is not running.

Note: You cannot perform this operation with the virtual hostname or virtual IP address. You need to use the physical hostname or physical IP address.

The MSDP-related backup and restore jobs are terminated during the switchover. Make sure that no such jobs are running before the switchover.

Note: This command can only be used on appliance model 53xx media servers. Appliance model 52xx master or media servers cannot be used to run this command.

OPTIONS

```
Switchover hostname
```

Use this command to switch the services from one node to the target node. The *hostname* is the hostname of the target node.

Main > Manage > Libraries commands

This appendix includes the following topics:

- [Manage > Libraries > Configure](#)
- [Manage > Libraries > Deny](#)
- [Manage > Libraries > Down](#)
- [Manage > Libraries > Inventory](#)
- [Manage > Libraries > List](#)
- [Manage > Libraries > Requests](#)
- [Manage > Libraries > Reset](#)
- [Manage > Libraries > Resubmit](#)
- [Manage > Libraries > Up](#)

Manage > Libraries > Configure

Manage > Libraries > Configure – Used to configure attached robotic tape libraries for a media server.

SYNOPSIS

`Configure MediaServer`

DESCRIPTION

This command enables you to configure the attached libraries for a media server.

OPTIONS

`Configure MediaServer`

Use this command to configure the attached libraries for a media server.

MediaServer is the name of the media server.

Manage > Libraries > Deny

Manage > Libraries > Deny – Deny a pending tape request.

SYNOPSIS

Deny *RequestID*

DESCRIPTION

Use this command to deny a pending tape request.

OPTIONS

Deny *RequestID*

Use this command to deny a pending tape request.

RequestID is the ID for the pending tape request. You must run the Libraries
> Requests command to retrieve the request ID.

Manage > Libraries > Down

Manage > Libraries > Down – Use to stop a drive.

SYNOPSIS

Down *DriveName*

DESCRIPTION

Use this command to stop a drive that you identify by a drive name.

OPTIONS

Down *DriveName*

Use this command to stop a drive.

DriveName defines the name of the drive that you want to stop.

Manage > Libraries > Inventory

Manage > Libraries > Inventory – Inventory libraries for volumes.

SYNOPSIS

```
Inventory MediaServer
```

DESCRIPTION

This command enables you to inventory libraries for volumes for a designated media server.

OPTIONS

```
Inventory MediaServer
```

Use this command to inventory libraries for volumes for a media server.

MediaServer is the name of the media server.

Manage > Libraries > List

Manage > Libraries > List – List attached libraries and tape drives for the media server.

SYNOPSIS

List

DESCRIPTION

This command enables you to list the attached libraries and the tape drives for the media server in the form of a Drive Status output. This output provides pertinent information such as the drive name, label, drive type, the host, drive path, and the current status.

OPTIONS

List
Configure the attached libraries for the media server.

EXAMPLES

The following drive status and robots information is produced when you run the List command.

```
DRIVE STATUS

Drive Name Label Ready RecMID ExtMID Wr.Enbl. Type Host DrivePath Status
=====

Libraries> List

ROBOTS

Robot:          ROBOT0
Robot Type:     TLD(8)
Media Server:   ascm2
Serial Number:  RBD31A0008
Inquiry:        ATL      M2500          3.07
```

Manage > Libraries > Requests

Manage > Libraries > Requests – List the pending tape requests.

SYNOPSIS

Requests

DESCRIPTION

This command enables you to list all pending tape requests.

OPTIONS

Request

Lists the pending tape requests.

EXAMPLES

To view the pending tape requests, type the following command from the Libraries view:

Requests

The result shows the pending requests. If there are no pending requests, the following appears.

PENDING REQUESTS

<NONE>

Manage > Libraries > Reset

Manage > Libraries > Reset – Use to reset a drive.

SYNOPSIS

Reset *DriveName*

DESCRIPTION

This command enables you to reset a specific drive.

OPTIONS

Reset *DriveName*

Use this command to reset a drive.

DriveName is the name of the drive. Run the Manage > Libraries > List to retrieve the *DriveName*.

Manage > Libraries > Resubmit

Manage > Libraries > Resubmit – Use to resubmit a pending tape request.

SYNOPSIS

`Resubmit RequestID`

DESCRIPTION

This command enables you to resubmit a pending tape request.

OPTIONS

`Resubmit RequestID`

Use to resubmit a pending tape request.

RequestID contains the RequestID for the pending request.

See [“Logging on to the NetBackup Appliance Shell Menu ”](#) on page 12.

Manage > Libraries > Up

Manage > Libraries > Up – Use to start a drive.

SYNOPSIS

Up *DriveName*

DESCRIPTION

This command enables you to start a drive and to bring it back online for use.

OPTIONS

Up *DriveName*

Use this command to start a drive.

DriveName contains the name of the drive.

Main > Manage > Libraries > Advanced > ACS commands

This appendix includes the following topics:

- [Manage > Libraries > Advanced > ACS > ACS_CSI_HOSTPORT](#)
- [Manage > Libraries > Advanced > ACS > ACS_SEL_SOCKET](#)
- [Manage > Libraries > Advanced > ACS > ACS_SSI_HOSTNAME](#)
- [Manage > Libraries > Advanced > ACS > ACS_SSI_INET_PORT](#)
- [Manage > Libraries > Advanced > ACS > ACS_SSI_SOCKET](#)
- [Manage > Libraries > Advanced > ACS > ACS_TCP_RPCSERVICE](#)
- [Manage > Libraries > Advanced > ACS > ACS_UDP_RPCSERVICE](#)
- [Manage > Libraries > Advanced > ACS > API_BARCODE_RULES](#)
- [Manage > Libraries > Advanced > ACS > TestACS](#)
- [Manage > Libraries > Advanced > ACS > ViewVMconf](#)

Manage > Libraries > Advanced > ACS > ACS_CSI_HOSTPORT

Manage > Libraries > Advanced > ACS > ACS_CSI_HOSTPORT – Use to add or remove the ACS CSI host name and the socket name in the `vm.conf` file.

SYNOPSIS

```
ACS_CSI_HOSTPORT Operation SSIHOSTNAME PORTNAME
```

DESCRIPTION

Use this command to add or remove the ACS library software host name and the socket name in the `vm.conf` file.

OPTIONS

```
ACS_CSI_HOSTPORT Operation SSIHOSTNAME PORTNAME
```

Use this command to add or remove the ACS CSI host name and socket name in the `vm.conf` file. The `vm.conf` entry specifies the port where the `acsssi` process sends its ACSLS requests on the ACSLS server. The ACSLS CSI must use this port to accept inbound ACSLS requests from `acsssi` processes.

Operation is Add or Remove.

SSIHOSTNAME contains the name of the SSI host name of the ACS library host. Do not use the IP address of the ACS library host for this parameter.

PORTNAME contains a value of 1024 - 65535, or 0. The value must match the one on the ACSLS server for the port that the CSI uses for inbound packets. If 0 (zero), NetBackup uses the previous behavior of CSI and `acsssi` (no specific ports).

Manage > Libraries > Advanced > ACS > ACS_SEL_SOCKET

Manage > Libraries > Advanced > ACS > ACS_SEL_SOCKET – Use to add or remove the ACS SEL socket name in the `vm.conf` file on the specified host.

SYNOPSIS

`ACS_SEL_SOCKET Operation SOCKETNAME`

DESCRIPTION

Use this command to add or remove the ACS SEL socket name in the `vm.conf` file on the specified host.

OPTIONS

`ACS_SEL_SOCKET Operation SOCKETNAME,`

Use this command to add or remove the ACS SEL socket name in the `vm.conf` file on the specified host.

Operation is Add or Remove.

SOCKETNAME defaults to 13740. If the `ACS_SEL_SOCKET` entry is specified in the `vm.conf` file, the default can be changed.

Manage > Libraries > Advanced > ACS > ACS_SSI_HOSTNAME

Manage > Libraries > Advanced > ACS > ACS_SSI_HOSTNAME – Use to add or remove the ACS SSI host name in the `vm.conf` file on the local host.

SYNOPSIS

`ACS_SSI_HOSTNAME Operation SSIHOSTNAME`

DESCRIPTION

Use this command to add or remove the ACS SSI host name in the `vm.conf` file on the local host.

OPTIONS

`ACS_SSI_HOSTNAME SSIHOSTNAME`

Use this command to add or remove the ACS SSI host name in the `vm.conf` file on the local host.

Operation is Add or Remove.

SSIHOSTNAME contains the host name to which RPC return packets from ACS library software are routed for ACS network communications. By default, the local host name is used. Do not use the IP address of the host for this parameter.

Manage > Libraries > Advanced > ACS > ACS_SSI_INET_PORT

Manage > Libraries > Advanced > ACS > ACS_SSI_INET_PORT – Use to add or remove the ACS SSI INET PORT host name and the socket name in the `vm.conf` file.

SYNOPSIS

```
ACS_SSI_INET_PORT Operation SSIHOSTNAME PORTNAME
```

DESCRIPTION

Use this command to add or remove the host name of the ACS library host in the `vm.conf` file.

OPTIONS

```
ACS_SSI_INET_PORT Operation SSIHOSTNAME PORTNAME
```

Use this command to add or remove the host name of the ACS library host in the `vm.conf` file.

Operation is Add or Remove.

SSIHOSTNAME contains the host name of the ACS library host. Do not use the IP address of the ACS library host for this parameter.

PORTNAME contains the port that `acsssi` uses for incoming ACSLS responses. Valid values are 1024 - 65535 and 0. This value must be unique for each `acsssi` process. A value from 1024 - 65535 indicates the number to be used as the TCP port on which `acsssi` accepts ACSLS responses.

Manage > Libraries > Advanced > ACS > ACS_SSI_SOCKET

Manage > Libraries > Advanced > ACS > ACS_SSI_SOCKET – Use to add or remove the host name of the ACS library host in the `vm.conf` file.

SYNOPSIS

`ACS_SSI_SOCKET Operation SSIHOSTNAME SOCKETNAME`

DESCRIPTION

Use this command to add or remove the host name of the ACS library host in the `vm.conf` file.

OPTIONS

`ACS_SSI_SOCKET Operation SSIHOSTNAME SOCKETNAME`

Use this command to add or remove the host name of the ACS library host in the `vm.conf` file.

Operation is Add or Remove.

SSIHOSTNAME contains the host name of the ACS library host. Do not use the IP address of the ACS library host for this parameter.

SOCKETNAME defaults to 13741. If the `ACS_SSI_SOCKET` entry is specified in the `vm.conf` file, specify socket names on an ACS library software host basis.

Manage > Libraries > Advanced > ACS > ACS_TCP_RPCSERVICE

Manage > Libraries > Advanced > ACS > ACS_TCP_RPCSERVICE – Use to add or remove the ACS_TCP_RPCSERVICE entry in the `vm.conf` file on the specified host.

SYNOPSIS

`ACS_TCP_RPCSERVICE Operation`

DESCRIPTION

Use this command to add or remove the `ACS_TCP_RPCSERVICE` entry in the `vm.conf` file.

OPTIONS

`ACS_TCP_RPCSERVICE Operation`

Use this command to specify the method over which `acsssi` communicates with ACSLS servers: TCP or UDP.

Operation is Add or Remove.

Only one entry should be entered into the `vm.conf` file. NetBackup uses UDP if both entries are found or if neither entry is found. For `acsssi` firewall support, `ACS_TCP_RPCSERVICE` must be entered in the `vm.conf` file.

Manage > Libraries > Advanced > ACS > ACS_UDP_RPCSERVICE

Manage > Libraries > Advanced > ACS > ACS_UDP_RPCSERVICE – Use to add or remove the ACS_UDP_RPCSERVICE entry in the `vm.conf` file on the specified host.

SYNOPSIS

`ACS_UDP_RPCSERVICE Operation`

DESCRIPTION

Use this command to add or remove the `ACS_UDP_RPCSERVICE` entry in the `vm.conf` file.

OPTIONS

`ACS_UDP_RPCSERVICE Operation`

Use this command to specify the method over which `acsssi` communicates with ACSLS servers: TCP or UDP.

Operation is Add or Remove.

Only one entry should be entered into the `vm.conf` file. NetBackup uses UDP if both entries are found or if neither entry is found. For `acsssi` firewall support, `ACS_TCP_RPCSERVICE` must be entered in the `vm.conf` file.

Manage > Libraries > Advanced > ACS > API_BARCODE_RULES

Manage > Libraries > Advanced > ACS > API_BARCODE_RULES – Use to enable or disable NetBackup barcode rule support for API robots.

SYNOPSIS

API_BARCODE_RULES *Operation*

DESCRIPTION

Use this command to enable or disable NetBackup barcode rule support for API robots.

NetBackup barcode rules allow default media mappings to be overridden. Barcode rules are especially useful when multiple generations of the same tape drive use the same type of media.

OPTIONS

API_BARCODE_RULES *Operation*

Use this command to enable or disable NetBackup barcode rule support for API robots.

Operation is Add or Remove.

Use Add to enable NetBackup barcode rule support for API robots. Use Remove to disable NetBackup barcode rule support for API robots.

Manage > Libraries > Advanced > ACS > TestACS

Manage > Libraries > Advanced > ACS > TestACS – Use to test ACSLS communications.

SYNOPSIS

`TestACS ACSLSHOSTNAME`

DESCRIPTION

Use this command to test the ACSLS communications based on the ACS settings in the `vm.conf` file.

OPTIONS

`TestACS ACSLSHOSTNAME`

Tests the ACSLS communications.

ACSLSHOSTNAME is the ACSLS host name.

Manage > Libraries > Advanced > ACS > ViewVMconf

Manage > Libraries > Advanced > ACS > ViewVMconf – Use to view the `vm.conf` file entries.

SYNOPSIS

ViewVMconf

DESCRIPTION

Use this command to view the entries in the `vm.conf` file.

OPTIONS

ViewVMconf

Use to view the `vm.conf` file entries.

Main > Manage > License commands

This appendix includes the following topics:

- [Manage > License > Add](#)
- [Manage > License > List](#)
- [Manage > License > ListInfo](#)
- [Manage > License > Remove](#)

Manage > License > Add

Manage > License > Add — Add a license key.

SYNOPSIS

Add

DESCRIPTION

You can use this command to add a license key.

OPTIONS

Add *LicenseFilename*

Use to add a license key.

Manage > License > List

`Manage > License > List` – List the licenses.

SYNOPSIS

`List`

DESCRIPTION

You use this command to list the installed licenses.

OPTIONS

`List`

Use to list the installed licenses.

Manage > License > ListInfo

`Manage > License > ListInfo` – List detailed information about the installed licenses.

SYNOPSIS

`ListInfo`

DESCRIPTION

Use this command to list detailed information about the installed licenses.

OPTIONS

`ListInfo`

Use to list detailed information about the installed licenses.

Manage > License > Remove

Manage > License > Remove – Remove a license key.

SYNOPSIS

Remove

DESCRIPTION

You use this command to remove a license key.

OPTIONS

Remove

Use to remove a license key.

Main > Manage > MountPoints commands

This appendix includes the following topics:

- [Manage > MountPoints > List](#)
- [Manage > MountPoints > Mount](#)
- [Manage > MountPoints > Unmount](#)

Manage > MountPoints > List

`Manage > MountPoints > List` – List all the existing mount points on the current appliance.

SYNOPSIS

`List [Type]`

DESCRIPTION

You can use the `List` command to list all the existing mount points on your appliance.

OPTIONS

`List [Type]`

List all the existing mount points on the current appliance. `[Type]` is an optional parameter that displays the mount points of specified type.

EXAMPLES

The following is an example output of the `List` command.

```
abc123.MountPoints> list
abc456:/storage on /mnt/remote/garry type nfs (rw,relatime,vers=3,rsize=
32768,wsiz=32768,namlen=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,
mountaddr=10.182.1.249,mountvers=3,mountport=695,mountproto=udp,local_lo
ck=none,addr=10.182.1.249)
```

Manage > MountPoints > Mount

Manage > MountPoints > Mount – Use to mount a remote NFS drive as a backup source.

SYNOPSIS

```
Mount RemotePath MountPoint [FileSystemType] [Options]
```

DESCRIPTION

Mount command is used to mount an NFS drive as a backup source.

OPTIONS

```
Mount RemotePath MountPoint [FileSystemType] [Options]
```

Use to mount a remote NFS device as a backup source. Use the parameters *RemotePath*, *MountPoint*, *[FileSystemType]*, and *[Options]* to specify the details of NFS drive. This command includes the following parameters:

RemotePath Provide the address of device or directory to be mounted. You should use the format `HOST:DIRECTORY` to write the device name.

MountPoint Provide the name of the local mount point where the device should be mounted. This appears as a subdirectory under `/mnt/remote`. After the command is run successfully, this subdirectory is created under `/mnt/remote`.

Note: An error may be displayed if the full directory path (example: `/tmp/garry`) is specified instead of just a mount point name(example: `garry`).

[FileSystemType] Identify the type of device to be mounted.

[Options] Specify comma-separated list of parameters to be passed to the appliance along with the `Mount` command. You can only use options specific for mounting the NFS drive.

EXAMPLES

The following is an example output when you run the `Mount` command to mount `garry`.

```
abc123.MountPoints> Mount abc456:/storage garry  
- [Info] Successfully mounted the requested source on '/mnt/remote/garry'.
```

The following is an example output when you list mount points.

```
abc123.MountPoints> list  
abc456:/storage on /mnt/remote/garry type nfs (rw,relatime,vers=3,rsize=  
32768,wsiz=32768,namlen=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,  
mountaddr=10.182.1.249,mountvers=3,mountport=695,mountproto=udp,local_lo  
ck=none,addr=10.182.1.249)
```

Manage > MountPoints > Unmount

Manage > MountPoints > Unmount – Used to unmount a mounted NFS drive.

SYNOPSIS

```
Unmount MountPoint [Force]
```

DESCRIPTION

Use the `Unmount` command to unmount a mounted NFS drive. If the directory name is specified correctly the following process takes place:

- The NFS is unmounted successfully.
- The directory is removed from the file system.
- In case the directory is on a nested path, only that directory is removed.

OPTIONS

```
Unmount MountPoint [Force]
```

Unmount a previously mounted NFS drive. *MountPoint* is the name of the local mount point that appears as a subdirectory where the NFS drive is mounted.

You can use the `Manage > Mountpoints > List` command to list and verify the existing mount points.

The following options are used to identify the NFS drive to be unmounted:

MountPoint Enter the name of the mount point. The mount point is a subdirectory under `/mnt/remote`. For example, `garry`.

Note: If the specified mount point is valid, it is un-mounted from the `/mnt/remote` directory. An error may be displayed if the full directory path (example: `/tmp/garry`) is specified instead of just a mount point name (example: `garry`).

[*Force*] Specify this parameter to unmount the NFS forcibly.

EXAMPLES

The following is an example output for un-mounting the mount point `garry`.

```
abc123.MountPoints> Unmount garry
- [Info] Deleting mount entry from configuration files.
```


- [Info] Umount the directory from system.
- [Info] Successfully unmount the request source from '/mnt/remote/garry'.

Main > Manage > NetBackup CLI commands

This appendix includes the following topics:

- [Manage > NetBackupCLI > Create](#)
- [Manage > NetBackupCLI > Delete](#)
- [Manage > NetBackupCLI > List](#)
- [Manage > NetBackupCLI > PasswordExpiry](#)

Manage > NetBackupCLI > Create

Manage > NetBackupCLI > Create – Create a NetBackup user account.

SYNOPSIS

Create *UserName*

DESCRIPTION

The `Create` command is used to create NetBackup user account.

OPTIONS

Create *UserName*

Create a NetBackup user account. Use the *UserName* parameter to define the user that you want to create.

Review the following password policy and create a password.

- At least eight characters are required.
- At least one lower case letter (a-z) and one number (0-9) are required.
- Dictionary words are not accepted.
- The last seven passwords cannot be reused.
- The new password cannot be similar to the current and previous passwords.

Manage > NetBackupCLI > Delete

Manage > NetBackupCLI > Delete – Delete a NetBackup user account.

SYNOPSIS

Delete *UserName*

DESCRIPTION

The `Delete` command is used to delete a NetBackup user account.

OPTIONS

Delete *UserName*

Use to delete a NetBackup user account. Use the *UserName* parameter to define the user that you want to delete.

Manage > NetBackupCLI > List

Manage > NetBackupCLI > List – View a list of NetBackup users.

SYNOPSIS

List

DESCRIPTION

List command is used to view a list of NetBackup users.

OPTIONS

List

Use to view a list of NetBackup users.

Manage > NetBackupCLI > PasswordExpiry

Manage > NetBackupCLI > PasswordExpiry – Manage the NetBackup command-line passwords.

SYNOPSIS

```
PasswordExpiry Age UserName Days
PasswordExpiry Now UserName
PasswordExpiry Show [UserName]
PasswordExpiry Warn UserName Days
```

DESCRIPTION

When you create a NetBackupCLI user account, you can manage the password of that account through the NetBackup Appliance Shell Menu. You have the ability to do the following:

- Set the age of the password in days, for one or more users.
- Force the expiration of a password for one or more users.
- Configure a warning of when a password is set to expire for one or more users.
- Show the current expiry password information of one or more users.

OPTIONS

```
PasswordExpiry Age UserName Days
```

Specify a maximum number of days that a password is valid.

Use the *Days* variable to set the number of days the password is valid. In addition, use the *UserName* variable to specify the user or users that you want this setting to apply. Enter `All` if you want this setting to apply to all users.

```
PasswordExpiry Now UserName
```

Force a password to expire immediately for one or more users.

Use the *UserName* variable to specify the user or users whose password is about to expire. Enter `All` if you want to expire the password for all users.

```
PasswordExpiry Show [UserName]
```

View the password expiry information.

Use the `[UserName]` variable to specify the user or users. Enter `All` if you want to expire the password for all users. You can also enter `Default` to view the default settings.

`PasswordExpiry Warn UserName Days`

Configure a warning period in which you receive a warning before the password expires. You can also configure one or more users to receive the warning.

Use the `Days` variable to set the number of days or warning before the password expires. In addition, you use the `UserName` variable to specify the user or users who receive the warning. Enter `All` if you want this setting to apply to all users. You can also enter `Default` to specify the default settings.

Main > Manage > OpenStorage commands

This appendix includes the following topics:

- [Manage > OpenStorage > Install](#)
- [Manage > OpenStorage > List](#)
- [Manage > OpenStorage > Readme](#)
- [Manage > OpenStorage > Share](#)
- [Manage > OpenStorage > Uninstall](#)

Manage > OpenStorage > Install

Manage > OpenStorage > Install – Use this command to install an OpenStorage plug-in

SYNOPSIS

```
Install plugin_name
```

DESCRIPTION

Before the installation of the OST the appliance performs the following steps:

1. Untars the `tar.gz` file and extract its contents.
2. Checks and verifies if the plug-in exists in the install directory.
3. Checks and verifies if the plug-in directory path is correct. The default path is `/usr/opensv/lib/ost-plugins`.
4. Checks if `nbrmms` is running and terminates it.

Note: The `nbrmms` process should be terminated for the installation to proceed. The installer exits if `nbrmms` does not terminate.

5. Copies `libstspi<vendor_name>.so` and `libstspi<vendor_name>MT.so` into a plug-in directory `/usr/opensv/lib/ost-plugins`

Note: If the plug-in already exists, you are prompted with the following message:
`A plugin already exists, do you want to proceed with the installation. Type Y to proceed.`

6. After the installation is completed, the appliance restarts the `nbrmms` process.

OPTIONS

```
Install plugin_name
```

Use this command to install the *plugin_name.tar.gz*.

EXAMPLES

The following online procedure is executed after you run the `Install` command.

```
abc123.OpenStorage> Install plugin_name.tar.gz
```

```
- [Info] Going to install the plugin. It will take several minutes to finish.
```

```
Welcome to the installation of plugin package plugin_name.tar.gz.
```

```
- [Info] Extracting the contents of the tar file      ok
```

```
- [Info] Terminating the nbrmms process before proceeding with the installation.  ok
```

```
- [Info] Executing the install script
```

```
- [Info] Install script exited successfully!
```

```
- [Info] Restarting nbrmms      ok
```

```
- [Info] Successfully installed the plugin package plugin_name.tar.gz
```

Manage > OpenStorage > List

Manage > OpenStorage > List – Use to list software information.

SYNOPSIS

List Available

List Installed

DESCRIPTION

This command displays all the installed OpenStorage plug-ins and their details.

OPTIONS

List Available

Use this command to list all the OST plug-ins that have been downloaded. The plug-ins are validated against their name and format. The valid plug-ins are listed.

List Installed

Use this command to list the OST plug-in that has been installed on the appliance.

EXAMPLES

The following example demonstrates the displayed output when you run the List Available command.

```
Validating the plugin plugin_name.tar.gz    ok
List of plugins downloaded on the appliance:
plugin_name.tar.gz
```

The following example demonstrates the displayed output when the List Installed command is run.

```
OpenStorage> List Installed
```

Details of the installed OpenStorage plugin:

Plugin Info:

Plugin Name: libstspiDataDomainMT.so

Prefix: DataDomain:
Label: Data Domain Plugin
Build Version: 11
Build Version Minor: 1
Operating Version: 11
Vendor Version: 2.4.0.0-246426

Plugin Name: libstspiQuantumMT.so
Prefix: Quantum
Label: Quantum OST plugin
Build Version: 11
Build Version Minor: 1
Operating Version: 11
Vendor Version: 2.6.0.2088 Quantum MT plugin

Manage > OpenStorage > Readme

Manage > OpenStorage > Readme – Use this command to view the instructions for installing the OpenStorage plug-ins.

SYNOPSIS

Readme

DESCRIPTION

The `Readme` command displays the instructions to install the OpenStorage plug-in.

OPTIONS

Use this command to view the instructions to install the OpenStorage plug-in.

EXAMPLES

The following example displays the instructions that are provided when you run the `Readme` command.

```
OpenStorage> readme
```

```
Plugin Readme  
=====
```

The following procedures explain how to copy an OpenStorage plugin on to the NetBackup 52xx appliance and install the plugin.

To copy the plugin from a local computer:

1. Login as the user 'admin' to the appliance.
2. Use the 'Share Open' command to open the NFS and CIFS shares so the appliance can receive the plugin.

For NFS: (nbuappliance:/inst/plugin/incoming)

For CIFS: (\\nbuappliance\incoming_plugins)

3. On the local computer, perform the following steps:

- a. Mount/Map the appropriate NFS/CIFS share.
For CIFS, you must map using the appliance
'admin' user's credentials.
 - b. Download the OpenStorage package from the
appropriate source.
 - c. Upload the package to the mounted share.
 - d. Unmap/Unmount the mounted share.
4. Use the 'Share Close' command to close the NFS and CIFS shares.
 5. Use the 'List Available' command to list the available packages.
Note the name of the plugin to install.

To install an OpenStorage plugin on the NetBackup 52xx:

1. Use the 'Install' command to install the plugin.

Use the name of the plugin that you noted in the procedure
above when you entered the 'List Available' command.

Manage > OpenStorage > Share

Manage > OpenStorage > Share – Use this command to share or to stop sharing directory for uploading plug-in.

SYNOPSIS

Share Open

Share Close

DESCRIPTION

The `Share Open` command enables you to share a directory for uploading the OST plug-in. You can then use the `Share Close` command to stop sharing the directory. This operation is accomplished by opening and closing the Network File System (NFS) and Common Internet File System (CIFS) protocol shares.

OPTIONS

Share Open

Use this command to share a directory.

Share Close

Use this command to stop sharing a directory.

EXAMPLES

The following example displays the output when you run the `Share Open` command.

```
OpenStorage> Share open
```

The CIFS share `\server_name\incoming_plugins`

and the NFS share `server_name:/inst/plugin/incoming`

have been opened on this appliance.

The following example displays the output when you run the `Share Close` command.

```
OpenStorage> Share close
```

The plugin share closed successfully.

Manage > OpenStorage > Uninstall

Manage > OpenStorage > Uninstall – Use this command to uninstall the OpenStorage plug-in

SYNOPSIS

```
Uninstall
```

DESCRIPTION

The OST plug-ins can be uninstalled by deleting the shared libraries in `/usr/open/lib/ost-plugins` directory.

OPTIONS

```
Uninstall
```

Use this command to uninstall the plug-in *plugin_name.tar.gz* that is currently installed on the system.

EXAMPLES

The following example demonstrates the process that you need to follow when you run the `Uninstall` command.

```
OpenStorage> Uninstall plugin_name.tar.gz
```

Displays the following message:

```
- [Info] Checking for the installed OpenStorage plugin ...

>> The plugin package plugin_name.tar.gz is currently installed
on the system. Do you want to continue uninstalling it? (yes/no) yes

>> There might be some existing backups on the storage server.

Are you sure you want to continue uninstalling the plugin? (yes/no) yes

- [Info] Uninstalling the plugin package plugin_name.tar.gz ..... ok

- [Info] Successfully uninstalled the plugin package plugin_name.tar.gz
```


Main > Manage > Software commands

This appendix includes the following topics:

- [Manage > Software > Cancel](#)
- [Manage > Software > Delete](#)
- [Manage > Software > Download](#)
- [Manage > Software > DownloadProgress](#)
- [Manage > Software > Firmware](#)
- [Manage > Software > Install](#)
- [Manage > Software > List](#)
- [Manage > Software > Readme](#)
- [Manage > Software > Rollback](#)
- [Manage > Software > Share](#)
- [Manage > Software > UpgradeStatus](#)
- [Manage > Software > VxUpdate](#)

Manage > Software > Cancel

Manage > Software > Cancel – Cancel the download process of a software update or the software patch, which can be in any of these installation stages - downloading or stopped or finished, or postcheck.

SYNOPSIS

```
Cancel update_name
```

DESCRIPTION

Use this command to cancel a patch download in one of the following stages:

- Downloading - The software update is in the process of being downloaded.
- Stopped - The downloading process has stopped abruptly; therefore the download cannot be completed.
- Finished - The software update is downloaded completely. However, you must run the `Software > List Downloaded` command to view the software updates that are available for installation.
- Postcheck - During downloading, the software update splits into several files. Once the split files are downloaded, they need to be merged into the software update. The merging is termed as Postcheck.

OPTIONS

```
Cancel update_name
```

This command cancels downloading of patch. Here, *update_name* is the name of the software patch update.

Manage > Software > Delete

Manage > Software > Delete – Delete a software update.

SYNOPSIS

```
Delete update_name
```

DESCRIPTION

You can use this command to delete a specific software release update, sometimes referred to as a patch. Use the `Main_Menu > Manage > Software > List Downloaded` command to obtain the list of software release updates that are downloaded.

OPTIONS

```
Delete update_name
```

Delete a specific release update. Here *update_name* is the specific name of the update that you want to delete.

Manage > Software > Download

Manage > Software > Download – Download a software update.

SYNOPSIS

Download *update_name*

DESCRIPTION

You can use this command to download a specific release update.

OPTIONS

Download *update_name*

Download a specific update, where *update_name* is the name of the update that you want to download.

Manage > Software > DownloadProgress

Manage > Software > DownloadProgress – Show the progress of an online patch download.

SYNOPSIS

```
DownloadProgress
```

DESCRIPTION

Use this command to display the download progress of a software patch.

OPTIONS

```
DownloadProgress
```

Display the download progress of a software patch.

Manage > Software > Firmware

Manage > Software > Firmware – Check firmware status and update firmware for hardware components.

SYNOPSIS

Firmware Status

Firmware Update

DESCRIPTION

Use the `Status` command to obtain a firmware status of hardware components such as the RAID controller, BIOS, hard disk drives, PCIe cards, and Expansion I/O module.

Note: Starting with appliance software version 3.2, this command is no longer supported. To update the appliance firmware, refer to the following article for details about downloading and using the firmware update tool:

https://www.veritas.com/support/en_US/article.100046032

Use the `Update` command to update the firmware.

A firmware update must be performed during a maintenance window as a system restart is required. All appliance operations must be turned off before starting a firmware update. Administrators should plan accordingly.

Manage > Software > Install

Manage > Software > Install – Use to install an EEB or a software release update.

SYNOPSIS

```
Install update_name
```

DESCRIPTION

Use this command to install a new or an existing software update or an engineering binary (EEB) to an appliance that you designate.

To use this command you must know the name of the software update or EEB that you want to install. To see a list of the software updates and EEB that are available for you to install, run `Software > List AvailablePatch` command. This command checks the Veritas site for the latest software update. Once you find the software update or EEB that you want to install, you must run the `Software > Download update_name` command, where *update_name* is the name of the software update.

After you have downloaded the software update, you can now run the `Software > Install update_name` command.

OPTIONS

```
Install update_name
```

Install a software release update.

update_name is the name of the update that you want to install.

Manage > Software > List

Manage > Software > List – Lists the available patch information.

SYNOPSIS

```
List AddOns  
List AvailablePatch  
List Details All  
List Details Base  
List Downloaded  
List Downloaded Details [update_name]  
List EEBs  
List Version
```

DESCRIPTION

This command shows the patches that have been applied to a particular appliance. In addition, you can use this command to show the patches that are available for installation for a particular appliance.

OPTIONS

```
List AddOns  
    Use this command to list software add-ons that are installed.  
  
List AvailablePatch  
    Use this command to check the Veritas site for any software updates that are available.  
  
List Details All  
    Use this command to view all of the release updates that are available.  
  
List Details Base  
    Use this command to view all the release updates that were applied to your appliance during the factory installation.  
  
List Downloaded  
    List downloaded software updates.
```


List Downloaded Details *update_name*

List the detailed information of a downloaded software update.

List EEBs

Show a detailed listing of all of the factory-installed Emergency Engineering Binaries (EEBs).

List Version

Use this command to view the version of your appliance.

Manage > Software > Readme

Manage > Software > Readme – Defines the NetBackup patch process.

SYNOPSIS

Readme

DESCRIPTION

This command defines the patch process for the appliance.

OPTIONS

Readme

This command defines the patch process for the appliance.

EXAMPLES

This command contains the following patch information.

Patch Readme

=====

The following procedures explain how to copy a software release update on to the NetBackup Appliance and install the update.

To download software update directly from the Veritas Support Web Site:

1. Use the 'List AvailablePatch' command to look for the latest release update
2. Use the 'Download' command to download the release update.
3. Use the 'List Downloaded' command to list all of the downloaded release updates. Note the name of the update to install.

To upload a software update from a local computer:

1. Login as the user 'admin' to the appliance.
2. Use the 'Share Open' command to open the NFS and CIFS shares so the appliance can receive the release updates.
For NFS: (abc123:/inst/patch/incoming)
For CIFS: (\\abc123\incoming_patches)
3. On the local computer, perform the following steps:
 - a. Mount/Map the appropriate NFS/CIFS share.
For CIFS, you must map using the appliance 'admin' user's credentials.
 - b. Download the release update from the Veritas Support Web site.
 - c. Unzip the release update and review the README file in the zip.

- d. Upload the unzipped release update to the mounted share.
 - e. Unmap/Unmount the mounted share.
4. Use the 'Share Close' command to close the NFS and CIFS shares.
 5. Use the 'List Downloaded' command to list all of the downloaded release updates. Note the name of the update to install.

To install a release update on the NetBackup Appliance:

1. Use the 'Install' command to install the release update.
Use the name of the release update that you noted in the procedures above when you entered the 'List Downloaded' command.

For more detailed information about this process, see the *NetBackup appliance Administrator's Guide*.

Manage > Software > Rollback

Manage > Software > Rollback – Rollback a specific EEB.

SYNOPSIS

```
Rollback eeb_name.rpm
```

DESCRIPTION

Use this command to rollback any Emergency Engineering Binaries (EEBs) that are installed on your appliance. You can use the `List` commands to view the software version and all installed EEBs. You can then specify which EEB you want to roll back.

You can only specify one EEB at a time with this command. However, you can use this command multiple times to roll back as many installed EEBs as you want.

OPTIONS

```
Rollback eeb_name.rpm
```

Rollback a specified EEB, where *eeb_name.rpm* is the name of the EEB to rollback.

For example, run the following command to roll back EEB ABC5200_EEB_1-1.2.3.4:

```
Software> Rollback ABC5200_EEB_1-1.2.3.4.rpm
```

Note: You must include the `.rpm` extension when you enter the EEB name.

Manage > Software > Share

Manage > Software > Share – Share or unshare a directory for incoming patches

SYNOPSIS

Share Open

Share Close

DESCRIPTION

You can use this command to share or not share the directory that is used to receive incoming patches for your appliance. This operation is accomplished by opening and closing the Network File System (NFS) and Common Internet File System (CIFS) protocol shares.

OPTIONS

Share Open

Open the NFS and the CIFS shares for the directory that receives incoming patches.

For CIFS, you must map using the appliance "admin" user's credentials.

Share Close

Close the NFS and the CIFS shares for the directory that receives incoming patches.

Manage > Software > UpgradeStatus

Manage > Software > UpgradeStatus – View the version and the software upgrade status.

SYNOPSIS

UpgradeStatus

DESCRIPTION

This command displays the version and the upgrade status of the appliance.

OPTIONS

UpgradeStatus

View the version and the upgrade status of the appliance.

EXAMPLES

The following is an example output of the Main > Manage > Software > UpgradeStatus command:

```
abc123.Software> UpgradeStatus
```

```
Command backup_system_files is completed. The upgrade is 21% completed.
```

Manage > Software > VxUpdate

Manage > Software > VxUpdate – Manage the packages in the VxUpdate repository.

SYNOPSIS

VxUpdate

DESCRIPTION

This command lets you manage the packages in the VxUpdate repository.

OPTIONS

AddPkg

Add VxUpdate packages to the repository. Supported packages must be Veritas signed and include VxUpdate client packages and NetBackup EEB packages.

DelPkg

Delete packages from the repository.

ListPkgs

See a list of the packages that currently reside in the repository.

ShowPkgDetails

See the details of an individual package in the repository.

ViewAllPkgs

See the details of all packages in the repository.

EXAMPLES

The following shows an example of the output for the VxUpdate AddPkg command:

```
n4-h23.VxUpdate> AddPkg vxupdate_nbclient_8.2_suse_ppc64le.sja
Adding package to the repository. This may take a few minutes...
Successfully added deployment package ID: 1 to the repository.
```

The following shows an example of the output for the VxUpdate DelPkg command:

```
n4-h23.VxUpdate> DelPkg 1
Package ID 1 has been deleted from the repository.
```

The following shows an example of the output for the VxUpdate ListPkgs command:

```
n4-h23.VxUpdate> ListPkgs
```

ID	Type	Version	OS	File Name
1	client	8.2	suse_ppc64le	vxupdate_nbclient_8.2_suse_ppc64le.sja

The following shows an example of the output for the `VxUpdate ShowPkgDetails` command:

```
n4-h23.VxUpdate> ShowPkgDetails 1
```

```
Package ID: 1
Package File Name: vxupdate_nbclient_8.2_suse_ppc64le.sja
Package Type: client
Operating System: suse_ppc64le
Release Version: 8.2
Installables: nbclient_8.2
Package Size: 95.02 MB
Created Date/Time (UTC): 2019-06-01 03:04:33
```

The following shows an example of the output for the `VxUpdate ViewAllPkgs` command:

Main > Manage > Storage commands

This appendix includes the following topics:

- [Manage > Storage > Add](#)
- [Manage > Storage > Create](#)
- [Manage > Storage > Delete](#)
- [Manage > Storage > Edit](#)
- [Manage > Storage > Monitor](#)
- [Manage > Storage > Move](#)
- [Manage > Storage > Remove](#)
- [Manage > Storage > Resize](#)
- [Manage > Storage > Scan](#)
- [Manage > Storage > Show](#)
- [Manage > Storage > Erase](#)

Manage > Storage > Add

Manage > Storage > Add – Use this command to add a new disk. It also displays the disks that are in a `New Available` state and can be added.

SYNOPSIS

```
Add [Disk ID]
```

DESCRIPTION

This command enables you to add a storage disk. The total capacity of the disk gets added to the `Unallocated` space.

OPTIONS

```
Add [DiskID]
```

Use to add storage disk, where `[DiskID]` is the ID of the disk. The Disk ID appears when you run the `Show Disk` command. For example, `S0001FB3BC00000A62501ABDA009`. After a disk is added, the total capacity of the disk gets added to the `Unallocated` space.

Note: If the disk ID is not specified with the `Add` command, the appliance lists the disks that can be added. Only a disk in `New Available` state can be added.

EXAMPLES

The following is an example of the information that is displayed when you run the `Add [DiskID]` command.

```
Storage > Add S0001FB3BC00000A62501ABDA009
- Performing sanity check on disks and partitions... (5 mins approx)
- Checking whether storage configuration exists
- Checking the state of the 'S0001FB3BC00000A62501ABDA009' disk
- Initializing the 'S0001FB3BC00000A62501ABDA009' disk
- Configuring the S0001FB3BC00000A62501ABDA009 disk storage...
- Adding the 'S0001FB3BC00000A62501ABDA009' disk space to 'Unallocated' space
- Succeeded
```

Manage > Storage > Create

Manage > Storage > Create—Use this command to create a new standard share, optimized share, or optimized share reserve.

SYNOPSIS

Create Share Standard

Create Share Optimized

Create OptimizedShareReserve

DESCRIPTION

This command exists under the Main > Manage > Storage view. The Create command lets you create the following:

- Standard Share
- Optimized Share
- Optimized Share Reserve

OPTIONS

Create Share Standard

Use this command to create a standard share. A wizard guides you through the creation process.

Create Share Optimized

Use this command to create an optimized share. A wizard guides you through the creation process.

Note: If you have not created the optimized share reserve, the command prompts you to create it before you create the first optimized share.

Create OptimizedShareReserve

Use this command to create the optimized share reserve.

SEE ALSO

See [“About the commands under the Manage view”](#) on page 16.

Manage > Storage > Delete

Manage > Storage > Delete—Use this command to delete existing standard shares, optimized shares, or optimized share reserves.

SYNOPSIS

Delete Share *ShareName*

Delete OptimizedShareReserve

DESCRIPTION

This command exists under the Main > Manage > Storage view. The Delete command lets you delete the following:

- Standard Shares
- Optimized Shares
- Optimized Share Reserve

OPTIONS

Delete Share *ShareName*

Use this command to delete a standard share or optimized share.

ShareName defines the name of the share you want to delete.

Delete OptimizedShareReserve

Use this command to delete the optimized share reserve.

Note: All optimized shares must be deleted before you can delete the optimized share reserve.

Manage > Storage > Edit

Manage > Storage > Edit – Use this command to edit a share.

SYNOPSIS

```
Edit Share Description ShareName  
Edit Share Clients Add ShareName  
Edit Share Clients Update ShareName  
Edit Share Clients Delete ShareName
```

DESCRIPTION

This command exists under the Main > Manage > Storage view. The Edit Share command lets you edit the details of a share. You can change the description and add, modify, or delete clients.

OPTIONS

```
Edit Share Description ShareName  
    This command edits the description of a previously created share. You must  
    enter a value for ShareName to edit.  
Edit Share Clients Add ShareName  
    This command enables you to add additional clients to a previously created  
    share. You must enter a value for ShareName to add clients.  
Edit Share Clients Update ShareName  
    This command enables you to update existing clients of a previously created  
    share. You must enter a value for ShareName to update clients.  
Edit Share Clients Delete ShareName  
    This command enables you to delete the clients of a previously created share.  
    You must enter a value for ShareName to delete clients.
```

EXAMPLES

The following example demonstrates how to change the description of a share.

```
Manage > Storage > Edit Share Description share_1  
- [Info] Old Description :  
    "My Test Share description"
```

```
>> Enter the New Description ( Enter to keep old description ) : My New Test Share description
- [Info] Successfully edited description of share 'share_1'.
```

The following example demonstrates how to add clients to a share.

```
Manage > Storage > Edit Share Clients Add share_1
- [Info] List of Oracle server clients that can access this share
    hostA (rw, root_squash,secure)
    10.182.0.2 (rw, root_squash, anonuid=1024, anongid=1024)
>> Enter comma-separated list of Oracle server clients you would like to add : hostC, HostD
>> Enter comma-separated list of NFS export options for the Oracle clients added above.
    The following options are supported:
        ro, rw, no_root_squash, root_squash, all_squash, anonuid, anongid , secure, insecure
    For detailed information about the NFS export command options, refer to
        NetBackup Appliance Administrator's guide.
>> Export options for 'hostC' (rw, no_root_squash, secure) :
    rw, root_squash, anonuid=1024, anongid=1024
>> Export options for 'hostD' (rw, no_root_squash, insecure) :
    rw, no_root_squash, secure

- [Info] Summary of clients:
    hostA (rw, root_squash,secure)
    10.182.0.2 (rw, root_squash, anonuid=1024, anongid=1024)
    hostC (rw, root_squash, anonuid=1024, anongid=1024)
    hostD (rw, root_squash, anonuid=1024, anongid=1024)

- [Info] Successfully edited clients of share 'share_1'.
```

The following example demonstrates how to update the clients of a share.

```
Manage > Storage > Edit Share Clients Update share_1
- [Info] List of Oracle server clients that can access this share
    hostA (rw, root_squash,secure)
    10.182.0.2 (rw, root_squash, anonuid=1024, anongid=1024)
>> Enter comma-separated list of Oracle server clients you would like to update : hostA
>> Enter comma-separated list of NFS export options for the Oracle clients added above.
    The following options are supported:
        ro, rw, no_root_squash, root_squash, all_squash, anonuid, anongid , secure, insecure
    For detailed information about the NFS export command options, refer to
        NetBackup Appliance Administrator's guide.
>> Export options for 'hostA' (rw, root_squash, anonuid=1024, anongid=1024) :
    rw, no_root_squash, secure
- [Info] Summary of clients:
    hostA (rw, no_root_squash, secure)
```

```
10.182.0.2 (rw, root_squash, anonuid=1024, anongid=1024)
- [Info] Successfully updated clients of share 'share_1'.
```

The following example demonstrates how to delete clients from a share.

```
Manage > Storage > Edit Share Clients Delete share_1
- [Info] List of Oracle server clients that can access this share
    hostA (rw, root_squash,secure)
    10.182.0.2 (rw, root_squash, anonuid=1024, anongid=1024)
>> Enter comma-separated list of Oracle server clients you would like to delete : hostA
- [Info] Summary of clients:
    10.182.0.2 (rw, root_squash, anonuid=1024, anongid=1024)
- [Info] Successfully deleted clients of share 'share_1'.
```

Manage > Storage > Monitor

Manage > Storage > Monitor – Use to monitor storage tasks.

SYNOPSIS

Monitor

DESCRIPTION

This command enables you to monitor the current status of storage tasks currently in progress.

OPTIONS

Monitor

Use to monitor the current status of storage tasks currently in progress.

EXAMPLES

The following example displays the initiated procedure when you run the `Monitor` command during a resize operation.

```
Storage > Monitor
```

```
Press 'CTRL + C' to quit.
```

```
Resizing the AdvancedDisk storage partition...
```

```
The estimated time to resize the partition is 2 to 5 minutes.
```

```
Stopping NetBackup processes... (2 mins approx)
```


Manage > Storage > Move

Manage > Storage > Move – Use to move storage partition from one disk to another.

SYNOPSIS

```
Move Partition SourceDiskID TargetDiskID [Size] [Unit]
```

DESCRIPTION

This command lets you move a storage partition from one disk to another.

OPTIONS

```
Move Partition SourceDiskID TargetDiskID [Size] [Unit]
```

Use to move a partition from one storage disk to another, where:

- *Partition* refers to the storage partition like AdvancedDisk, Configuration, MSDP etc.
The NetBackup Catalog partition cannot be moved.
Optimized shares cannot be moved.
- *SourceDiskID* refers to the disk ID of the source disk. Use `Show Distribution` to view the disk ID and the partitions on it. A sample disk ID is `S0001FB362501ABDA00000009se`
- *TargetDiskID* refers to the disk ID of the target disk. Use `Show Distribution` to view the disk ID and the partitions on it. A sample disk ID is `S0001FB362501ABDA00000009se`.
- *[Size]* refers to the partition size. Partition size must be greater than 0. If you specify a partition size that is greater than the actual partition size, the appliance moves the whole partition. The default value is `[1]`.
- *[Unit]* refers to unit size (GB/TB/PB). The default value is `[PB]`.

Examples

The following example displays the initiated procedure when you run the `Move` command.

```
Storage > Move AdvancedDisk S0001FB362501ABDA00000009se
S2301FB3BC00540A62501ABDA00000009se 5 GB
- [Info] Performing sanity check on disks and partitions...(5 mins approx)
- [Warning] Do not reboot the appliance while the partition move is in
```

```
progress.  
- [Info] The estimated time to move the partition can range from  
    0 hours, 1 minutes to 0 hours, 2 minutes depending on the  
    system load.  
    The greater the system load the longer it takes to complete the  
    move operation.  
>> Do you want to continue? (yes/no) yes  
    Moving part '1/1' disks...    Done  
- [Warning] No recipients are configured to receive software  
    notifications.  
    Use 'Settings->Alerts->Email Software Add' command to configure  
    the appropriate Email address.  
- [Info] Succeeded.
```

Manage > Storage > Remove

Manage > Storage > Remove – Use this command to remove a storage disk.

SYNOPSIS

Remove *DiskID*

DESCRIPTION

The command removes a storage disk and changes the state to `New Available`. You can remove disks with status **In Use** that do not contain any partitions. You can also remove disks with status **Foreign**.

If the disk has a **In Use** status and has partitions, you must first move the partitions to other disks. Use the `Show Distribution` command to see the partitions that are on the disk and then use the `Move` command to move the partitions to another disk. Once the partitions have been moved, try removing the disk again.

A disk with status **Foreign** may have data. If you try to remove such a disk, any data present on it is also removed.

OPTIONS

Remove *DiskID*

Use to remove an existing disk and changes the state to `New Available`. Retrieve the disk ID by running the `Show Disk` command. For example, a sample Disk ID is `S0001FB3BC00000A62501ABDA0000009se`.

Warning: After removing a storage disk, if the appliance reboots it can hang and display the **Boot splash** screen. Press the `ESC` key to proceed. The RAID controller firmware provides step-by-step instructions to help you boot the appliance.

EXAMPLES

The following is an example of the information that is displayed when you run the `Remove Disk ID` command.

```
Storage > Remove S000162501ABDA000009se
- [Info] Performing sanity check on disks and partitions...(5 mins approx)
- [Info] Checking the type of 'S000162501ABDA000009se' disk...
- [Info] Checking the state of 'S000162501ABDA000009se' disk...
```

- [Info] Removing the 'S000162501ABDA000009se' disk space from 'Unallocated'...
- [Info] Succeeded.

The following output displays the updated status of the removed storage expansion unit after using the `Show Disk` command.

Storage> Show Disk

Disk ID	Type	Total	Unallocated	Status

SE0000000000000000000se	System	150 GB	-	In Use
S0001FB3BC00A0000009se	Base	150 GB	33.968 GB	In Use
S000162501ABDA000009se	Expansion	35 TB	-	New Available

You cannot issue commands for disks with the status 'n/a'.

Manage > Storage > Resize

Manage > Storage > Resize – Use to manage the size of a selected partition type of storage.

SYNOPSIS

Resize Partition Size Unit

DESCRIPTION

This command enables you to create, resize, or delete the storage partitions in your appliance. The `Resize` command can be used for a single storage partition at a time. You can use this command to resize the storage capacity of a partition to a higher or a lower value. The disk storage cannot be expanded to a size that is greater than the unallocated space.

Note: Shares can only be resized with this command. They cannot be created or deleted. Use the Create and Delete commands to create and delete shares.

Review the following considerations:

- You can create a partition using `Resize` only if the appliance is configured as a master or a media server.
- You can resize a partition to a higher or lower value depending on the type of partition. The size is expanded by using the unallocated space.
- You can delete a partition using `Resize` only if the appliance is in a factory state (when it is not configured as a master or media server).

Review the "Resizing a storage partition" topic in the Administrator's Guide before resizing a partition.

An informational message like the following is displayed when you resize a partition:

```
The estimated time to resize the partition can range from
0 hours, 2 minutes to 0 hours, 5 minutes depending on the
system load. The greater the system load the longer it takes
to complete the resize operation.
```

OPTIONS

Resize Partition Size Unit

Use to resize the storage partitions, where:

- *Partition* refers to the name of the partition like AdvancedDisk, Catalog, Configuration, MSDP, etc.
- *Size* refers to the size to which you want to resize the partition.
- *Unit* refers to the unit for resizing the partition in (GB/TB/PB).

EXAMPLES

The following example displays the initiated procedure when you run the `Resize` command.

```
Storage > Resize AdvancedDisk 1 TB
- [Info] Performing sanity check on disks and partitions...(5 mins approx)
- [Info] The estimated time to resize the partition can range from
0 hours, 2 minutes to 0 hours, 5 minutes depending on the system load.
The greater the system load the longer it takes to complete the
resize operation.

Do you want to continue? (yes/no) yes
- [Info] Shrinking the 'AdvancedDisk' storage partition...
- [Warning] No recipients are configured to receive software notifications.
Use Main > Settings > Email Software Add command to configure the
appropriate email address.
- [Info] Succeeded.
```

Manage > Storage > Scan

Manage > Storage > Scan – Use this command to refresh the storage disks and devices information.

SYNOPSIS

Scan

DESCRIPTION

This command enables you to refresh the storage disks and devices information.

Note: Whenever a storage device is connected or disconnected, use this command to detect the storage device, or refresh its status. If the disks of the connected storage device are in a foreign state, import the RAID group, and run the `Scan` command. If the `Scan` command does not display the updated storage device information, then restart the appliance to refresh the storage device information.

OPTIONS

Scan

Use to refresh the storage disks and devices information.

EXAMPLES

The following example displays the initiated procedure when you run the `Scan` command.

```
Storage > Scan
- [Info] Performing sanity check on disks and partitions...(5 mins approx)
- [Info] The Scan operation can take up to 15 minutes to complete.
- [Info] Initiating refresh of the storage devices...
- [Info] Succeeded.
```

NOTE: If you perform a 'Main-Manage-Storage Show Disk' command and the device information does not appear in the output, verify if the disk drives are in a foreign state. If the disk drives are in foreign state, import them and then perform a 'Main > Manage > Storage Scan' operation to refresh the device information. The device information may appear properly.

If the device information still does not appear, then restart the appliance to refresh the device information.

For 53xx appliances, the connected devices are scanned and the following output may be displayed:

```
Storage> Scan
- [Info] Performing sanity check on disks and partitions... (5 mins approx)
- [Info] The scan operation can take up to 15 minutes to complete.
- [Info] Refreshing the storage devices...
- [Info] Created 14 new disks (RAID groups) on External Storage.
- [Info] Succeeded.

- [Info] The new disks are being initialized. The disk initialization
happens in the background and may take up to 56 hours depending on the
system load. You can continue to use the appliance during this time.
However, if one or more of the new disks are used by partitions during
the disk initialization process, the performance of backup and restore
operations on the specific disks degrades by up to 30%.
```

NOTE: If you run the 'Manage->Storage->Show Disk' command and the device information does not appear in the output, run the 'Manage->Storage->Scan' to import and refresh the device information. If the device information still does not appear, restart the appliance to refresh the device information.

Manage > Storage > Show

Manage > Storage > Show – View NetBackup storage information.

SYNOPSIS

Show ALL

Show Disk

Show Distribution

Show Partition [Info] [PartitionType] [Name]

DESCRIPTION

This command enables you to view the storage capacity and parameters of the storage devices and partitions within your appliance.

Note: The Available and Used Size values displayed for the Media Server Deduplication Pool (MSDP) partition on the **Manage > Storage > Partitions** page or by using the **Manage > Storage > Show** command on the NetBackup appliance may not be the full space available or used by the MSDP partition. This is because space is reserved by the file system and also by MSDP. The file system reserves space for its own use. In addition, MSDP reserves 4 percent of the storage space for the deduplication database and transaction logs.

Check the MSDP disk pool sizes from the NetBackup Administration Console to obtain the MSDP statistics.

OPTIONS

Show All

This command shows all of the storage information.

Show Disk

This command shows the storage disk ID, type, capacity, unallocated space, and status.

Show Distribution

This command shows the storage distribution of each partition on the disk.

Show Partition [Info] [PartitionType] [Name]

Shows the storage partition information. You can specify the following three options:

Parameter 1 - [Info]

Specifies whether to view the usage information, the disk pool and storage unit configuration, or to view both. The available options are `ALL`, `Configuration`, and `Usage`. The default value is `ALL`.

Parameter 2 - [PartitionType]

Specifies the partition type. The available options are `ALL`, `AdvancedDisk`, `Configuration`, `MSDP`, `MSDPCatalog`, `Share`. The default value is `ALL`.

Parameter 3 - [Name]

Specifies the numerical name of a partition. For example, '0'. You can find the partition name in the `Show All` output. The default value is `ALL`, which displays information of all partitions of the specified type.

For example, to view the storage unit and disk pool configuration for all of MSDP partitions, run the following command:

Show Partition Configuration MSDP ALL

To view the usage information of all the partitions, run the following command:

Show Partition Usage ALL ALL

EXAMPLES

The following is an example output of the `Show Partition Configuration MSDP ALL` command:

```
MSDP
-----
Disk Pool (DP)   | Storage Unit (STU)
-----
dp_disk_abc123  | stu_disk_abc123
```

Manage > Storage > Erase

Manage > Storage > Erase – Used to manage the non-certified disk erasure process.

SYNOPSIS

Erase Configure

Erase Show

Erase Abort

DESCRIPTION

The non-certified disk erasure enables you to erase any storage disks on the appliance. When you erase a storage disk, all the data stored on the disk is destroyed and cannot be recovered.

The command enables you to manage the non-certified disk erasure process as follows:

- Configure disk erasure to erase one or more disks at a time. You can specify a pass algorithm for overwriting the data on the disk.
For more information about the pass algorithm, see the *NetBackup Appliance Administrator's Guide*.
- View disk erasure tasks in progress. You can also view the disk erasure history for each storage disk on the appliance.
- Abort the disk erasure operation.

OPTIONS

Erase Configure

Configure the disk erasure to erase one or more disk at a time. The command shows relevant information such as disk ID, storage shelf location, and storage partition distribution to help you determine which disks to erase.

Configure disk erasure to erase all the disks on the appliance shared storage. This command requires you to enter the pass algorithm to be used. The available options are 1, 3, and 7.

This command requires you to do the following in two steps.

1. Enter your selection of storage disks to erase.
2. Enter the pass algorithm to be used. The available options are 1, 3, and 7.

Erase Show

View the disk erasure tasks in progress. You can also view the disk erasure history for each storage disk on the appliance.

Erase Abort

Abort the disk erasure operation for a disk.

Aborting a disk erasure operation results in the corruption of all data on the disk. Once the data is corrupted, it cannot be recovered.

When you are prompted, enter the task ID that corresponds to the disk for which you want to abort the disk erasure operation. Use a comma-separated list if you want to abort multiple tasks.

Note: When you abort a disk erasure operation, any erasure progress on the disk is lost. You must configure disk erasure again to erase the disk.

Main > Manage > Tapes commands

This appendix includes the following topics:

- [Manage > Tapes > Cleaning](#)
- [Manage > Tapes > Delete](#)
- [Manage > Tapes > Eject](#)
- [Manage > Tapes > Freeze](#)
- [Manage > Tapes > Inventory](#)
- [Manage > Tapes > List](#)
- [Manage > Tapes > ListNetBackupMedia](#)
- [Manage > Tapes > Suspend](#)
- [Manage > Tapes > Unfreeze](#)
- [Manage > Tapes > Unsuspend](#)

Manage > Tapes > Cleaning

Manage > Tapes > Cleaning – Designate a tape as the cleaning tape.

SYNOPSIS

Cleaning *mediaid*

DESCRIPTION

Use this command to designate which tape in a tape library is the cleaning tape.

OPTIONS

Cleaning *mediaid*

Use to indicate which tape is the cleaning tape.

mediaid is the media identifier.

Manage > Tapes > Delete

Manage > Tapes > Delete – Delete media from a NetBackup database.

SYNOPSIS

Delete *mediaid*

DESCRIPTION

Use this command to identify a piece of media to delete from a NetBackup database.

OPTIONS

Delete *mediaid*

Use to delete media from a NetBackup database.

mediaid is the media identifier.

Manage > Tapes > Eject

Manage > Tapes > Eject – Eject media from a tape library.

SYNOPSIS

`Eject mediaid`

DESCRIPTION

Use this command to identify and eject media from a tape library.

OPTIONS

`Eject mediaid`

Use to eject media from a tape library.

mediaid is the media identifier.

Manage > Tapes > Freeze

Manage > Tapes > Freeze – Freeze media in a NetBackup database.

SYNOPSIS

`Freeze mediaid`

DESCRIPTION

Use this command to select a piece of media to freeze in a NetBackup database.

OPTIONS

`Freeze mediaid`

Use to freeze media in a NetBackup database.

mediaid is the media identifier.

Manage > Tapes > Inventory

`Manage > Tapes > Inventory` – Inventory all of the libraries for the volumes that have been added or removed.

SYNOPSIS

`Inventory`

DESCRIPTION

Use this command to inventory all of the libraries for the volumes that have been added or removed.

OPTIONS

`Inventory`

Inventory all libraries for added or removed volumes.

Manage > Tapes > List

Manage > Tapes > List – Show a list of the media.

SYNOPSIS

List

DESCRIPTION

Use this command to list the media. This command provides the following types of information about the media:

- Media ID
- Media type
- Robot type
- Robot number
- Robot slot
- Side/face
- Optical partner
- Number of mounts and cleanings
- Last mount time

OPTIONS

List

Lists the media.

Manage > Tapes > ListNetBackupMedia

Manage > Tapes > ListNetBackupMedia – Show a list of the media that NetBackup uses.

SYNOPSIS

ListNetBackupMedia

DESCRIPTION

Use this command to show a list of the media that NetBackup uses.

OPTIONS

ListNetBackupMedia

List the media that NetBackup uses.

Manage > Tapes > Suspend

Manage > Tapes > Suspend – Suspend media in a NetBackup database.

SYNOPSIS

`Suspend mediaid`

DESCRIPTION

Use this command to select and suspend media in a NetBackup database.

OPTIONS

`suspend mediaid`

Use to suspend media in a NetBackup database.

mediaid is the media identifier.

Manage > Tapes > Unfreeze

Manage > Tapes > Unfreeze – Unfreeze the media that has been frozen in a NetBackup database.

SYNOPSIS

```
Unfreeze mediaid
```

DESCRIPTION

Use this command to unfreeze the media that has been frozen in a NetBackup database.

OPTIONS

```
Unfreeze mediaid
```

Unfreeze the frozen media in a NetBackup database.

mediaid is the media identifier.

Manage > Tapes > Unsuspend

Manage > Tapes > Unsuspend – Unsuspend the media that has been suspended in a NetBackup database.

SYNOPSIS

```
Unsuspend mediaid
```

DESCRIPTION

Use this command to unsuspend the media that had been suspended in a NetBackup database.

OPTIONS

```
Unsuspend mediaid
```

Unsuspend media in a NetBackup database.

mediaid is the media identifier.

Main > Manage > Certificates commands

This appendix includes the following topics:

- [Manage > Certificates > Generate](#)
- [Manage > Certificates > Delete](#)

Manage > Certificates > Generate

Manage > Certificates > Generate – Use the Generate command to generate and download a certificate for a vCenter or SCVMM client.

SYNOPSIS

Generate *hostname*

DESCRIPTION

Use the Generate command to create new certificates for vCenter or SCVMM clients on the appliance. After the certificate has been generated, it is downloaded to the following location:

`/usr/openv/var/global/wsl/credentials/clients/hostname.zip`

OPTIONS

Generate *hostname*

Use to generate a certificate for the NetBackup client. Enter the client hostname for which you want to generate a certificate.

Manage > Certificates > Delete

Manage > Certificates > Delete – Delete an existing certificate.

SYNOPSIS

`Delete hostname`

DESCRIPTION

You can use the `Delete` command to delete an existing certificate for a vCenter or SCVMM client on the appliance.

OPTIONS

`Delete hostname`

Delete a damaged certificate. Specify a client hostname that you want to delete.

Main > Monitor commands

This appendix includes the following topics:

- [Monitor > Beacon](#)
- [Monitor > MemoryStatus](#)
- [Monitor > NetBackup](#)
- [Monitor > NetworkStatus](#)
- [Monitor > SDCS](#)
- [Monitor > Top](#)
- [Monitor > Uptime](#)
- [Monitor > Who](#)
- [Monitor > Hardware](#)

Monitor > Beacon

`Monitor > Beacon` – This command flashes or stops flashing lights on your appliance.

SYNOPSIS

`Beacon Duration`

`Beacon Stop`

DESCRIPTION

The Beacon command enables you to flash the disk drive lights or to stop flashing the lights on the specified storage shelf (or enclosure) or hard disk drives of a 52xx appliance.

When two storage shelves are attached to a 5230 appliance, you can use the `Beacon` command to identify a specific storage shelf.

OPTIONS

`Beacon Duration Enclosure EnclosureID [Minutes]`

Use this command to specify an amount of time to allow the disk drive lights of an enclosure to flash. Here, *EnclosureID* is the device ID of the enclosure and [Minutes] is the duration of time, in minutes, that lights can flash. [Minutes] is an optional parameter. If you do not enter a value for this parameter, it takes the default value of 10 minutes.

`Beacon Duration HDD EnclosureID SlotNo [Minutes]`

Use this command to specify an amount of time to allow a disk drive light to flash. Here, *EnclosureID* is the device ID of the enclosure and *SlotNo* is the slot number of the disk. [Minutes] is the duration of time, in minutes, that lights can flash. [Minutes] is an optional parameter. If you do not enter a value for this parameter, it takes the default value of 10 minutes.

`Beacon Duration WWID [WWID] [Minutes]`

Use this command to specify an amount of time to allow the disk drive lights of a storage unit to flash. Here, *WWID* is the device ID of a specific disk group. [Minutes] is the duration of time, in minutes, that lights can flash. [Minutes] is an optional parameter. If you do not enter a value for this parameter, it takes the default value of 10 minutes.

Beacon Stop Enclosure *EnclosureID*

Use this command to stop flashing the lights of all the disk drives of an enclosure. Here, *EnclosureID* is the device ID of the enclosure.

Beacon Stop HDD *EnclosureID SlotNo*

Use this command to stop flashing the light of a disk drive. Here, *EnclosureID* is the device ID of the enclosure and *SlotNo* is the slot number of the disk.

Beacon Stop WWID [WWID]

Use this command to stop flashing the lights of the disk drives of an expansion unit. Here, [WWID] is the device ID of the expansion unit. If you do not enter a value for this parameter, it displays a list of available expansion WWIDs.

Monitor > MemoryStatus

Monitor > MemoryStatus – Displays memory usage statistics of the host in KB.

SYNOPSIS

MemoryStatus

DESCRIPTION

Use this command to report memory usage statistics in KB.

OPTIONS

MemoryStatus

Use this command to report memory usage statistics in KB.

EXAMPLES

The following is an example of information that is displayed when you run the Main
> Monitor > MemoryStatus command.

```
abc123.Monitor> MemoryStatus
```

	total	used	free	shared	buffers	cached
Mem:	8065028	6617948	1447080	0	347384	5111668
-/+ buffers/cache:		1158896	6906132			
Swap:	10993656	0	10993656			
Total:	19058684	6617948	12440736			

	total	used	free	shared	buffers	cached
Mem:	8065028	6617940	1447088	0	347384	5111664
-/+ buffers/cache:		1158892	6906136			
Swap:	10993656	0	10993656			
Total:	19058684	6617940	12440744			

	total	used	free	shared	buffers	cached
Mem:	8065028	6617940	1447088	0	347384	5111664
-/+ buffers/cache:		1158892	6906136			
Swap:	10993656	0	10993656			
Total:	19058684	6617940	12440744			

	total	used	free	shared	buffers	cached
--	-------	------	------	--------	---------	--------

Mem:	8065028	6618328	1446700	0	347384	5111712
-/+ buffers/cache:		1159232	6905796			
Swap:	10993656	0	10993656			
Total:	19058684	6618328	12440356			

	total	used	free	shared	buffers	cached
Mem:	8065028	6618320	1446708	0	347384	5111716
-/+ buffers/cache:		1159220	6905808			
Swap:	10993656	0	10993656			
Total:	19058684	6618320	12440364			

	total	used	free	shared	buffers	cached
Mem:	8065028	6618320	1446708	0	347384	5111716
-/+ buffers/cache:		1159220	6905808			
Swap:	10993656	0	10993656			
Total:	19058684	6618320	12440364			

	total	used	free	shared	buffers	cached
Mem:	8065028	6618304	1446724	0	347384	5111716
-/+ buffers/cache:		1159204	6905824			
Swap:	10993656	0	10993656			
Total:	19058684	6618304	12440380			

	total	used	free	shared	buffers	cached
Mem:	8065028	6618148	1446880	0	347384	5111712
-/+ buffers/cache:		1159052	6905976			
Swap:	10993656	0	10993656			
Total:	19058684	6618148	12440536			

	total	used	free	shared	buffers	cached
Mem:	8065028	6617636	1447392	0	347384	5111720
-/+ buffers/cache:		1158532	6906496			
Swap:	10993656	0	10993656			
Total:	19058684	6617636	12441048			

	total	used	free	shared	buffers	cached
Mem:	8065028	6617636	1447392	0	347384	5111724
-/+ buffers/cache:		1158528	6906500			
Swap:	10993656	0	10993656			
Total:	19058684	6617636	12441048			

	total	used	free	shared	buffers	cached
Mem:	8065028	6618212	1446816	0	347384	5111724

-/+ buffers/cache:	1159104	6905924
Swap:	10993656	0 10993656
Total:	19058684	6618212 12440472

Monitor > NetBackup

Monitor > NetBackup – Display and control various aspects of backup jobs

SYNOPSIS

NetBackup Jobs All

NetBackup Jobs Failed

DESCRIPTION

This command exists under the `Main > Monitor` view. Use this command to display all of the backup jobs that are configured for your appliance or the failed jobs.

Note: This command is available only for a Master appliance.

OPTIONS

NetBackup Jobs All

Display backup job information including job IDs, type, status, policy, schedule, client, destination, media server, active PID, and FATPipe.

NetBackup Jobs Failed

Display the failed backup job IDs.

Monitor > NetworkStatus

Monitor > NetworkStatus – Displays the network statistics for the host.

SYNOPSIS

NetworkStatus

DESCRIPTION

Use this command to view network statistics for the appliance.

OPTIONS

NetworkStatus

Use this command to view the network statistics for the appliance.

EXAMPLES

The following example display information that is displayed when you run the Main > Manage > NetworkStatus command.

```
abc123.Monitor> NetworkStatus
eth0          eth1          eth2          eth3
KB/s in  KB/s out  KB/s in  KB/s out  KB/s in  KB/s out  KB/s in  KB/s out
0.00      0.00      0.00      0.00      18.27     0.42      0.00      0.00
0.00      0.00      0.00      0.00      19.11     0.26      0.00      0.00
0.00      0.00      0.00      0.00      5.40      0.26      0.00      0.00
0.00      0.00      0.00      0.00      14.69     0.26      0.00      0.00
0.00      0.00      0.00      0.00      11.07     0.26      0.00      0.00
0.00      0.00      0.00      0.00      21.99     0.26      0.00      0.00
0.00      0.00      0.00      0.00      15.97     0.26      0.00      0.00
0.00      0.00      0.00      0.00      22.95     0.26      0.00      0.00
0.00      0.00      0.00      0.00      7.91      0.26      0.00      0.00
0.00      0.00      0.00      0.00      15.99     0.26      0.00      0.00
0.00      0.00      0.00      0.00      16.54     0.58      0.00      0.00
0.00      0.00      0.00      0.00      10.63     0.26      0.00      0.00
0.00      0.00      0.00      0.00      4.43      0.26      0.00      0.00
0.00      0.00      0.00      0.00      16.60     0.26      0.00      0.00
```

Monitor > SDCS

Monitor > SDCS – Configure and monitor Symantec Data Center Security (SDCS).

SYNOPSIS

Audit

ServerInfo

DESCRIPTION

Use this command to monitor Symantec Data Center Security (SDCS) events and configuration on the appliance.

OPTIONS

The following commands and options are available under Monitor > SDCS:

Audit

Search, filter, and edit the retention settings of the SDCS audit log.

- Use the `Audit Search <search_string>` command to search the audit log for the specified string. Use quotation marks if your search string contains multiple words.
- Use the `Audit SetSettings FileNumber <file_number>` command to set the number of SDCS audit files that are maintained.
- Use the `Audit SetSettings RetentionPeriod <days>` command to set the number of days that the audit files are maintained.
- Use the `Audit ShowSettings` command to view the retention period (days) of the audit files.
- Use the `Audit View` command and options to filter and display the audit log based on available criteria.
 - `Audit View Date <ToDate> [FromDate]`

View audit records using the `FromDate` to `ToDate` parameters. The format is `mm/dd/yyyy[-hh:mm:ss]`. If `FromDate` is omitted, it equals `ToDate` with `hh:mm:ss` set to zeroes.
 - `Audit View EventID <ID#>`

Retrieve the detailed view of the audit record that contains the given event ID.

- `Audit View EventType <event_code>`
Retrieve the audit records that match the given event type. Each event type is represented by a four-letter code that appears in the SDCS audit log. You can view the available codes using the `Audit View EventTypeCodes` command.
- `Audit View EventTypeCodes`
Display the event type codes that can be used with the `Audit View EventType` command, along with a brief description of each code.
- `Audit View Filter <criteria>`
View the audit records that match the filter criteria.
- `Audit View Severity <severity_code>`
Retrieve the audit records that match the given severity. Each event is represented by a one-letter code that appears in the SDCS audit log. You can view the available codes using the `Audit View SeverityCodes` command.
- `Audit View SeverityCodes`
Display the severity codes that can be used with the `Audit View Severity` command, along with a brief description of each code.

ServerInfo

Set and display SDCS server information to make the appliance a managed agent.

- Use the `ServerInfo GetServerCert <hostname> <port>` command to get an SDCS server certificate. The `<hostname>` parameter is the fully qualified domain name of the SDCS server. The port is the port number of the SDCS server. The default port is 443.
- Use the `SDCS > ServerInfo Set` command to define the SDCS server information to make the appliance a managed agent.
- Use the `SDCS > ServerInfo Show` command to display the SDCS management server configuration.

Monitor > Top

Monitor > Top – Display the top process information.

SYNOPSIS

Top

DESCRIPTION

This command exists under the Main > Monitor view. You can use this command to view the top process information.

OPTIONS

Top

Provides the information (frequently refreshed) about the most CPU-intensive processes currently running.

EXAMPLES

The following is an example of process information that is displayed for the Main > Monitor > Top command.

```
abc123.Monitor> Top
top - 10:44:02 up 1 day, 23:05,  5 users,  load average: 0.01, 0.03, 0.05
Tasks: 576 total,   1 running, 575 sleeping,   0 stopped,   0 zombie
CPU(s):  0.1%us,   0.2%sy,   0.0%ni, 99.7%id,   0.0%wa,   0.0%hi,   0.0%si,   0.0%st
Mem:    128636M total,    9053M used,   119583M free,    251M buffers
Swap:    66671M total,      0M used,   66671M free,    2762M cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 58718 root        20   0 1315m  43m  11m S   1  0.0   21:11.19 nbappdbsrv
119378 root        20   0  9176 1604  868 R   1  0.0    0:00.12 top
 60796 root        20   0  490m  42m  25m S   1  0.0    3:37.96 nbsl
   1937 root        20   0     0     0   0 S   0  0.0    0:01.33 kdmflush
   2046 root        20   0     0     0   0 S   0  0.0    0:06.31 flush-253:9
   4285 root        39  19     0     0   0 S   0  0.0   11:14.74 kipmi0
 11254 root        20   0  9268  964  476 S   0  0.0    1:49.97 irqbalance
 57836 root        20   0 63.3g  84m  9.9m S   0  0.1   34:30.40 NB_dbdrv
 57892 root        20   0  652m  21m  12m S   0  0.0    1:06.68 nbvmtmgr
```

Monitor > Uptime

`Monitor > Uptime` – Display the uptime statistics for the current host.

SYNOPSIS

`Uptime`

DESCRIPTION

Use this command to display the uptime statistics for the current host.

OPTIONS

`Uptime`

Prints the current time, how long the system has been running, the number of users currently logged in (which may include the same user multiple times) and system load averages.

Monitor > Who

Monitor > Who – Display current logon sessions on the current host.

SYNOPSIS

Who

DESCRIPTION

Use this command to display current logon sessions on the current host.

OPTIONS

Who

Lists the names of users currently logged in, their terminal, the time they have been logged in, and the name of the host from which they have logged in.

EXAMPLES

The following is an example of information that is displayed when you run the Main > Monitor > Who command.

```
abc123.Monitor> Who
10:44:37 up 1 day, 23:05, 5 users, load average: 0.01, 0.02, 0.05
USER      TTY      LOGIN@  IDLE   JCPU   PCPU WHAT
admin     tty1     Mon11   46:59m 0.11s  0.01s login -- admin
admin     pts/0    Mon11   46:41m 0.09s  0.18s sshd: admin [priv]
admin     pts/1    Mon12   46:40m 0.11s  0.18s sshd: admin [priv]
admin     pts/2    09:43   1:01m  0.11s  0.02s sshd: admin [priv]
admin     pts/3    10:17   0.00s  0.14s  0.01s sshd: admin [priv]
```

Monitor > Hardware

`Monitor > Hardware` – View the various hardware components, view the errors and the health status.

SYNOPSIS

```
Hardware ShowErrors
```

```
Hardware ShowComponents
```

```
Hardware ShowHealth Appliance [Item]
```

```
Hardware ShowHealth StorageShelf [Item]
```

```
Hardware ShowHealth PrimaryShelf [Item]
```

```
Hardware ShowHealth ExpansionShelf [ExpansionShelfID] [Item]
```

DESCRIPTION

Use this command to do the following:

- Display the hardware components such as the appliance or the compute node, or the storage shelves. The items that are associated with these components also display.
- View the errors that are related to the hardware components of an appliance. You can use this information to notify Veritas Technical Support of the errors.
- View the performance and status of various hardware components of the appliance and the attached storage.

OPTIONS

```
Hardware ShowComponents
```

Display all the hardware components and items of an appliance.

```
Hardware ShowErrors
```

Display all the errors that are related to hardware status.

```
Hardware ShowHealth Appliance [Item]
```

View the performance and status of various hardware components of the appliance. The [Item] parameter specifies the hardware part for which the data is queried.

The following options are available for the [Item] parameter. The default value is ALL.

For a 52xx appliance:

```
(All/Fan/CPU/Disk/Fibrechannel/RAID/Power/Temperature/Product/  
PCI/Network/Firmware/Adapter/Partition/MSDP/MSDPCLoud/DIMM) [all]
```

For a 5250 appliance:

```
(All/Fan/CPU/Disk/Fibrechannel/RAID/Power/Temperature/Product/  
PCI/Network/Adapter/Partition/MSDP/DIMM/Mini_SSD) [all]
```

For a 53xx appliance:

```
(All/Fan/CPU/Disk/Fibrechannel/RAID/Power/Temperature/Product/  
PCI/Network/Firmware/Connection/StorageStatus/Partition/DIMM) [all]
```

For example, to view the serial number of the appliance, run the following command:

Hardware ShowHealth Appliance Product

```
Hardware ShowHealth StorageShelf [Item]
```

View the performance and status of various hardware components of the storage shelf that is attached to a 52xx appliance. The [Item] parameter specifies the hardware part for which the data is queried.

The following options are available for the [Item] parameter. The default value is ALL.

```
(All/Fan/Disk/Power/Temperature/Product) [all]
```

```
Hardware ShowHealth PrimaryShelf [Item]
```

View the performance and status of the primary storage shelf of the NetBackup 53xx Appliance.

The following options are available for the [Item] parameter. The default value is ALL.

```
(All/Fan/Disk/RAID/Power/Temperature/Product/Firmware/BBU/  
Controller/Volume/Connection) [all]
```

```
Hardware ShowHealth ExpansionShelf [ExpansionShelfID] [Item]
```

View the performance and status of the expansion storage shelf(shelves) of the NetBackup 53xx Appliance.

Where [ExpansionShelfID] is the ID of a specific expansion shelf. By default, the data is displayed for all the storage shelves. To check the expansion shelf IDs, use the Main > Monitor > Hardware ShowComponents command.

The following options are available for the [Item] parameter. The default value is ALL.

```
(All/Fan/Disk/Power/Temperature/Product) [all]
```

For example, to view the status of fan on the expansion storage shelf with an ID of 1, run the following command:

Hardware ShowHealth ExpansionShelf 1 FAN

ShowHealth Appliance Partition ExportCSV

Export the status of all the partitions on an appliance. Follow the instructions on the shell menu to find the CSV file for more details.

EXAMPLES

The following is an example output of the `Monitor > Hardware ShowHealth Appliance Product` command.

```
abc123.Monitor> Hardware ShowHealth Appliance Product
Compute Node abc123.company.com
```

Time Monitoring Ran: Tue Jul 19 2016 02:29:15 PDT

```
+-----+
|           Hardware monitor information           |
|+-----+-----+-----+-----+|
|| Name           | Manufacturer | Serial           | |
|+-----+-----+-----+-----+|
|| NetBackup 52xx | Veritas      | abc123serialno   | |
|+-----+-----+-----+-----+|
|                                     |
+-----+
```

The following is an example output of the `Main > Monitor > Hardware ShowHealth ExpansionShelf 1 Fan` command:

Node abc122

Time Monitoring Ran: Thu Mar 27 2014 07:20:43

Compute node does not have any errors.

```
+-----+
|           Expansion Storage Shelf 1 Fan Information           |
```

ID	Location	Status	State	Acknowledge
1	Tray 1 Right	Optimal	OK	N/A
2	Tray 1 Left	Optimal	OK	N/A
3	Tray 1 Right	Optimal	OK	N/A
4	Tray 1 Left	Optimal	OK	N/A

Main > Network commands

This appendix includes the following topics:

- [Network > Configure](#)
- [Network > Date](#)
- [Network > DNS](#)
- [Network > Gateway](#)
- [Network > Hostname](#)
- [Network > Hosts](#)
- [Network > IPv4](#)
- [Network > IPv6](#)
- [Network > LinkAggregation](#)
- [Network > NetStat](#)
- [Network > NTPServer](#)
- [Network > Ping](#)
- [Network > SetProperty](#)
- [Network > Show](#)
- [Network > TimeZone](#)
- [Network > TraceRoute](#)

- [Network > Unconfigure](#)
- [Network > VLAN](#)
- [Network > WANOptimization](#)

Network > Configure

Network > Configure – Configure the appliance to a network.

SYNOPSIS

```
Configure IPAddress Netmask GatewayIPAddress [InterfaceNames]  
[BondingMode]
```

DESCRIPTION

You can use the `Configure` command to configure the IP address of a single interface on the network that you want to connect your appliance to. When you use this command, you need to define the IP address, the netmask address, and the gateway address.

If multiple interfaces with separate IP addresses are used, use the `Network > IPv4` or the `Network > IPv6` commands to configure each network interface individually.

Use the `Network > Gateway` command to add the routing information for default route or to add route for VLAN interfaces.

Caution: If you have an operational NetBackup 53xx high availability configuration, do not make the following changes on the public network interface card (NIC):

Change the IPv4 address.

Create any bond with the IPv6 address.

OPTIONS

```
Configure IPAddress Netmask GatewayIPAddress [InterfaceNames]  
[BondingMode]
```

Configure the IP address and default gateway for the appliance. The command configures the IP address and sets the default gateway.

Where *IPAddress* is the IPv4 or IPv6 address, *Netmask* is the netmask, *Gateway/IPAddress* is the default gateway IP address, and [*InterfaceNames*] is the name of the device.

This device can be a physical interface, a bond, or a VLAN interface.

Remember that you should not use both an IPv4 and an IPv6 address in the same command. For example, you cannot use `Configure 9ffe::9`

255.255.255.0 1.1.1.1.. You should use `Configure 9ffe::46 64 9ffe::49 eth1` to configure an interface using IPv6 address.

In the `[InterfaceNames]` field the following applies:

- If you enter a single interface name, then the IP address is configured on that device.
- If you enter a comma-separated list of interface names, then a bond is created and the IP address is configured on the bonded device. You must ensure that the interfaces that comprise the list are of same type, either **FIBRE** or **COPPER**). In addition, the interfaces must support the same speed and at least one of the interfaces in the list is cabled.
- If you do not enter an interface name, the best possible interface or interfaces are selected based on the port type (**FIBRE** or **COPPER**), speed, and the link status.

You define the bonding mode in the `BondingMode` field. You can enter one of the following modes:

- `balance-rr`
- `active-backup`
- `balance-xor`
- `broadcast`
- `802.3ad`
- `balance-tlb`
- `balance-alb` (This bonding mode is the default value.)

EXAMPLES

The following example shows how to configure your appliance network settings:

```
Network > Configure 10.180.2.3 255.255.255.0 10.180.2.1 eth1
```

The following examples show how to configure your appliance using the Auto selection, specifying a specific interface, or multiple interfacing and creating a bond.

- Specify explicit interfaces such as `eth2` and `eth3` to create a bond. For this example, you provide the IPAddress, NetMask, Gateway IPAddress, interface names, and the bonding mode, in that order.

```
Network > Configure 10.180.2.3 255.255.255.0 eth2,eth3 balance-alb
```

You can also create a bond and configure it using IPv6 addresses:

```
Network > Configure 9ffe::207 64 9ffe::49 eth,eth3
```


Network > Date

Network > Date – Set or show the computer system time.

SYNOPSIS

```
Date Set Month Day HHMMSS Year
```

```
Date Show
```

DESCRIPTION

You can use this command to set or show the system time.

OPTIONS

```
Date Set Month Day HHMMSS Year
```

Set the system time.

Where *Month* is the name of the month. *Day* is the day of the month and has a range of one to 31. The variable *HHMMSS* is the hour, minute, and seconds in a 24-hour format and the fields are separated by semi-colons, for example, HH:MM:SS. The variable *Year* is the current year and the range for this field is 1970 through 2037.

The following is sample entry for this command:

```
Date Set Apr 29 23:44:34 2011
```

```
Date Show
```

Show the system date and time.

Network > DNS

Network > DNS – Configure the DNS information for the appliance.

SYNOPSIS

```
DNS Add NameServer IPAddress
DNS Add SearchDomain DomainName
DNS Delete Domain
DNS Delete NameServer IPAddress
DNS Delete SearchDomain DomainName
DNS Domain Name
DNS Show
```

DESCRIPTION

You can use this command to perform the following tasks:

- Add or delete a name server to the DNS configuration.
- Add or delete a domain name to the DNS search list.
- Set the appliance DNS domain name.
- Show the current DNS information.

OPTIONS

```
DNS Add NameServer IPAddress
```

Add a DNS nameserver to the DNS configuration.

Where *IPAddress* is the IP address of the DNS name server.

```
DNS Add SearchDomain DomainName
```

Add a DNS search domain to the configuration.

Where *DomainName* is the target domain to add for searching.

```
DNS Delete Domain
```

Delete a DNS domain name.

```
DNS Delete NameServer IPAddress
```

Delete a DNS named server from the configuration.

Where *IPAddress* is the IP address of the DNS name server.

DNS Delete SearchDomain *DomainName*

Delete a DNS search domain from the configuration.

Where *IPAddress* is the IP address of the DNS name server.

DNS Domain *Name*

Set the appliance domain name, where *Name* is the domain name of the appliance

DNS Show

Show the current DNS information.

Network > Gateway

Network > Gateway — Add or delete routing information.

SYNOPSIS

```
Gateway Add GatewayIPAddress [TargetNetworkIPAddress] [Netmask]  
[InterfaceName]
```

```
Gateway Delete TargetNetworkIPAddress [Netmask]
```

```
Gateway Show IPVersion
```

DESCRIPTION

Use this command to add or delete a route from the kernel routing table. With this command you can also view the kernel routing table. Refer to Linux route man page for more advanced use cases.

With this command you can define the IPv4 or IPv6 address that you plan to add or delete as well as display the current gateway information. If multiple networks are added to the appliance configuration, you can use the `Gateway Add` command to add the gateway to all of the destination networks.

Remember that you should not use both IPv4 and IPv6 address in the same command. For example, you cannot use `Gateway Add 9ffe::3 255.255.255.0 eth1`. You should use `Gateway Add 6ffe::3 6ffe:: 64 eth1`.

OPTIONS

```
Gateway Add GatewayIPAddress [TargetNetworkIPAddress] [Netmask]  
[InterfaceName]
```

Add a route to a kernel routing table.

Where the *GatewayIPAddress* variable is the new IPv4 or IPv6 gateway address. The *TargetNetworkIPAddress* is the target network IPv4 or IPv6 address. The *Netmask* variable is the target network netmask, and *InterfaceName* is the interface name. The *TargetNetworkIPAddress*, *Netmask*, and *InterfaceName* are optional when you set up the default gateway. After the default gateway has been added, you must use these fields to add any additional gateways.

```
Gateway Delete TargetNetworkIPAddress [Netmask]
```

Delete the route from the kernel routing table.

Where *TargetNetworkIPAddress* is the target network address. The *Netmask* variable is the target network netmask.

Gateway Show [IPVersion]

Display the gateway and the route information. Here, [IPVersion] parameter is an optional parameter. It defines the IP protocols - IPv4 and IPv6. If you do not enter a value for the [IPVersion] parameter, the information is displayed for IPv4.

To know the gateway information for a VLAN interface, enter the VLAN interface ID for the [IPVersion] parameter.

EXAMPLES

Use the following example to set the default gateway.

```
Gateway Add 10.180.1.1
```

Use the following example to add a route to the destination network 192.168.2.0.

```
Gateway Add 191.168.2.1 192.168.2.0 255.255.255.0
```

```
Gateway Add 6ffe::3 6ffe:: 64 eth1
```

Use the following example to delete the default gateway.

```
Gateway Del default
```

Use the following example to delete a route to the destination network, 10.180.0.0 or 6ffe:: 64.

```
Gateway Delete 10.180.0.0
```

```
Gateway Delete 6ffe:: 64
```

Network > Hostname

Network > Hostname – Set or show the hostname for your appliance.

SYNOPSIS

Hostname Set *Name*

Hostname Show

DESCRIPTION

You can use this command to set the host name of the appliance.

OPTIONS

Hostname Set *Name*

Set the host name.

The *Name* variable contains the short host name or the fully qualified domain name (FQDN) of the host.

Note: The host name can only be set during an initial configuration session. After the initial configuration has completed successfully, you can re-enter the initial configuration by performing a factory reset on the appliance. See the *NetBackup appliance Administrator's Guide* for more information.

Hostname Show

Display the host name.

Network > Hosts

Network > Hosts – Manage the IP address and host name mapping.

SYNOPSIS

```
Hosts Add IPAddress FQHN ShortName
```

```
Hosts Delete IPAddress
```

```
Hosts Show
```

DESCRIPTION

You can use this command to view the hosts configuration information, such as the IP address and host name mapping. You can also use this command to add or delete an IP address from the hosts file.

OPTIONS

```
Hosts Add IPAddress FQHN ShortName
```

Add an IP address to the host name mapping.

IPAddress is the IPv4 or IPv6 address to add.

FQHN is the fully qualified host name. And *ShortName* is the short host name.

```
Hosts Delete IPAddress
```

Delete an IP address from the host name mapping.

IPAddress is the IPv4 or the IPv6 address to be deleted.

```
Hosts Show
```

Display the IP address and host name mapping.

Network > IPv4

Network > IPv4 – Change the IPv4 address of a network interface.

SYNOPSIS

```
IPv4 IPAddress NetMask [InterfaceNames]
```

DESCRIPTION

Use this command to change the IPv4 address of a network interface. You can use this command to configure multiple network interfaces. To do that, you must repeat the command for each network that you want to add.

Caution: If you have an operational NetBackup 53xx high availability configuration, do not change the IPv4 address on the public network interface card (NIC).

OPTIONS

```
IPv4 IPAddress NetMask [InterfaceNames]
```

Change the IPv4 address of a network interface.

Where *IPAddress* is the name of the new IPv4 address. The *NetMask* variable is the name of the netmask. The [*InterfaceNames*] parameter is a comma-separated list of interface names. The [*InterfaceNames*] field is optional. If an interface name is not provided, the command searches for an interface and configures it.

You may enter a VLAN interface ID for the [*InterfaceNames*] parameter. However, unlike the physical interface or bond interface, if you do not provide a value for the for the [*InterfaceNames*] parameter, the command does not search for VLAN interfaces.

Network > IPv6

Network > IPv6 – Add an IPv6 address without specifying a gateway address.

SYNOPSIS

```
IPv6 IPAddress Prefix [InterfaceNames]
```

DESCRIPTION

Use this command to configure the IPv6 address of a network interface. You cannot use this command to configure multiple interfaces.

Caution: If you have an operational NetBackup 53xx high availability configuration, do not create any bond with the IPv6 address on the public network interface card (NIC).

OPTIONS

```
IPv6 IPAddressPrefix [InterfaceNames]
```

Change the IPv6 address of a network interface.

Where *IPAddress* is the IPv6 address, *Prefix* is the prefix length, and [*InterfaceNames*] is the name of the device.

The [*InterfaceNames*] parameter is a comma-separated list of interface names. The [*InterfaceNames*] parameter is an optional field. If an interface name is not provided, the command searches for an interface and configures it.

You may enter a VLAN interface ID for the [*InterfaceNames*] parameter. However, unlike the physical interface or bond interface, if you do not provide a value for the [*InterfaceNames*] parameter, the command does not search for VLAN interfaces.

EXAMPLES

Use the following example to assign an IPv6 address to a specific interface:

```
IPv6 9ffe::9 64 eth1
```

Use the following example to create a bond when multiple interfaces are given:

```
IPv6 9ffe::9 64 eth2,eth3
```

Network > LinkAggregation

Network > LinkAggregation – Manage link aggregation.

SYNOPSIS

```
LinkAggregation Create Slaves [BondingMode]  
LinkAggregation Delete InterfaceNames  
LinkAggregation Disable [InterfaceName]  
LinkAggregation Enable [Slaves] [BondingMode]  
LinkAggregation Show [InterfaceNames]  
LinkAggregation Status
```

DESCRIPTION

You can use this command to manage link aggregation.

You can use this command to enable bonding (link aggregation), across the available network cards. If only one port is configured, bonding is not available. If multiple ports are configured on your appliance, they are identified automatically.

You have the ability to bond multiple ports or define specific ports to bond by what you enter in the [Slaves] option. To bond multiple ports, you must use a comma to separate the device names. In addition, you should ensure that all of the ports that participate in a bond are connected to the same switch. And make sure that is no additional port configuration is done at the switch.

There are eight different bond modes that you can choose from. Some of the bond modes require additional configuration on the switch or the router. You should take additional care when you select a bond mode.

For more information about the bond modes and any required switch configuration, see the following documentation:

<http://www.kernel.org/doc/Documentation/networking/bonding.txt>

You can also use this command to do the following:

- To create a bond without associating an IP address to it.
- To delete a existing bond.
- To display the status of the link aggregation.
- To show the link aggregation properties of one or more interfaces.

- To turn off the link aggregation.

OPTIONS

`LinkAggregation Create Slaves [BondingMode]`

Create a bond.

Here, the *Slaves* variable defines the device name that you want to bond and the *[BondingMode]* parameter is used to define the bond mode in which to configure bonding, or link aggregation. The eight available modes are, `balance-rr` | `active-backup` | `balance-xor` | `broadcast` | `802.3ad` | `balance-tlb` | `balance-alb`. The default mode is `balance-alb`.

Conform to following guidelines to create a bond:

- Ensure that the interfaces that participate in bond formation have the same port speed (i.e. either 1GB or 100GB).
- At least one of the interfaces that participates in bond formation must be plugged.
- Ensure that none of the interfaces that are selected for creating the bond have any VLANs tagged to them.
- Verify that any of the selected interfaces are not already a part of another bond.

You can create this bond with or without assigning an IP address to it. The criteria for assigning or not assigning an IP address to the bond depends solely on the interfaces that are selected for creating the bond.

Consider the following two cases to understand IP address assignment to a bond:

- An IP address is assigned to a newly created bond, if any of the interfaces that are selected for creating a bond already have an IP address assigned to them.
- An IP address is not assigned to a newly created bond, if the interfaces that are selected for creating a bond do not have IP addresses assigned to them.

A bond without an IP address associated to it is prerequisite for tagging a VLAN to a bonded interface.

If the selected interfaces are configured with IP addresses, an error message is displayed to indicate that a single interface must be configure with an IP address to create the bond.

Note: You may use the `Create` and the `Enable` commands to configure a bond over a private interface, for example, `eth0`. This option is not available through the NetBackup Appliance Web Console.

`LinkAggregation Delete InterfaceNames`

Use this command to delete a bond. Here, *InterfaceNames* defines the bond device name that you want to disable.

Note: To delete a bond, ensure that the no IP address is configured on the bond. If an IP address is configured to the bond, you must first unconfigure the IP address. To unconfigure the IP address, run the `Network > Unconfigure` command.

`LinkAggregation Disable [InterfaceName]`

Turns off the link aggregation. The `[InterfaceName]` is optional. You use this option to define the bond device name that you want to disable. You can use the `LinkAggregation > Status` command to obtain the device name.

LinkAggregation cannot be turned-off if there are multiple bonds present. To turn-off link aggregation on a specific bond, you must enter the bond name in the `[InterfaceName]` parameter.

`LinkAggregation Enable [Slaves] [BondingMode]`

Use to turn on link aggregation. This command assigns IP address to the newly created bond.

The `[Slaves]` option defines the device names that you want to bond. Use a comma as a delimiter between the device names. This field is optional. The device names are identified automatically based on the current network settings and properties.

The `[BondingMode]` parameter is used to define the bond mode in which to configure bonding, or link aggregation. The eight available modes are, `balance-rr` | `active-backup` | `balance-xor` | `broadcast` | `802.3ad` | `balance-tlb` | `balance-alb`. The default mode is `balance-alb`.

`LinkAggregation Status [HostName]`

Show the status of the link aggregation. If no interfaces have been configured, the following message appears:

No virtual interfaces have been configured.

`LinkAggregation Show [InterfaceNames]`

Show the link aggregation properties of one or more interfaces.

Use the [InterfaceNames] option to define the interface or interfaces that you want to view the properties of. Use a comma to separate the interface names if you want to view the properties of more than one.

Network > NetStat

Network > NetStat — Identify network statistical information

SYNOPSIS

NetStat a

NetStat an

NetStat ia

NetStat s

DESCRIPTION

The `NetStat` command displays various network-related information such as network statistical information.

OPTIONS

NetStat a

Examine network connections for all interfaces textually.

NetStat an

Examine network connections for all interfaces numerically.

NetStat ia

Examine network interface stats.

NetStat s

Examine network summary stats for all interfaces numerically.

Network > NTPServer

Network > NTPServer – Manage the NTP Servers.

SYNOPSIS

NTPServer Add *Server*

NTPServer Delete *Server*

NTPServer Show

DESCRIPTION

Use this command manage the NTP servers. With this command, you can to do the following:

- Add an NTP server to the sync time.
- Delete an NTP server.
- Show the known NTP Servers.

OPTIONS

NTPServer Add *Server*

Add an NTP Server. Where *Server* is the name of the server to add.

NTPServer Delete *Server*

Delete an NTP Server. Where *Server* is the name of the server to delete.

NTPServer Show

Show the known NTP Servers.

Network > Ping

`Network > Ping` – An attempt to reach a host or IP address with `ICMP ECHO_REQUESTs`

SYNOPSIS

`Ping Host`

DESCRIPTION

Use this command to test whether a particular host is reachable across an Internet Protocol (IP) network. The command sends a small packet of information to a hostname or an IP address to test network communications. It then provides information on how long the packet took to come back to its origin.

OPTIONS

`Ping Host`

Send a small packet of `ICMP ECHO_REQUESTs` to a host name or an IPv4 or IPv6 address of the target computer to test the network communications.

Where *Host* is the hostname or the IPv4 or IPv6 address of the target computer.

Network > SetProperty

Network > SetProperty – Set the Ethernet interface property.

SYNOPSIS

```
SetProperty InterfaceName Property Value
```

DESCRIPTION

You can use this command to set Ethernet interface property. You can define the name of the device, the property name such as an MTU. And you can define the property value, such as 1500 for the MTU.

OPTIONS

```
SetProperty InterfaceName Property Value
```

Set Ethernet interface property.

Enter the name of the interface name in the *InterfaceName* variable. An example of this value is **eth1**. The *Property* variable is the property name, such as **mtu**. The *Value* variable is the property value, for example 1500.

The following is sample entry for this command:

```
SetProperty eth1 mtu 1500
```

This command changes the Maximum transmission unit (MTU) of interface (eth1) to 1500.

Network > Show

Network > Show – List the network properties.

SYNOPSIS

Show Configuration

Show Properties [InterfaceNames]

Show Status

DESCRIPTION

Use this command to list the network properties.

OPTIONS

Show Configuration

Display the network interface properties.

Show Properties [InterfaceNames]

Display the network properties. The `InterfaceNames` is an optional parameter.

The interface name can be a physical interface, bonded interface, or a VLAN interface. If you enter multiple interface names, separate the names with a comma.

Show Status

View the following network status information:

- Device status
- Routing status
- Link aggregation status
- VLAN interface status

Network > TimeZone

Network > TimeZone – Set the time zone.

SYNOPSIS

TimeZone Reset

TimeZone Set

TimeZone Show

DESCRIPTION

You can use this command to set time zone for which your appliance is located. You can reset the time zone to the Coordinated Universal Time (UTC) or show the currently configured time zone.

OPTIONS

TimeZone Reset

Reset the time zone to UTC.

TimeZone Set

Set the time zone.

TimeZone Show

Show the currently configured time zone.

Network > TraceRoute

Network > TraceRoute – Display the network packet route

SYNOPSIS

```
TraceRoute Host
```

DESCRIPTION

Use this command to display the network path of Internet routers that a packet takes as it travels from the appliance to the destination IP address or host.

OPTIONS

```
TraceRoute Host
```

Display the network route that a packet took to a destination host name or the IPv4 or IPv6 address of the target computer.

Where *Host* is the hostname or the IPv4 or IPv6 address of the target computer.

Network > Unconfigure

`Network > Unconfigure` – Remove the IP address and shut down the interface.

SYNOPSIS

```
Unconfigure InterfaceNames [IPAddress]
```

DESCRIPTION

Use this command to remove the IP address and shut down the interface.

This network interface can be a physical interface, a bonded interface, or a VLAN interface.

Caution: For the NetBackup 53xx high availability configuration, you cannot remove the public network interface card (NIC) or remove the IPv4 address on the public NIC.

OPTIONS

```
Unconfigure InterfaceNames [IPAddress]
```

Remove the IP address and shut down the interface. *InterfaceNames* is the name of the interface.

[*IPAddress*] is the IPv4 address. [*IPAddress*] is an optional parameter.

The *InterfaceNames* can be a VLAN interface, or a ethernet interface, or a bonded interface

Network > VLAN

`Network > VLAN` – Tag a VLAN, view its properties and status, or delete a tagged VLAN.

SYNOPSIS

`VLAN Delete VLANID`

`VLAN Show Properties Interfaces InterfaceNames`

`VLAN Show Status Interfaces InterfaceNames`

`VLAN Tag VLANID InterfaceNames [IPAddress] [Netmask]`

DESCRIPTION

Use these commands to configure and manage VLAN for your appliance in your existing network environments.

To tag a VLAN using a bond or a physical interface, conform to the following guidelines

- Ensure that the selected interface or ethernet device is plugged.
- Verify that the selected interface is not a part of a bond.
- The selected interface must not have an IP address configured to it. If the selected interface is configured with an IP address, you must first unconfigure the IP address and then tag a VLAN to it. To unconfigure the IP address, run the `Network > Unconfigure` command.

Note: A VLAN can be tagged to a private network interface (for example, eth0) only through the NetBackup Appliance Shell Menu and not through the NetBackup Appliance Web Console.

Use the `VLAN Show` command options to view the properties and statuses of your network interfaces.

OPTIONS

`VLAN Delete VLANID`

Delete a protocol-based VLAN. Here, *VLANID* is a numeric identifier for a tagged VLAN.

If the VLAN interface is configured with an IP address, you must first unconfigure the IP address to delete the VLAN.

VLAN Show Properties Interfaces *InterfaceNames*

View all the properties of a VLAN, where *InterfaceNames* is the name of the interface to which a VLAN is tagged. If you do not provide a value for the [InterfaceNames] parameter, the command displays properties for all the network interfaces that are available. Some of the property types that are included are MAC address, speed, and port type.

VLAN Show Status Interfaces *InterfaceNames*

View the status of a VLAN. The VLAN status can be *PLUGGED* or *UNPLUGGED*. Here, *InterfaceNames* is the name of the interface to which a VLAN is tagged.

VLAN Tag *VLANID* *InterfaceNames* [IPAddress] [Netmask]

Tag a VLAN to a physical interface or a bond. Here, *VLANID* is the VLAN identifier, which is numeric value and it can range between 1 - 4094. *InterfaceNames* is the name of the interface to which you want to tag the VLAN. [IPAddress] can be an IPv4 or an IPv6 address and [Netmask] is netmask for IPv4 or prefix length for IPv6. The *VLANID* and *InterfaceNames* are mandatory variables; whereas [IPAddress] and [Netmask] are optional parameters.

EXAMPLES

The following is an example of information that is displayed when you run the `Main > Network > VLAN Show Properties` command.

```
nb-appliance.Network> VLAN Show properties
```

```
Card: vlan12  [  PLUGGED|UP  ]
      BOOTPROTO      : |static          |
      DESCRIPTION    : |test          |
      DEVICE         : |vlan12        |
      ETHERDEVICE     : |eth1          |
      ETHTOOL_OPTIONS : |undef         |
      IPADDR         : |10.10.10.10   |
      MTU            : |1400          |
      NETMASK        : |255.255.255.0 |
      NETWORK        : |undef         |
      REMOTE_IPADDR   : |undef         |
      STARTMODE      : |auto          |
      USERCONTROL    : |no            |
      VLAN           : |yes           |
      BUS_ID         : |undef         |
      FLAGS          : |RBMU          |
```

ID	:	12	
LINK	:	yes	
MAC	:	00:50:56:B5:74:13	
MASTER	:	undef	
MODEL	:	undef	
PORT_TYPE	:	Twisted Pair	
SERIAL	:	undef	
SKIP_ADDITIONAL_DISCOVERY	:	0	
SKIP_LINKSTATE_DISCOVERY	:	0	
SPEED	:	1Gb/s	
VIRTUAL_DEV	:	undef	
VLANCOUNT	:	0	
ADMINPORT	:	No	
VIRTUAL	:	No	
IPADDR_V6	:	undef	

Network > WANOptimization

Network > WANOptimization – Manages wide area network data throughput optimization.

SYNOPSIS

```
Enable ALL
Enable interfaceList
Disable ALL
Disable interfaceList
Status
```

DESCRIPTION

Use this option to manage the WAN Optimization settings.

The WAN Optimization feature uses various techniques for increasing data-transfer efficiencies across wide-area networks. As a result, using WAN optimization can improve inbound and outbound data transfers to and from your appliance.

This feature includes the following benefits:

- Improves NetBackup Auto Image Replication performance.
NetBackup Auto Image Replication is a disaster recovery solution. Its purpose is to create off-site copies of mission critical backups to protect against site loss. For example, the backups that are generated in one NetBackup domain can be replicated to storage in other NetBackup domains. These other NetBackup domains may be located in diverse geographical locations. Because WAN optimization can improve wide area network data throughput to and from your appliance, more efficient backup data transfers and disaster recovery transfers can occur.
- Benefits appliances for which data is sent across slower networks. For example, such as networks with a latency greater than 20 milliseconds and packet loss rates greater than 0.01% (1 in 10,000).
- Operates on individual TCP connections. Evaluates each inbound and outbound network connection to determine whether the performance can be improved.
- Improves the network performance with minimal dependency on the outbound network traffic.
- Improves the network performance of optimized duplications.

- Improves the network performance of restores to remote clients.
- Imposes no network overhead. WAN optimization is non-intrusive, as it does not impose any network overhead in situations where the overall network data transfers are high. In some scenarios, when the overall network data transfer is high, the connection speed may not be optimized despite this feature being enabled.

Note: If you run a factory reset of the appliance, note the following:

A factory reset disables WAN optimization for all network interface bonds when you retain your network configuration. To retain your network configuration, you can select **Retain network configuration** in the NetBackup Appliance Web Console (**Manage > Appliance Restore > Retain network configuration**). After the factory reset completes, you can then enable WAN optimization again for the network interface bonds.

If you choose *not* to retain your network configuration, all network interface bonds are lost during the factory reset. After the reset completes, the appliance automatically enables WAN optimization for all network interface ports, including those that comprised the bonds.

OPTIONS

Enable ALL

Enable WAN optimization for all appliance network interface ports and NIC bonds at the same time.

You can also optimize NIC bonds with this command. Bonds consist of two or more physical NIC/eth ports that have been teamed together to form a logical network port. The logical network port is called a bond.

Note: When configuring multiple network interfaces as a NIC bond, use the NetBackup Appliance Shell Menu `Network > LinkAggregation` to comprise the bond. You can also use the **Network** page of the NetBackup Appliance Web Console (**Settings > Network > Network Configuration > Create Bond**). NIC bonds that are configured with tools other than the above mentioned appliance tools appear as *Disabled* when you run the WAN optimization `Status` command. They also appear as *Disabled* when you view them in the NetBackup Appliance Web Console.

Use either the NetBackup Appliance Shell Menu or the NetBackup Appliance Web Console to enable these NIC bonds.

The following example shows how to use the `Enable ALL` command:

```
myappliance1.WANOptimization> Enable ALL (provided the ports are not  
part of a bond)
```

`Enable interfaceList`

Enable WAN optimization for selected network interface (NIC/eth) ports on the appliance.

interfaceList specifies the selected NIC ports or NIC bonds.

Note: Individual NIC ports cannot be optimized for WAN communications if they are teamed in a NIC bond. When you enable WAN optimization for a bond, WAN optimization is applied to each NIC port in the bond.

The following are examples of how to use the `Enable` command and its parameters:

- `myappliance1.WANOptimization> Enable eth2` (provided the port is not part of a bond)
- `myappliance1.WANOptimization> Enable bond0`
- `myappliance1.WANOptimization> Enable eth0,eth1` (provided the ports are not part of a bond)
- `myappliance1.WANOptimization> Enable bond1,bond2`
- `myappliance1.WANOptimization> Enable eth0,bond1` (provided the port is not part of a bond)

`Disable ALL`

Disable WAN optimization for all appliance network interface ports and NIC bonds at the same time.

The following example shows how to use the `Disable ALL` command:

```
myappliance1.WANOptimization> Disable ALL
```

`Disable interfaceList`

Disable WAN optimization for selected network interface (NIC/eth) ports on the appliance.

You can also disable WAN optimization for NIC bonds with this command. Bonds consist of two or more physical NIC/eth ports that have been teamed together to form a logical network port. The logical network port is called a bond.

interfaceList specifies the selected NIC ports or NIC bonds.

Note: `interfaceList` lets you disable WAN optimization for selected NIC ports or NIC bonds, unless the selected port has been teamed together with another port to form a bond. To disable WAN optimization for the ports within the bond, you must specify the bond name when you run the `Disable` command.

The following are examples of how to use the `Disable` command and its parameters:

- `myappliance1.WANOptimization> Disable eth2` (provided the port is not part of a bond)
- `myappliance1.WANOptimization> Disable bond0`
- `myappliance1.WANOptimization> Disable eth0,eth1` (provided the ports are not part of a bond)
- `myappliance1.WANOptimization> Disable bond1,bond2`
- `myappliance1.WANOptimization> Disable eth0,bond1` (provided the port is not part of a bond)

Note: When you disable WAN optimization for a bond, WAN optimization is disabled for each port within the bond.

WANOptimization > Status

Shows the current WAN optimization status.

The appliance displays the optimization status in a table that resembles the following example:

Bond	Interface	State	IPv4 Address	IPv6 Address	WAN Optimization
bond0	eth3	Plugged			Enabled
	eth4	Plugged			
	eth5	Plugged			
	eth6	Plugged			
bond1	eth7	Plugged			Enabled
	eth8	Plugged			
	eth9	Plugged			
	eth0	Plugged			Enabled
	eth1	Plugged	10.200.71.130		Enabled
	eth2	Plugged		dc81::250:56ff:fe72:3a4e	Enabled

Main > Network > Security commands (IPsec)

This appendix includes the following topics:

- [Network > Security > Configure](#)
- [Network > Security > Delete](#)
- [Network > Security > Export](#)
- [Network > Security > Import](#)
- [Network > Security > Provision](#)
- [Network > Security > Refresh](#)
- [Network > Security > Show](#)
- [Network > Security > Unconfigure](#)

Network > Security > Configure

Network > Security > Configure – Configure IPsec between any two hosts.

SYNOPSIS

```
Configure Host1Info [Host2Info]
```

DESCRIPTION

You can use this command to configure IPsec between any two hosts. You can define the hosts by the host name. You can also identify them by the user ID and password.

OPTIONS

```
Configure Host1Info [Host2Info]
```

Use this command to configure IPsec between any two hosts. The *Host1Info* variable can contain the following information that is separated by a comma. The host name, the user ID (optional), and the password (optional). The [*Host2info*] variable can contain the host name, the user ID (optional), and the password (optional).

Network > Security > Delete

`Network > Security > Delete` – Remove IPsec policies for a list of remote hosts on a local system.

SYNOPSIS

`Delete Hosts`

DESCRIPTION

You can use this command to remove IPsec policies for a list of remote hosts on a local system.

OPTIONS

`Delete Hosts`

Remove IPsec policies for a list of remote hosts on a local system. Use the *Hosts* variable to define one or more host names. Use a comma to separate multiple host names.

Network > Security > Export

Network > Security > Export – Export the IPsec credentials.

SYNOPSIS

```
Export [EnterPasswd] [PathValue]
```

DESCRIPTION

Use this command to export the IPsec credentials to a specified location.

Note: The IPsec credentials are removed during a reimage process. The credentials are unique for each appliance and are included as part of the original factory image.

The IPsec credentials are not included on the USB drive that is used to reimage the appliance.

OPTIONS

```
Export [EnterPasswd] [PathValue]
```

Use this command to export the IPsec credentials. The `EnterPasswd` field is used to answer the question, "Do you want to enter a password?". You must enter a value of **yes** or **no** in this field. In addition, you must specify a path that defines where you want to place the exported credentials.

Network > Security > Import

Network > Security > Import – Import the IPsec credentials.

SYNOPSIS

```
Import [EnterPasswd] [PathValue]
```

```
Import
```

DESCRIPTION

On 5230, 5240, 5330, and 5340 NetBackup Appliances, you can use the `Import [EnterPasswd] [PathValue]` command to import the IPsec credentials to a specified location.

On 5250 NetBackup Appliances, a copy of the IPsec credentials is stored on the SSD. You can use the `Import` command to import the IPsec credentials from the SSD.

OPTIONS

```
Import [EnterPasswd] [PathValue]
```

On 5230, 5240, 5330, and 5340 NetBackup Appliances, you can use this command to import the IPsec credentials. The `EnterPasswd` field is used to answer the question, "Do you want to enter a password?". You must enter a value of **yes** or **no** in this field. In addition, you must specify a path that defines where you want to place the imported credentials.

```
Import
```

On 5250 NetBackup Appliances, IPsec credentials that are unique for each appliance and are included as part of the original factory image. Because IPsec credentials are removed during a reimage or factory reset process, you can use this command to automatically import the IPsec credentials to enable secure communication between appliances.

Network > Security > Provision

`Network > Security > Provision` – Provision IPsec policies for a list of remote hosts on a local system.

SYNOPSIS

`Provision Hosts`

DESCRIPTION

Use this command to provision IPsec policies for a list of remote hosts on a local system.

OPTIONS

`Provision Hosts`

Provision IPsec policies for a list of remote hosts on a local system. Use the *Hosts* variable to define one or more host names. Use a comma to separate multiple host names.

Network > Security > Refresh

Network > Security > Refresh – Use to reload the IPsec configuration.

SYNOPSIS

```
Refresh [Auto]
```

DESCRIPTION

Use this command to reload the IPsec configuration. With auto-refresh, refresh the configurations on all referenced hosts. The default setting for this command is `NoAuto`.

OPTIONS

```
Refresh [Auto]
```

Use this command to reload the IPsec configuration. The [Auto] options defines whether the configurations on all referenced hosts are refreshed or not. You can enter **Auto** or **NoAuto**. The default value is **NoAuto**.

Network > Security > Show

`Network > Security > Show` – Display the IPsec policies for a local host or a provided host.

SYNOPSIS

```
Show [Verbose] [HostInfo]
```

DESCRIPTION

You can use this command to display the IPsec policies for a local host or a provided host. You can define whether the output is verbose or not. And you define the host.

OPTIONS

```
Show [Verbose] [HostInfo]
```

Display the IPsec policies for a local host or a provided host. The `[Verbose]` options is used to define whether the output is verbose or not. The values that you can enter in this field are `VERBOSE` or `NOVERBOSE`. The default value is `NOVERBOSE`.

The `[HostInfo]` option can contain the following information that is separated by a comma. The host name, the user ID (optional), and the password (optional).

Network > Security > Unconfigure

Network > Security > Unconfigure – Unconfigure IPsec between any two hosts.

SYNOPSIS

```
Unconfigure Host1Info [Host2Info]
```

DESCRIPTION

You can use this command to unconfigure IPsec between any two hosts.

OPTIONS

```
Unconfigure Host1Info [Host2Info]
```

Use this command to unconfigure IPsec between any two hosts. The *Host1Info* variable can contain the following information that is separated by a comma. The host name, the user ID (optional), and the password (optional). The [*Host2info*] variable can contain the host name, the user ID (optional), and the password (optional).

Main > Reports commands

This appendix includes the following topics:

- [Reports > Deduplication](#)
- [Reports > Process](#)

Reports > Deduplication

Reports > Deduplication – Show the deduplication statistics for the appliance.

SYNOPSIS

```
Deduplication
```

DESCRIPTION

Use this command to show the deduplication statistics for the appliance.

OPTIONS

```
Deduplication
```

Shows the deduplication statistics for the appliance.

EXAMPLES

The following command shows an example of how the Deduplication statistics are displayed.

```
abc123.Reports> Deduplication
```

```
Deduplication statistics
Deduplication technology  MSDP
Deduplication rate       79.019%
Data Protected           301622 MB
Space Used For Protection 63282 MB
Physical free space      9735902 MB
Logical free space       0 MB
Total free space         9735902 MB
Maximum Disk Space       10065305 MB
Used Disk Space          329402 MB
```

Reports > Process

Reports > Process – Show the status of a current process.

SYNOPSIS

Process

DESCRIPTION

Use this command to show the status of a current process.

OPTIONS

Process

Show the status of a current process.

EXAMPLES

The following is an example output of the Process command.

```
Reports> Process
NB_dbsrv:      Down          bpcd:          Running Responding
bpdbm:         Down          bpjobd:        Down
bprd:          Down          nbars:         Down
nbemm:         Down          nbjm:          Down
nbpem:         Down          nbrb:          Down
nbrmms:        Running       nbsl:          Running
nbstserv:      Down          nbsvcmon:      Running
postmaster:    Running       spad:          Running
spoold:        Running       vmd:           Running Responding
vnetd:         Running
```


Main > Settings commands

This appendix includes the following topics:

- [Settings > Cloud](#)
- [Settings > Deduplication](#)
- [Settings > FibreTransport](#)
- [Settings > iSCSI > Initiator](#)
- [Settings > iSCSI > Interface](#)
- [Settings > iSCSI > Target](#)
- [Settings > LogForwarding](#)
- [Settings > LifeCycle](#)
- [Settings > NetBackup](#)
- [Settings > NetBackup DNAT](#)
- [Settings > Password](#)
- [Settings > Share](#)
- [Settings > SNMP polling](#)
- [Settings > Sysctl](#)
- [Settings > SystemLocale](#)

Settings > Cloud

Settings > Cloud – Manage cloud storage server settings.

SYNOPSIS

Credentials

DESCRIPTION

Note: Starting with appliance software version 3.2, this command is no longer available. To manage credentials settings on a CloudCatalyst appliance, first create a NetBackup CLI user, then use the `tpconfig` command. To create a NetBackup CLI user, see the *NetBackup Appliance Administrator's Guide*. For information about the `tpconfig` command, see the *Veritas NetBackup Commands Reference Guide*.

Note: This command is only present after you configure the appliance to use NetBackup CloudCatalyst.

Use this command to manage a limited number of settings for CloudCatalyst on the appliance.

OPTIONS

Credentials

Edit access details (credentials) for the currently configured cloud provider. For example, use this command if you want to change the access key ID and secret access key for an Amazon S3 account.

EXAMPLES

```
nb-appliance.Settings> Cloud Credentials
Cloud storage provider - Amazon S3
>> Enter access key ID:
>> Enter secret access key:
- [Info] The Amazon S3 credentials have been updated successfully.
```

Settings > Deduplication

Settings > Deduplication – Change the deduplication parameters.

SYNOPSIS

Defaults

Show

Tune BACKUPRESTORERANGE *Addresses*

Tune BANDWIDTH_LIMIT *Limit*

Tune COMPRESSION *Comp*

Tune DONT_SEGMENT_TYPES Append *FileTypes*

Tune DONT_SEGMENT_TYPES Change *FileTypes*

Tune ENCRYPTION *Value*

Tune LOCAL_SETTINGS *Override*

Tune LOGLEVEL *Value*

Tune MAX_IMG_MBSIZE *Value*

Tune MAX_LOG_MBSIZE *Value*

Tune OPTDUP_BANDWIDTH *Value*

Tune OPTDUP_COMPRESSION *Value*

Tune OPTDUP_ENCRYPTION *Value*

Tune OPTDUP_TIMEOUT *Time*

Tune WS_RETRYCOUNT *Count*

Tune WS_TIMEOUT *Time*

DESCRIPTION

You can use the `Deduplication` command with the `Default` and `Show` options to display the default values for each of the `Deduplication` parameters and the current parameter values, respectively. You can use the `Deduplication Tune` command to adjust the following parameters:

Table R-1 Deduplication parameters and default values

Setting	Default value	Possible values	Action
BACKUPRESTORERANGE	N/A	Classless Inter-Domain Routing format or comma-separated list of IP addresses	Specifies the IP address or range of addresses of the local network interface card (NIC) for backups and restores.
BANDWIDTH_LIMIT	0	0 (no limit) to the practical system limit, in KBs/sec	Determines the maximum bandwidth that is allowed when backing up or restoring data between the media server and the deduplication pool. The value is specified in KBytes/second. The default is no limit.
COMPRESSION	1	0 (off) or 1 (on)	Specifies whether you want compression. Default is set to compress files. If you do not want compression, change the value to 0.

Table R-1 Deduplication parameters and default values (*continued*)

Setting	Default value	Possible values	Action
DONT_SEGMENT_TYPES	N/A	Any file extension	<p>You can specify a list of comma-separated file name extensions. Files in the backup stream that have the specified extensions are given a single segment if smaller than 16 MB. Larger files are deduplicated using the maximum 16-MB segment size.</p> <p>Example:</p> <pre>DONT_SEGMENT_TYPES = mp3,avi</pre> <p>This setting prevents NetBackup from analyzing and managing segments within the file types that do not deduplicate globally.</p>
ENCRYPTION	0	0 (off) or 1 (on)	<p>Specifies whether to encrypt the data. Default is set to not encrypt files. If you want encryption, change the value to 1.</p> <p>If you set this parameter to 1 on all hosts, the data is encrypted during transfer and in the storage.</p>

Table R-1 Deduplication parameters and default values (*continued*)

Setting	Default value	Possible values	Action
LOCAL_SETTINGS	0	0 (allow override) or 1 (always use local settings)	Specifies whether to allow the <code>pd.conf</code> settings of the deduplication storage server to override the settings in the local <code>pd.conf</code> file.
LOGLEVEL	0	An integer, 0 to 10 inclusive	Specifies the amount of information that is written to the log file. The range is from 0 to 10, with 10 being the most logging. Note: Only change this value if a Veritas representative directs you to do so.
MAX_IMG_MBSIZE	50,000	0 to 50,000, in MBs	The maximum backup image fragment size in megabytes. Note: Only change this value if a Veritas representative directs you to do so.
MAX_LOG_MBSIZE	500	0 to 50,000, in MBs	The maximum size of the log file in megabytes.
OPTDUP_BANDWIDTH	0	0 (no limit) to the practical system limit, in KBs/sec	Determines the maximum bandwidth that is allowed for optimized duplication. The value is specified in KBytes/second.

Table R-1 Deduplication parameters and default values (*continued*)

Setting	Default value	Possible values	Action
OPTDUP_COMPRESSION	1	0 (off) or 1 (on)	Specifies whether to compress optimized duplication data. Default is set to not compress files. If you want compression, change the value to 1.
OPTDUP_ENCRYPTION	0	0 (off) or 1 (on)	<p>Specifies whether to encrypt the optimized duplication data. Default is set to not encrypt files. If you want encryption, change the value to 1.</p> <p>If you set this parameter to 1 on all hosts, the data is encrypted during transfer and on the storage.</p>
OPTDUP_TIMEOUT	N/A	expressed in minutes	Specifies the number of minutes before the optimized duplication times out. Indicated in minutes.
WS_RETRYCOUNT	3	Integer	<p>This parameter applies to the PureDisk Deduplication Option only. It does not affect NetBackup deduplication.</p> <p>The <code>WSRetryCount</code> parameter lets you configure the amount of retries that are attempted in case the Web service fails or times out.</p>

Table R-1 Deduplication parameters and default values (*continued*)

Setting	Default value	Possible values	Action
WS_TIMEOUT	120	Integer	<p>This parameter applies to the PureDisk Deduplication Option only. It does not affect NetBackup deduplication.</p> <p>The <code>WSTimeout</code> parameter lets you increase or decrease the timeout value for Web service calls made from NetBackup media servers to PureDisk storage units.</p>

OPTIONS

Deduplication Defaults

Display the default values for the Deduplication parameters.

Deduplication Show

Display the current values for the Deduplication parameters.

Deduplication Tune BACKUPRESTORERANGE *Addresses*

Specify the IP addresses or range of addresses of the local network interface card for backup and restore. The *Addresses* variable contains an IP addresses list or a range of addresses.

Deduplication Tune BANDWIDTH_LIMIT *Limit*

The maximum bandwidth that is allowed when backing up or restoring data between the media server and the deduplication pool. The *limit* variable contains the maximum bandwidth limit. The value for this variable is in KBytes/second.

Deduplication Tune COMPRESSION *Comp*

Whether you want compression. The *Compression* variable lets you enable or disable compression. You enter either `Enable` or `Disable`.

Deduplication Tune DONT_SEGMENT_TYPES Append *FileTypes*

Append new file types to the list of file types that NetBackup does not analyze or manage segments. The *FileTypes* variable lists the file types.

Deduplication Tune DONT_SEGMENT_TYPES Change *FileTypes*

Change the whole list of file types. The *FileTypes* variable lists the file types.

Deduplication Tune ENCRYPTION *Value*

Specify whether you want to encrypt the data. Use the *Value* variable to enable or disable encryption. The values that you can enter are *Enable* or *Disable*.

Deduplication Tune LOCAL_SETTINGS *Override*

Whether to allow settings of the deduplication server to override the local settings. The *Override* variable determines whether to allow an override to occur. The values that you can enter in this field are *AllowOverride* or *UseLocalSetting*.

Deduplication Tune LOGLEVEL *Value*

The amount of information that is written to the log file. The *Value* variable sets the range from 0 to 10. A value of 10 provides the most logging.

Deduplication Tune MAX_IMG_MBSIZE *Value*

Set the maximum backup image fragment size. The *Value* variable contains the maximum size of the backup image fragment in megabytes. You can enter a value between zero and 50000.

Deduplication Tune MAX_LOG_MBSIZE *Value*

Set the maximum size of the log file. The *Value* variable contains the maximum size of the log file in megabytes. You can enter a value between zero and 50000.

Deduplication Tune OPTDUP_BANDWIDTH *Value*

The maximum bandwidth that is allowed for optimized duplication. The *Value* variable contains the maximum bandwidth in KBs/sec.

Deduplication Tune OPTDUP_COMPRESSION *Value*

Whether to compress the optimized duplication data. The *Value* variable lets you enable or disable compression. The values for this field are: *Enable* or *Disable*.

Deduplication Tune OPTDUP_ENCRYPTION *Value*

Whether to encrypt the optimized duplication data. The *Value* variable lets you enable or disable encryption. The values for this field are: *Enable* or *Disable*.

Deduplication Tune OPTDUP_TIMEOUT *Time*

The number of minutes before the optimized duplication times out. The *Time* variable is the number of minutes before the optimized duplication times out.

Deduplication Tune WS_RETRYCOUNT *Count*

The amount of retries that are attempted in case the Web service fails or times out. The *Count* variable is the amount of retries that are attempted in case the Web service fails or times out.

Deduplication Tune WS_TIMEOUT *Time*

The timeout value for Web service calls made from NetBackup media servers to PureDisk storage units. The *Time* variable is the timeout value for Web service calls made from NetBackup media servers to PureDisk storage units.

EXAMPLES

The `Defaults` command shows the values of each of the Deduplication parameters:

```
Deduplication> Defaults
BACKUPRESTORERANGE      : N/A
BANDWIDTH_LIMIT         : 0
COMPRESSION              : 1
DONT_SEGMENT_TYPES      : N/A
ENCRYPTION               : 0
LOCAL_SETTINGS          : 0
LOGLEVEL                 : 0
MAX_IMG_MBSIZE           : 50000
MAX_LOG_MBSIZE           : 500
OPTDUP_BANDWIDTH        : 0
OPTDUP_COMPRESSION       : 1
OPTDUP_ENCRYPTION        : 0
OPTDUP_TIMEOUT           : N/A
SEGKSIZE                 : 128
WS_RETRYCOUNT           : 3
WS_TIMEOUT               : 120
```

Settings > FibreTransport

Settings > FibreTransport – Administer Fibre Transport for this appliance.

SYNOPSIS

```
FibreTransport NBUAppliances Disable
FibreTransport NBUAppliances Enable
FibreTransport NBUAppliances Show
FibreTransport SANClient Disable
FibreTransport SANClient Enable
FibreTransport SANClient Show
FibreTransport Deduplication Disable
FibreTransport Deduplication Enable FactoryDefault
FibreTransport Deduplication Enable [Current]
FibreTransport Deduplication Show
```

DESCRIPTION

Use this command to do the following:

- administer Fibre Transport for SAN client backups and restores
- administer Fibre Transport for duplication to another appliance
- administer Fibre Transport for duplication on this appliance as a target host

Note: To use this appliance as a target host, you must enable the NBUAppliances service on the source host(s). To enable that service, log on to the source appliance, and run the `Main > Settings> FibreTransport NBUAppliances Enable` command from the NetBackup Appliance Shell Menu.

Note: You must restart the appliances in the FC zone if you have caused the physical state of a port in the zone to change by disabling or enabling this appliance as a target host for data duplication.

See [Manage > FibreChannel > Show](#) on page 52.

OPTIONS

`FibreTransport NBUApliances Disable`

Disable Fibre Transport for duplication to another appliance. By default, Fibre Transport to another appliance is disabled.

This option restarts the deduplication storage daemons. Therefore, any active backup, restore, or duplication jobs fail.

`FibreTransport NBUApliances Enable`

Enable Fibre Transport for duplication to another appliance.

This option restarts the deduplication storage daemons. Therefore, any active backup, restore, or duplication jobs fail.

`FibreTransport NBUApliances Show`

Display the status of the Fibre Transport services to another appliance.

`FibreTransport SANClient Disable`

Disable Fibre Transport for SAN client backups and restores to this appliance. By default, Fibre Transport for backups and restores is disabled.

This option restarts the NetBackup SAN client daemons. Therefore, any active backup, restore, or duplication jobs fail.

`FibreTransport SANClient Enable`

Enable Fibre Transport for SAN client backups and restores to this appliance.

This option restarts the NetBackup SAN client daemons. Therefore, any active backup, restore, or duplication jobs fail.

`FibreTransport SANClient Enable [2|4]`

Enable Fibre Transport for SAN Client backups and restores to this appliance.

By default, the feature is disabled on new appliances or on appliances that have been factory reset.

The available port number settings are optional, since they are typically configured using the `Manage > FibreChannel > Configure` command. The options are as follows:

- No ports specified
If you enter the command without specifying the number of ports, the feature is enabled but the port configuration does not change. For new appliances or appliances that have been factory reset, the port configuration remains at 2 by default.
- 2
Sets Port 1 to the target mode on the following FC HBA cards:
NetBackup 5230 and 5330 - cards in slots 5 and 6

NetBackup 5340 - cards in slots 1, 2, 4, 5, 6 depending on the I/O configuration

- 4

Sets Ports 1 and 2 to the target mode on the following FC HBA cards:

NetBackup 5230 and 5330 - cards in slots 5 and 6

NetBackup 5340 - cards in slots 1, 2, 4, 5, 6 depending on the I/O configuration

Changing this option restarts the NetBackup SAN client daemons. Therefore, any active backup, restore, or duplication jobs fail.

`FibreTransport SANClient Show`

Display the status of the Fibre Transport server for SAN client backups and restores.

`FibreTransport Deduplication Disable`

Disable Fibre Transport on the appliance as a target host for optimized duplication and Auto Image Replication. This reverts the physical state of all the target mode ports to initiator.

`FibreTransport Deduplication Enable FactoryDefault`

Enable Fibre Transport on the appliance as a target host for optimized duplication and Auto Image Replication. The factory default port configuration is used.

When the feature has been enabled, you can use this command to restore the customized port configuration to the factory default state.

Note: This command restarts the Deduplication service if the feature state is changed from disabled to enabled. The service restart causes the ongoing jobs to fail, and then failover to LAN. Veritas recommends that you cancel or suspend all jobs before changing the feature state.

`FibreTransport Deduplication Enable [Current]`

Enable Fibre Transport on the appliance as a target host for optimized duplication and Auto Image Replication. The preexisting port configuration is used.

If no HBA port has been configured before you enable this feature, the factory default port configuration is used.

Note: This command restarts the Deduplication service if the feature state is changed from disabled to enabled. The service restart causes the ongoing jobs to fail, and then failover to LAN. Veritas recommends that you cancel or suspend all jobs before changing the feature state.

FibreTransport Deduplication Show

Show whether the appliance is enabled as a target host for optimized duplication and Auto Image Replication.

EXAMPLES

The following is an example of information when you run the `FibreTransport SANClient Show` command.

```
- [Info] Fibre Transport Sever enabled.
```

The following is an example of information when you run the `FibreTransport NBUAppliances Show` command.

```
fc transport enabled.
```

The following is an example of information when you run the `FibreTransport Deduplication Disable` command.

```
[Info] Fibre Transport Deduplication is disabled.
```

The following is an example of information when you run the `FibreTransport Deduplication Enable` command.

```
[Info] Fibre Transport Deduplication is enabled.
```

The following is an example of information when you run the `FibreTransport Deduplication Show` command.

```
[Info] Fibre Transport Deduplication is disabled.
```

Settings > iSCSI > Initiator

Settings > iSCSI > Initiator – Monitor and manage iSCSI for this appliance.
iSCSI is only supported on configuration H of the NetBackup 5240 appliances.

SYNOPSIS

```
Initiator Set IQN IQN
```

```
Initiator Show IQN
```

DESCRIPTION

The `Initiator Set` and `Initiator Show` commands can help you to configure and view the iSCSI Qualified Name (or IQN) for the initiator.

OPTIONS

```
Initiator Set IQN IQN
```

This command sets the IQN for the NetBackup Appliance (initiator).

Note the following about IQN:

- The IQN must be up to 255 characters long.
- The IQN can only contain numbers (0-9), letters (A-Z and a-z), colons (:), hyphens (-), and periods (.).

Example: `iqn.1999-06.com.veritas:storage.lun1`

```
Initiator Show
```

Displays the IQN for the NetBackup appliance.

EXAMPLES

The following are example outputs when you run the `iSCSI > Initiator` commands:

```
appliance.iSCSI> Initiator Set IQN iqn.1996-06.com.veritas:abc  
- [Info] The IQN has been updated to iqn.1996-06.com.veritas:abc
```

```
appliance.iSCSI > Initiator Show IQN  
- [Info] Initiator IQN: iqn.1996-06.com.veritas:abc
```

Settings > iSCSI > Interface

Settings > iSCSI > Interface—The `iSCSI Interface Set`, `iSCSI Interface Remove` and `iSCSI Interface Show` commands can help you to configure the properties like gateway, IP address, MTU, Netmask, and VLAN for an iSCSI interface.

SYNOPSIS

```
iSCSI Interface Show

iSCSI Interface IPAddress Set IP address Interface name

iSCSI Interface Netmask Set Netmask Interface Name

iSCSI Interface Gateway Set Gateway Interface Name

iSCSI Interface MTU Set MTU Interface Name

iSCSI Interface VLAN Set VLAN ID Interface Name

iSCSI Interface IPAddress Remove Interface Name

iSCSI Interface Netmask Remove Interface Name

iSCSI Interface Gateway Remove Interface Name

iSCSI Interface MTU Reset Interface Name

iSCSI Interface VLAN Remove Interface Name
```

DESCRIPTION

The `iSCSI Interface Set`, `iSCSI Interface Remove` and `iSCSI Interface Show` commands can help you to configure the interface properties like Gateway, IP address, MTU, Netmask, and VLAN for an iSCSI interface.

OPTIONS

`Interface Show`

This command lets you view the interface properties.

`Interface IPAddress Set IP address Interface Name`

This command configures the IP address for the iSCSI interface. Only IPv4 addresses are supported.

`Interface Netmask Set Netmask Interface Name`

This command configures the Netmask for the iSCSI interface. You may optionally enter the iSCSI interface name that you want to configure. Run `iSCSI > Interface Show` to view all the available iSCSI interfaces.

Note the following about interface names:

- It can only contain numbers (0-9), letters (A-Z and a-z), colons (:), hyphens (-), underscores (_) and periods (.).
It must begin with numbers (0-9), letters (A-Z and a-z) and underscores (_) only.
Example: `iscsi.1`

`Interface Gateway Set Gateway Interface Name`

This command configures the gateway for the iSCSI interface. You may optionally enter the iSCSI interface name that you want to configure.

`Interface MTU Set MTU value Interface Name`

This command configures the MTU for the iSCSI interface. The MTU controls the maximum transmission unit size for an Ethernet frame. It must be a number from 68 to 65535. Note that when you configure the MTU for an iSCSI interface, the new MTU value is configured for both the iSCSI interface and the network interface to which it is mapped.

`Interface VLAN Set VLAN ID Interface name`

This command configures VLAN ID for the iSCSI interface. If you want to configure VLAN, you should configure it either on the network interface or on the iSCSI interface and not both. If you configure the VLAN for both the iSCSI and the network interface, the VLAN value that is configured for the network interface applies. You may choose to not configure VLAN on either the network or the iSCSI interface.

The VLAN ID must be a number from 1 to 4095.

`Interface IPAddress Remove Interface Name`

This command removes the IP address from the specified interface.

`Interface Netmask Remove Interface Name`

This command removes the Netmask from the specified interface.

`Interface Gateway Remove Interface Name`

This command removes the gateway from the specified interface.

`Interface MTU Reset Interface Name`

This command resets MTU to the default value (1500) on both the iSCSI interface and the network interface to which it maps. The MTU cannot be removed and can only be reset to its default value.

EXAMPLES

```
appliance.iSCSI> Interface Show
Showing the available interfaces...
```

Interface Name	Network Interface	MAC Address	IP Address	Netmask	Gateway	MTU	VLAN Tag
iscsi1	eth6	00:0e:1e:53:55:11	10.181.198.62			1500	
iscsi2	eth7	00:0e:1e:53:55:13				1500	

```
appliance.iSCSI> Interface IPAddress Set 10.181.198.40 iscsi2
- [Info] The IP address has been configured for iscsi2.
```

```
appliance.iSCSI> Interface IPAddress Remove iscsi2
- [Info] The IP address has been removed from iscsi2.
```

```
appliance.iSCSI> Interface MTU Set 2000 iscsi1
```

The new MTU value applies to both iscsi1 and also the network interface eth8.
Do you want to continue? (yes,no) [no]:yes
- [Info] The MTU has been configured for iscsi1 and eth8.

Settings > iSCSI > Target

Settings > iSCSI > Target – These commands help you to manage the connections between an initiator and targets.

SYNOPSIS

Target Discover Portal IP: [port] Interface name

Target Discover iSNS iSNS address Interface name

Target Connect Target IQN

Target Disconnect Target IQN

Target Show All

Target Show Connected

DESCRIPTION

- The `iSCSI Target Connect` or `iSCSI Target Disconnect` commands can help you to connect to or disconnect from a target device.
- You can discover targets by using the target portal address or the iSNS address (Internet Storage Name Service).
The `Target Discover Portal` command can help you discover targets by using the target portal address.
The `Target Discover iSNS` command can help you discover targets by using the iSNS server.
- The `Target Show` command displays all of the targets or the connected targets.

OPTIONS

Target Discover Portal IP: [port] Interface name

Run this command to discover iSCSI targets by using the target portal address. You are asked to provide a username and password. Type **yes** if your target requires authentication. The targets that are available on the specified portal address and interface are discovered and displayed.

Note the following considerations:

- The target portal address must be of the following format: <IPv4 address/hostname>[:port]. The host name can be a short name or a fully qualified domain name. Example: 192.116.116.50 or abc:3260.

- The iSCSI interface name can only contain numbers (0-9), letters (A-Z and a-z), colons (:), hyphens (-), underscores (_) and periods (.). It must begin with numbers (0-9), letters (A-Z and a-z) and underscores (_) only.

You must first discover a target in order to connect to it.

Note: If you run the `Target Discover Portal` or the following `Target Discover iSNS` command again after the targets are connected, it overrides the existing connection settings like target credentials. If the target requires authentication, you need to enter the target credentials again when the existing sessions are reconnected. The existing sessions need to be reconnected if the appliance restarts, or when you change the IQN for the appliance, or when the iSCSI processes are restarted, etc.

`Target Discover iSNS iSNS address Interface name`

Use this command to discover iSCSI targets by using the Internet storage name service (iSNS) method. Use this method if you have at least one iSNS server on your network. This method enables the iSCSI initiator to discover targets that are registered to the iSNS server. You must supply the iSNS server address and/or port. The iSCSI initiator can then query the specified iSNS server to discover targets. The default port for an iSNS server is 3205.

`Target Connect Target IQN [Portal Address] [Interface Name]`

After initiator and target connections are discovered, iSCSI initiators must be logged on to targets to establish connections and transfer data over iSCSI. To connect an initiator to a single target, specify the target IQN. Optionally, you may enter the portal address and the iSCSI interface name. Enter a user name and password if the target needs authentication.

Note the following about IQN, portal address, and user name:

- The IQN can only contain numbers (0-9), letters (A-Z and a-z), colons (:), hyphens (-), and periods (.). Example: `iqn.1999-06.com.veritas:storage.lun1`
- The target portal address must be of the following format: `<IP address/hostname>[:port]`. Only IPv4 addresses are supported. The host name can be a short name or a fully qualified domain name. Example: `192.116.116.50` or `abc:3260`.
- The user name can only contain numbers (0-9), letters (A-Z and a-z), hyphens (-), underscores (_), and periods (.). It must begin with numbers (0-9), letters (A-Z and a-z), and underscores (_) only. Example: `john.smith`.

`Target Disconnect Target IQN Portal Address`

Disconnects the target session that has the specific IQN and portal address. Other sessions that are connected to the target will not be affected.

Target Show All

Use this command to view all the discovered targets.

Note: When targets are discovered by using iSNS on two iSCSI interfaces like first run the `Target Discover iSNS` command for *iscsi1* and then *iscsi2*, only the recent record is displayed by the `Target Show All` command. For example, the **Interfaces** column in the `Target Show All` command may not show both the interfaces (*iscsi1*, *iscsi2*) for some targets. It actually shows the interface from the most recent command (*iscsi2* in this case) for some targets.

Target Show Connected

Use this command to view the connected targets.

EXAMPLES

The following are example outputs when you run the iSCSI > Target command:

```
appliance.iSCSI> Target Discover Portal 10.182.35.51 iscsi1
```

```
Does your target require a username and password? (yes,no)[no]:no
```

```
Showing the discovered targets...
```

No.	Target IQN	Target Portal Address	Interfaces
1	iqn.1996-03.veritas:abc	10.121.98.22:3260	iscsi1, iscsi2
2	iqn.1996-03.veritas:xyz	10.121.98.23:3260	iscsi1, iscsi2
3	iqn.1996-03.veritas:host	10.121.98.24:3260	iscsi1, iscsi2

```
appliance.iSCSI > Target Show All
```

```
Showing all the targets...
```

No.	Target IQN	Target Portal Address	Interfaces
1	iqn.1996-03.veritas:abc	10.121.98.22:3260	iscsi1
2	iqn.1996-03.veritas:xyz	10.121.98.23:3260	iscsi1

	3	iqn.1996-03.veritas:host	10.121.98.24:3260		iscsi1	
-----		-----		-----		-----

Settings > LogForwarding

Settings > LogForwarding – Enable/disable, and manage settings to forward logs to an external log management server.

SYNOPSIS

```
LogForwarding Enable
LogForwarding Disable
LogForwarding Interval
LogForwarding Share
LogForwarding Show
```

DESCRIPTION

Use this command to forward appliance logs to an external management server. Currently, only syslog forwarding is supported.

OPTIONS

```
LogForwarding Enable
```

Enable syslog forwarding functionality on the appliance. The command requires you to specify the following:

- Target server name or IP address
- Server port
- Protocol (UDP/TCP)
- Forwarding interval in minutes (0/15/30/45/60)
- Enabling TLS (yes/no)

```
LogForwarding Interval
```

Set or change how often syslogs are forwarded as follows:

- **0 (continuous)** - Forward syslogs as they are generated.
- **15 minutes** - Forward the syslogs every 15 minutes.
- **30 minutes** - Forward the syslogs every 30 minutes.
- **45 minutes** - Forward the syslogs every 45 minutes.
- **60 minutes** - Forward the syslogs every 60 minutes.

LogForwarding Share Open

Open NFS and CIFS shares to **/inst/logforwarding** on the appliance. Make sure that you have uploaded valid certificates to an opened share before you enable the TLS on the appliance. Two certificates and one private key are required as follows:

- ca-server.pem
- nba-rsyslog.pem
- nba-rsyslog.key

LogForwarding Share Close

Close the NFS and CIFS shares to **/inst/logforwarding** on the appliance for security purpose.

LogForwarding Show

View the status of the current log forwarding configuration.

LogForwarding Disable

Disable the Log Forwarding feature and delete the current log forwarding configuration.

EXAMPLES

Example 1 - Enable syslog forwarding on the appliance using TLS.

```
abc123.LogForwarding> enable
- [Info] Only syslog forwarding is supported at this time.
>> Enter server name or IP address: Veritas
>> Enter server port: 514
>> Select Protocol [UDP, TCP](TCP)
>> Set interval in minutes: [0, 15, 30, 45, 60](15)
>> Enable TLS(Only Anonymous authentication mode is supported)?
    [yes, no](yes) Yes

- [Info] Summary:
      Target server name or IP address:  Veritas
      Port:                             514
      Protocol:                         TCP
      Interval:                         15 minutes
      TLS:                              no

Do you want to continue? [yes, no] (yes) y
- [Info] Applying the changes...
- [Info] Logs are scheduled for forwarding every 15 minutes.
```


- [Info] Syslog forwarding is enabled.

Settings > LifeCycle

Settings > LifeCycle – Change the backup image life cycle parameter settings.

SYNOPSIS

LifeCycle Defaults

LifeCycle Show

LifeCycle Tune CLEANUP_SESSION_INTERVAL *Interval Unit*

LifeCycle Tune DUPLICATION_GROUP_CRITERIA *Criteria*

LifeCycle Tune IMAGE_EXTENDED_RETRY_PERIOD *Interval Unit*

LifeCycle Tune JOB_SUBMISSION_INTERVAL *Interval Unit*

LifeCycle Tune MAX_SIZE_PER_DUPLICATION_JOB *Size Unit*

LifeCycle Tune MAX_TIME_TIL_FORCE_SMALL_DUPLICATION_JOB *Time*

LifeCycle Tune MIN_SIZE_PER_DUPLICATION_JOB *Size Unit*

LifeCycle Tune REPLICA_METADATA_CLEANUP_TIMER *Time*

LifeCycle Tune TAPE_RESOURCE_MULTIPLIER *Value*

LifeCycle Tune VERSION_CLEANUP_DELAY *Time Unit*

DESCRIPTION

You can use the `LifeCycle` command with the `Default` and `Show` options to display the default values for each of the LifeCycle parameters and the current parameter values, respectively.

You can use the `LifeCycle Tune` command to adjust the following parameters:

- `CLEANUP_SESSION_INTERVAL` - To define how often the deleted life cycle policies should be cleaned up.
- `DUPLICATION_GROUP_CRITERIA` - To define how batches are created.
- `IMAGE_EXTENDED_RETRY_PERIOD` - To define how long NetBackup waits before an image copy is added to the next duplication job.
- `JOB_SUBMISSION_INTERVAL` - Set the frequency of job submission for all operations.
- `MAX_SIZE_PER_DUPLICATION_JOB` - To define how large the batch of images is allowed to grow.

- `MAX_TIME_TIL_FORCE_SMALL_DUPLICATION_JOB` - To define how old any image in the group can become before the batch is submitted as a duplication job.
- `MIN_SIZE_PER_DUPLICATION_JOB` - To define the size that the batch of images should reach before one duplication job is run for the entire batch.
- `REPLICA_METADATA_CLEANUP_TIMER` - To set the number of days after which the Import Manager stops trying to import the image.
- `TAPE_RESOURCE_MULTIPLIER` - To set the multiplier for the number of concurrently active duplication jobs that can access a single storage unit.
- `VERSION_CLEANUP_DELAY` - To define how much time must pass since an inactive version was the active version.

OPTIONS

`LifeCycle Defaults`

Show the default values of each of the parameters.

`LifeCycle Show`

Show the current values of each of the parameters.

`LifeCycle Tune CLEANUP_SESSION_INTERVAL Interval Unit`

How often the deleted life cycle policies should be cleaned up. The *Interval* variable denotes the time interval after which the policies are to be cleaned. The *Unit* variable is used to provide the unit for the time interval in Seconds, Minutes, Hours, Days, Weeks, Months, or Years. The default value is 24 hours. You must enter a value that is greater than 10 Seconds when the unit is set to Seconds.

`DUPLICATION_GROUP_CRITERIA Criteria`

Define how batches are created. Batches are created based on the life cycle policy name or the duplication job priority. You enter either `PolicyName` or `JobPriority`

`LifeCycle Tune IMAGE_EXTENDED_RETRY_PERIOD Interval Unit`

How long NetBackup waits before an image copy is added to the next duplication job. The *Unit* variable is used to provide the unit for the time interval in Seconds, Minutes, Hours, Days, Weeks, Months, or Years. The default value is 2 hours. You must enter a value that is greater than 10 Seconds when the unit is set to Seconds.

`LifeCycle Tune JOB_SUBMISSION_INTERVAL Interval Unit`

Use this command to set the frequency of job submission for all operations. The *Interval* variable is defined in minutes. The *Unit* variable is used to provide the unit for the time interval in Seconds, Minutes, Hours, Days, Weeks, Months,

or Years. The default value is 5 minutes. You must enter a value that is greater than 10 Seconds when the unit is set to Seconds. The maximum interval for this variable is not identified.

`LifeCycle Tune MAX_SIZE_PER_DUPLICATION_JOB Size Unit`

How large the batch of images is allowed to grow. The *Size* variable is the size of the duplication job. The *Unit* variable is used to provide the unit for the time interval in Bytes, KB, MB, GB, TB, or PB. If you select the unit as Bytes, you cannot enter a size that is less than 1024 Bytes. The maximum value is 2147483647. The default value is 100 GB.

`LifeCycle Tune MAX_TIME_TIL_FORCE_SMALL_DUPLICATION_JOB Time Unit`

How old any image in the group can become before the batch is submitted as a duplication job. The *Time* variable is the time of the image. The *Unit* variable is used to provide the unit for the time interval in Seconds, Minutes, Hours, Days, Weeks, Months, or Years. The default value is 30 minutes. You must enter a value that is greater than 10 Seconds when the unit is set to Seconds. The maximum seconds number is 2147483647.

The logical maximum number for the other unit options is as follows:

- Minutes: 35,791,394
- Hours: 396,523
- Days: 24,855
- Weeks: 3,550
- Months: 828
- Years: 68

If a user enters a higher number than the maximum, it automatically uses the allowed maximum number.

`LifeCycle Tune MIN_SIZE_PER_DUPLICATION_JOB Size Unit`

The size that the batch of images should reach before one duplication job is run for the entire batch. The *Size* variable denotes the size of the duplication job. The *Unit* variable denotes unit of size in Bytes, KB, MB, GB, TB, or PB. The default value is 8 GB. You must enter a value that is greater than 1024 Bytes.

`LifeCycle Tune REPLICATION_METADATA_CLEANUP_TIMER Time`

Set the number of days after which the Import Manager stops trying to import the image. The *Time* variable is defined in the number of days. You turn this parameter off if you enter a value of zero.

LifeCycle Tune TAPE_RESOURCE_MULTIPLIER *Value*

Set the multiplier for the number of concurrently active duplication jobs that can access a single storage unit. The *Value* variable contains the multiplier value that is between 1 to 2147483647. The default value is 2.

LifeCycle Tune VERSION_CLEANUP_DELAY *Time Unit*

How much time must pass since an inactive version was the active version. The *Time* variable denotes the time that must pass since an inactive version was the active version. The *Unit* variable is used to provide the unit for the time interval in Seconds, Minutes, Hours, Days, Weeks, Months, or Years. The default value is 14 hours. You must enter a value that is greater than 10 Seconds when the unit is set to Seconds.

EXAMPLES

The `Defaults` command shows the values of each of the LifeCycle parameters:

```
LifeCycle > Defaults
CLEANUP_SESSION_INTERVAL           : 24 hours
DUPLICATION_GROUP_CRITERIA        : 1
IMAGE_EXTENDED_RETRY_PERIOD       : 2 hours
JOB_SUBMISSION_INTERVAL           : 5 minutes
MAX_SIZE_PER_DUPLICATION_JOB      : 100 GB
MAX_TIME_TIL_FORCE_SMALL_DUPLICATION_JOB : 30 minutes
MIN_SIZE_PER_DUPLICATION_JOB      : 8 GB
REPLICA_METADATA_CLEANUP_TIMER     : 0 hours
TAPE_RESOURCE_MULTIPLIER           : 2
VERSION_CLEANUP_DELAY              : 14 days
```

Settings > NetBackup

Settings > NetBackup – Configure and adjust NetBackup settings.

SYNOPSIS

```
NetBackup AdditionalServers Add Servers
NetBackup AdditionalServers Delete Servers
NetBackup AdditionalServers Show
NetBackup AdditionalServers ShowAll
NetBackup CertificateUsage Disable Certificate
NetBackup CertificateUsage Enable Certificate
NetBackup DataBuffers Number Defaults
NetBackup DataBuffers Number Disk Count
NetBackup DataBuffers Number FT Count
NetBackup DataBuffers Number Restore Count
NetBackup DataBuffers Number Show
NetBackup DataBuffers Number Tape Count
NetBackup DataBuffers Size Defaults
NetBackup DataBuffers Size Disk Size
NetBackup DataBuffers Size FT Size
NetBackup DataBuffers Size Show
NetBackup DataBuffers Size Tape Size
NetBackup DataBuffers Size MULTICOPY Size
NetBackup DataBuffers Size NDMP Size
NetBackup Misc Defaults
NetBackup Misc Show
NetBackup Misc Tune DEFERRED_IMAGE_LIMIT Size
NetBackup Misc Tune DPS_PROXYDEFAULTRECVTMO Time
```

DESCRIPTION

You can use the `NetBackup` command to adjust various NetBackup settings. With this command, you can do the following:

- Add or delete additional servers to NetBackup on a master server appliance.
- Show the number of NetBackup data buffers. You can also display the default numbers of the NetBackup data buffers.
- Adjust the number of NetBackup data buffers for the following:
 - Disk
 - Fibre Transport
 - Tape
- Show the current values or the default values for the following:
 - Deferred image limit, `DEFERRED_IMAGE_LIMIT`. The default value is 64.
 - The Data Protection Server (DPS), proxy timeout, `DPS_PROXYDEFAULTRECVTMO`. The default value is 800.
- Change the number of images that you want to defer.
- Change the proxy default received timeout.

OPTIONS

`NetBackup AdditionalServers Add Servers`

Add servers to NetBackup additional servers list, where *Servers* is the list of server names or IP address.

Note: Only available on 52xx appliances in master server role.

`NetBackup AdditionalServers Delete Servers`

Delete servers from NetBackup additional servers list, where *Servers* is the list of server names or IP address.

Note: Only available on 52xx appliances in master server role.

`NetBackup AdditionalServers Show`

View the list of NetBackup additional servers excluding media servers.

Note: Only available on 52xx appliances in master server role.

NetBackup AdditionalServers ShowAll

View the list of all NetBackup additional servers. This list includes media servers.

Note: Only available on 52xx appliances in master server role.

NetBackup CertificateUsage Disable *Certificate*

Disable the Certificate Authority (CA) that is currently used on the appliance, where *Certificate* is either NBCA (NetBackup Certificate Authority) or ECA (External Certificate Authority).

NetBackup CertificateUsage Enable *Certificate*

Enable a Certificate Authority (CA) on the appliance, where *Certificate* is either NBCA (NetBackup Certificate Authority) or ECA (External Certificate Authority).

NetBackup DataBuffers Number Defaults

View the default numbers of NetBackup data buffers.

NetBackup DataBuffers Number Disk *Count*

Tune the number of NetBackup data buffers for a disk. The parameter name is `NUMBER_DATA_BUFFERS_DISK` and the default value is 30. The *Count* variable contains the number of data buffers.

NetBackup DataBuffers Number FT *Count*

Tune the number of NetBackup data buffers for Fibre Transport. The parameter name is `NUMBER_DATA_BUFFERS_FT` and the default value is 16. The *Count* variable contains the number of data buffers.

NetBackup DataBuffers Number Restore *Count*

Tune the number of NetBackup data buffers for restore. The *Count* variable contains the number of data buffers.

NetBackup DataBuffers Number Show

Show the number of data buffers.

NetBackup DataBuffers Number Tape *Count*

Tune the number of NetBackup data buffers for Tape. The parameter name is `NUMBER_DATA_BUFFERS` and the default value is 30. The *Count* variable contains the number of data buffers.

NetBackup DataBuffers Size Defaults

Set the NetBackup default data buffer size in Bytes.

NetBackup DataBuffers Size Disk *Size*

Set the NetBackup data buffer size for disk in Bytes. The *Size* variable contains the new size for data buffers.

`NetBackup DataBuffers Size FT Size`

Set the NetBackup data buffer size for tape in Bytes. The *Size* variable contains the new size for data buffers.

`NetBackup DataBuffers Size Show`

Show the NetBackup data buffer sizes for disk and tape in Bytes.

`NetBackup DataBuffers Size Tape Size`

Set the NetBackup data buffer size for tape in Bytes. The *Size* variable contains the number of data buffers.

`NetBackup DataBuffers Size MULTICOPY Size`

Set the NetBackup data buffer size in Bytes. The *Size* variable contains the number of data buffers.

`NetBackup DataBuffers Size NDMP Size`

Set the NetBackup data buffer size for NDMP (Network Data Management Protocol) in Bytes. The *Size* variable contains the number of data buffers.

`NetBackup Misc Defaults`

Show default value for miscellaneous NetBackup settings.

`NetBackup Misc Show`

Show all of the values for miscellaneous NetBackup settings.

`NetBackup Misc Tune DEFERRED_IMAGE_LIMIT Size`

Adjust the limit by which you want to defer an image. The default value is 64.

`NetBackup Misc Tune DPS_PROXYDEFAULTRECVTMO Time`

Adjust the timeout value for the DPS proxy default. The *Time* variable contains the timeout value. The default value is 800.

Settings > NetBackup DNAT

Settings > NetBackup DNAT – Enable/Disable Destination Network Address Translation (DNAT) on NetBackup appliance master and media servers

SYNOPSIS

Enable

Disable

DESCRIPTION

This command lets you enable or disable DNAT on NetBackup appliance master and media servers that communicate with (NAT)-enabled clients.

OPTIONS

NetBackup DNAT Enable

Enable DNAT on NetBackup appliance master or media servers that communicate with DNAT-enabled clients.

Note: Before enabling DNAT on a NetBackup appliance master or media server, check whether all clients in the NetBackup domain support Network Address Translation (NAT). If all clients do not support NAT, contact Veritas support to obtain an EEB to prevent memory leak issues.

NetBackup DNAT Disable

Disable DNAT on a NetBackup appliance master or media server.

EXAMPLES

The following is an example of information that is displayed when you run the Settings > NetBackup DNAT Enable command.

```
Settings> NetBackup DNAT Enable
>> If you have Network Address Translation (NAT) clients and
non-NAT clients, you must first contact Veritas Support
to obtain an EEB to prevent any possible memory leak issues.
If you have only NAT clients, you may continue with the configuration.
Do you want to continue? [yes, no] (yes)
>> Enabling DNAT requires restarting NetBackup services,
```

```
which may take several minutes.  
Do you want to continue? [yes, no] (yes)  
- [Info] DNAT has been enabled successfully.
```

The following is an example of information that is displayed when you run the `Settings > NetBackup DNAT Disable` command.

```
Settings> NetBackup DNAT Disable  
>> Disabling DNAT requires restarting NetBackup services, which may  
take several minutes. Do you want to continue? [yes, no] (yes)  
- [Info] DNAT has been disabled successfully.
```

To enable or disable DNAT on clients, you must update the `ACCEPT_REVERSE_CONNECTION` flag. Use the `/usr/opensv/netbackup/bin/admincmd/bpsetconfig` utility to enable or disable DNAT as follows.

- To enable DNAT on the client, use the following commands:

```
$ bpsetconfig  
bpsetconfig> ACCEPT_REVERSE_CONNECTION=True
```

- To disable DNAT on the client, use the following commands:

```
$ bpsetconfig  
bpsetconfig> ACCEPT_REVERSE_CONNECTION=False
```

After updating the `ACCEPT_REVERSE_CONNECTION` flag, make sure that you stop and restart NetBackup services by running the following commands:

- On UNIX clients:

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

- On Windows clients:

```
<install_path>\NetBackup\bin\bpdown  
<install_path>\NetBackup\bin\bpup
```

Settings > Password

Settings > Password – Change the local user password.

SYNOPSIS

Password *UserName*

DESCRIPTION

Use this command to change the password for a local user.

The following describes password requirements and restrictions:

- Minimum of eight characters.
- Minimum of one lower case character (a-z).
- Minimum of one number (0-9).
- Dictionary words are not allowed.
- The last seven passwords cannot be reused.
- The new password cannot be similar to the current or previous passwords.

OPTIONS

Password *UserName*

Change the password for a user on the appliance. *UserName* is the name of a local user.

Exit

Exit from the **Password** view without changing the password.

Note: This option is visible only to the **nbsecadmin** user.

Settings > Share

Settings > Share – Configure a media share.

SYNOPSIS

Share ClientInstall

DESCRIPTION

Use these commands to configure a media share for CIFS and NFS. You may open or close the client installation using these commands.

OPTIONS

Share ClientInstall Close

Close client installation media share for CIFS and NFS.

Share ClientInstall Open

Open client installation media share for CIFS and NFS.

Settings > SNMP polling

Settings > SNMP polling – Use SNMP tools to poll the appliance.

SYNOPSIS

SNMP polling

DESCRIPTION

Use these commands to enable or disable SNMP polling, or to obtain status about SNMP polling.

OPTIONS

SNMP polling enable

Enable SNMP polling.

SNMP polling disable

Disable SNMP polling.

SNMP polling status

Obtain status of SNMP polling.

Settings > Sysctl

Settings > Sysctl – Set, view, and list the sysctl parameter value.

SYNOPSIS

ApplianceDefault

List

Show

Tune

DESCRIPTION

This command lets you modify your sysctl parameter value. Sysctl is used to modify kernel parameters at runtime.

OPTIONS

ApplianceDefault *Parameter*

Set a parameter to the default value for the appliance installation. Here, *Parameter* is the name of the sysctl parameter.

List

List the sysctl parameters that can be modified.

Show *Parameter*

Display the sysctl parameter value. Here, *Parameter* is the name of the sysctl parameter.

Tune *Parameter Value*

Set a sysctl parameter value. Here, *Parameter* is the name of the sysctl parameter and *Value* is the parameter value.

EXAMPLES

The following is an example of information that is displayed when you run the Settings > Sysctl command.

```
abc123.Sysctl> List
net.ipv4.tcp_keepalive_time
vm.zone_reclaim_mode
vm.min_free_kbytes
```

Settings > SystemLocale

`Settings > SystemLocale`— Change the system locale of the appliance to correctly display, backup, and restore the files and the folders that are named with non-7-bit ASCII characters. For example, Chinese, Japanese, Korean, German Umlaut, or French accents.

SYNOPSIS

```
SystemLocale List
SystemLocale Set
SystemLocale Show
```

DESCRIPTION

Use these commands to view or change the system locale of your appliance for international support.

OPTIONS

The following options are available under the `SystemLocale` command:

```
SystemLocale List Language
```

List all available locales for a given language. Here, *Language* is the ISO 639-1 language code in 2 letters, for example, fr, ja, zh, fr, de, es, ru, and so on. This command displays all the system locales that are available and sorts them by the language code that you have specified.

```
SystemLocale Set Locale
```

Change the existing system locale of the appliance to another locale. Here, *Locale* is the value for a locale string.

If you want to back up a UNIX or a Linux system, you must set the appliance locale to the locale that your UNIX or Linux client is running on. For example, if your Solaris client is running on a French locale and it supports the Euro currency (fr_FR.ISO8859 -15), you must set *fr_FR@euro* as the system locale for your appliance.

Note: The locale names vary among various operating systems. The NetBackup appliance uses the locale naming convention same as Red Hat Linux.

If you want to back up a Windows system, you must set an appropriate UTF-8 locale because the NetBackup client sends the path information to the NetBackup database by converting it from the active code page to UTF-8. For example, you have installed a NetBackup client into a German Windows server and you want to back up a file named with a “ß” (Eszett) letter on it. In this case, you must set *de_DE.UTF-8* as the system locale for your appliance.

Note: Do not set the appliance system locale as per the locale that is used by the active code page on which your Windows client is running.

SystemLocale Show

View the current system locale on the appliance.

EXAMPLES

The following is an example of the information that is displayed when you run the Main > Setting > SystemLocale Show command.

```
abc123.Settings> SystemLocale Show
Current system locale is: en_US.UTF-8
```

The following is an example of the information that is displayed when you run the Main > Setting > SystemLocale List ja command. This command displays all Japanese locales that are currently available on the appliance.

```
abc123.Settings> SystemLocale List ja
ja_JP.UTF-8          ja_JP.eucJP          ja_JP.eucjp
ja_JP.shiftjisx0213  ja_JP.sjis           ja_JP.utf8
```

The following is an example of the information that is displayed when you run the Main > Setting > SystemLocale Set ja_JP.UTF-8 command.

```
abc123.Settings> SystemLocale Set ja_JP.UTF-8
Updating /etc/sysconfig/language ...      ok
Updating /etc/init.d/netbackup ...        ok
Updating /etc/init.d/nbappws ...          ok
The appliance system locale has been set to ja_JP.UTF-8.
>> Reboot the appliance for the changes to take effect? (yes/no)yes
- [Info] Rebooting appliance ...
```

Broadcast message from root (pts/0) (Mon Jan 28 00:16:26 2013):

The system is going down for reboot NOW!

Main > Settings > Alerts commands

This appendix includes the following topics:

- [Settings > Alerts > CallHome](#)
- [Settings > Alerts > Email](#)
- [Settings > Alerts > Hardware](#)
- [Settings > Alerts > SNMP](#)

Settings > Alerts > CallHome

Settings > Alerts > CallHome — Manage CallHome settings.

SYNOPSIS

```
CallHome Disable
CallHome Enable
CallHome NBInventory Disable
CallHome NBInventory Enable
CallHome Proxy Add name port [username] [passwd]
CallHome Proxy Disable
CallHome Proxy DisableTunnel
CallHome Proxy Enable
CallHome Proxy EnableTunnel
CallHome Proxy Test
CallHome Registration Show
CallHome Show
CallHome Test
```

DESCRIPTION

The `CallHome Registration Show` command displays your appliance registration information and your contact information. The [MyAppliance portal](#) is the unified address where you register the appliance and edit registration details.

You can use the `CallHome Enable` and `CallHome Disable` commands to instruct the appliance whether or not to send the appliance health status to Veritas Technical Support. Veritas uses the health status to automatically open Support cases to resolve problems faster. The functionality is enabled by default.

You can use the `CallHome NBInventory Enable` and `CallHome NBInventory Disable` commands to instruct the appliance whether or not to send installation deployment and product usage information to Veritas for use in the Product Improvement Program. The functionality is enabled by default.

In addition, you can use the `CallHome Proxy` command to specify proxy server information. If your appliance environment has a proxy server between the

environment and external Internet access, you must enable the proxy settings on the appliance. The proxy settings include both a proxy server and a port. The proxy server must accept https connections from the Veritas Call Home server. This feature is disabled by default. To use this feature, the proxy server on your site must be able to handle https requests.

OPTIONS

`CallHome Disable`

Disable the Call Home feature. Disabling Call Home also disables the Product Improvement Program.

`CallHome Enable`

Enable the Call Home feature. Enabling the feature lets you send the health status of the appliance to Veritas Technical Support. In case of any failure, Veritas Technical Support uses this information to resolve the issue.

`CallHome NBInventory Disable`

Disable the Product Improvement Program. Disabling the program prevents Veritas from capturing installation deployment and product usage information from your appliance.

`CallHome NBInventory Enable`

Enable the Product Improvement Program. Enabling the program allows Veritas to capture installation deployment and product usage information. The information that Veritas receives becomes part of a continuous quality improvement program that helps Veritas understand how customers configure, deploy, and use the product.

You cannot enable the Product Improvement Program if Call Home is disabled.

`CallHome Proxy Add name port [username] [passwd]`

Add a proxy server to the appliance. Here, *name* is the name of the proxy server that is either the TCP/IP address or the fully qualified name of the proxy server. *Port* is the proxy port number on the proxy server. The [username] is the name of the user for the proxy server authentication and [passwd] is the password for the proxy server authentication.

If you do not add "http(s):" at the start of the server name then by default http:// is added to it.

`CallHome Proxy Disable`

Disable the use of the proxy server settings.

`CallHome Proxy DisableTunnel`

Disable SSL tunneling for the proxy server.

CallHome Proxy Enable

Enable the use of the proxy server settings.

CallHome Proxy EnableTunnel

Enable SSL tunneling for the proxy server.

CallHome Proxy Test

In a high availability configuration, Call Home proxy settings on a node are synchronized automatically to the partner node. Log on to the partner node and run the command to verify that the synchronized settings work properly.

CallHome Registration Show

View registration details for the appliance and the link to the [MyAppliance portal](#) to register and edit contact information.

CallHome Show

View the Call Home and proxy settings that are currently configured for your appliance.

CallHome Test

Validate whether or not the appliance is able to send Call Home information to Veritas Technical Support.

EXAMPLES

The following example demonstrates how to add a proxy server to your appliance and the confirmation message that is returned.

```
Settings> Alerts> CallHome Proxy Add abc123.com 1234
```

Successfully set proxy server

The following example demonstrates how to disable the Call Home proxy server and the confirmation message that is returned.

```
Settings> Alerts> CallHome Proxy Disable
```

Successfully disabled proxy

The following example demonstrates how to disable SSL tunneling for the Call Home proxy server and the confirmation message that is returned.

```
Settings> Alerts> CallHome Proxy DisableTunnel
- [Info] Successfully added proxy tunnel flag
Successfully set proxy tunneling
```

The following example demonstrates how to add a proxy server to your appliance and the confirmation message that is returned.

```
Settings> Alerts> CallHome Proxy Enable
```

```
Proxy enabled successfully
```

The following example demonstrates how to enable SSL tunneling for the Call Home proxy server and the confirmation message that is returned.

```
Settings> Alerts> CallHome Proxy EnableTunnel
- [Info] Successfully added proxy tunnel flag
Successfully set proxy tunneling
```

The following is an example of the information that is displayed when you run the Settings > Alerts > CallHome Registration Show command.

```
Registration Information (Node: abc123.example.com)
```

Contact Name	John
Email ID	john@abc.com
Contact Number	121
Appliance Name	abc123
Company Name	VTAS
Street Name/Number	436376
City	Mounttain Vi
Zip/Pin	9999
State	CA
Country	USA

Note: Browse to the [MyAppliance portal](https://my.appliance.veritas.com) at <https://my.appliance.veritas.com> to register your appliance and your contact information.

The following is an example of information that is displayed when you run the Settings > Alerts > CallHome Show command.

```
abc123.Alerts> CallHome Show
CallHome and Proxy Settings
+-----+
| CallHome State |Disabled          |
+-----+-----+
|NBInventory State|Disabled          |
+-----+-----+
|   Proxy State   |Disabled          |
+-----+-----+
|   Tunnelling    |Enabled           |
+-----+-----+
| Proxy Server    |http://eng.veritas.com |
+-----+-----+
| Proxy Port      |443                |
+-----+-----+
| Proxy UserName  |admin              |
+-----+
```

Note: NBInventory refers to the NetBackup Product Improvement Program

Settings > Alerts > Email

Settings > Alerts > Email – Use to configure email support for the appliance.

SYNOPSIS

```
Email Hardware Add Addresses
Email Hardware Delete Addresses
Email NotificationInterval Time
Email SenderID Reset
Email SenderID Set Address
Email Show
Email Test
Email SMTP Add Server [Account] [Password]
Email SMTP Delete
Email Software Add Addresses
Email Software Delete Addresses
```

DESCRIPTION

Use this command to add, replace, or show the email address that the appliance uses. You can use this command to define one or more emails.

OPTIONS

```
Email Hardware Add Addresses
    Add or append a hardware administrator's email account for NetBackup to use.
    Where Addresses is the user's email address. To define multiple emails,
    separate them with a semi-colon.

Email Hardware Delete Addresses
    Delete a hardware administrator's email account for NetBackup to use.
    Where Addresses is the user's email address. To define multiple emails,
    separate them with a semi-colon.

Email NotificationInterval time
    Define the time span between the alert emails that are sent to the administrator.
```


Where *time* is the time between the alert emails that are sent to the administrator. This variable is defined in minutes.

Email SenderID Reset

Reset the current email ID to default email ID that is used for the emails that are received from the appliance.

Email SenderID Set Address

Set a sender email ID that is used for the emails that are received from appliance. Here, *Address* is the email address of the sender.

Email Show

View your email or SMTP settings

Email SMTP Add Server [Account] [Password]

Add an SMTP server that NetBackup can use.

The *Server* variable is the host name of the target SMTP server that is used to send emails. The *Account* option identifies the name of the account that was used or the authentication to the SMTP server. The *Password* option is the password for authentication to the SMTP server.

Email SMTP Delete

Delete the SMTP server that NetBackup uses.

Email SMTP Enable

Enable the SMTP server that NetBackup uses.

Email Software Add Addresses

Add or append a software administrator's email account for NetBackup to use.

Where *Addresses* is the user's email address. To define multiple emails, separate them with a semi-colon.

Email Software Delete Addresses

Delete a software administrator's email account for NetBackup to use.

Where *Addresses* is the user's email address. To define multiple emails, separate them with a semi-colon.

Email Test

A test email is sent to the email *Addresses* configured above. Check if a test email is received in your mail inbox. The email transmission is decided by the network connections, the SMTP settings and the email address settings of your appliance. Follow the prompted error messages to troubleshoot if the test email is not received.

Settings > Alerts > Hardware

Settings > Alerts > Hardware – Set or view a threshold value for the disk space of any partition.

SYNOPSIS

```
Hardware DiskspaceThreshold Set
```

```
Hardware DiskspaceThreshold Show
```

DESCRIPTION

You can set a threshold value for a disk space using this command and receive alerts when the disk space of any partition passes this threshold value.

OPTIONS

```
Hardware DiskspaceThreshold Set DiskThreshold
```

Set a threshold value for the disk space. The default value for disk space threshold is 80%. Here, the *DiskThreshold* variable defines a threshold value for the disk space in the range 1-99 in percent.

```
Hardware DiskspaceThreshold Show
```

View the threshold value that is set for your disk space.

Settings > Alerts > SNMP

Settings > Alerts > SNMP – Add SNMP information on your appliance that enables the host to send SNMP notifications for monitoring.

SYNOPSIS

SNMP Disable

SNMP Enable

SNMP Set *Server* [Community] [Port]

SNMP Show

SNMP ShowMIB

DESCRIPTION

The NetBackup appliance uses the SNMPv2-SMI application protocol to monitor the appliance. Use this command to add or change SNMP parameters on the server. You can use the following commands to display the current parameters and the changes that were made to the SNMP information. You can use this command to enable and disable SNMP notifications for appliance monitoring.

When you create and enable an SNMP community you enable appliance monitoring to occur on the appliance through the SNMP protocol. Notifications or traps are programmed to occur on the appliance. In addition, you can use this command to see the notification traps that have been configured for the appliance.

The following list is an example of the types of hardware notifications that are monitored through SNMP for the appliance:

- CPU
- Disk
- Fan
- Fibre Channel
- Power Supply
- RAID
- Temperature

OPTIONS

`SNMP Disable`

Disables the ability to send SNMP notifications (traps) for monitoring.

`SNMP Enable`

Enable the ability to send SNMP notifications (traps) for monitoring.

`SNMP Set Server [Community] [Port]`

Add information about SNMP. Here, *Server* is the name of the SNMP server, [Community] is the SNMP community, and [Port] is the SNMP port.

Note: The NetBackup appliance supports all the SNMP servers in the market. However, the ManageEngine™ SNMP server and the HP OpenView SNMP server are tested and certified for version 2.6 and later.

`SNMP Show`

Displays the parameters that are set after you have run an `SNMP Set Server` command. If you run this command before you have run a `SNMP Set Server` command, then default values for [Community] and [Port] are displayed and no value is displayed for *Server*.

`SNMP ShowMIB`

Display the contents of the Management Information Base (MIB) file. This file contains the notification traps that are configured to monitor the appliance.

EXAMPLES

You can use either of the following methods to configure a public SNMP community on port 8080. The example uses the [Community] and [Port] options.

```
abc123.Alerts> SNMP Set pqr222.xyz.com public 8080
Successfully set SNMP manager
```

When you run the `Settings> Alerts > SNMP ShowMIB` command, an output similar to the following is displayed.

```
VERITAS-APPLIANCE-MONITORING-MIB DEFINITIONS ::= BEGIN
```

```
IMPORTS
```

```
    DisplayString, mib-2 FROM RFC1213-MIB
```

```
    enterprises, OBJECT-TYPE, NOTIFICATION-TYPE, MODULE-IDENTITY FROM SNMPv2-SMI;
```

```
applianceMonitoringMib MODULE-IDENTITY
```

```
LAST-UPDATED "2016083000Z"  
ORGANIZATION "Veritas Technologies LLC"  
CONTACT-INFO "500 East Middlefield Road  
              Mountain View, CA 94043 US  
              Subject: appliance.mib"  
DESCRIPTION "The MIB module for Veritas Appliance Monitoring"
```

```
REVISION      "201609060000Z"  
DESCRIPTION   "Changed symc strings to vrts."
```

```
::= { products 9 }
```

```
veritassoftware      OBJECT IDENTIFIER ::= { enterprises 48328 }  
products             OBJECT IDENTIFIER ::= { veritassoftware 3 }  
  
systems              OBJECT IDENTIFIER ::= { applianceMonitoringMib 1 }  
software             OBJECT IDENTIFIER ::= { applianceMonitoringMib 2 }
```

```
-- system traps
```

```
vrtsystemName OBJECT-TYPE  
    SYNTAX DisplayString (SIZE(0..80))  
    MAX-ACCESS read-only  
    STATUS current  
    DESCRIPTION "System Name"  
    ::= { systems 1 }
```

```
vrtsfanTrap NOTIFICATION-TYPE  
    OBJECTS { vrtsystemName }  
    STATUS current  
    DESCRIPTION "Traps fan failures"  
    ::= { systems 3 }
```

```
vrtpowerTrap NOTIFICATION-TYPE  
    OBJECTS { vrtsystemName }  
    STATUS current  
    DESCRIPTION "Traps power failures"  
    ::= { systems 4 }
```

```
vrtsfibrechannelTrap NOTIFICATION-TYPE  
    OBJECTS { vrtsystemName }  
    STATUS current  
    DESCRIPTION "Traps FibreChannel failures"
```

```
::= { systems 5 }

vrtstemperatureTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Traps temperature failures"
::= { systems 6 }

vrtscpuTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Traps cpu failures"
::= { systems 7 }

vrtsdiskTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Traps disk failures"
::= { systems 8 }

vrt RAIDgroupTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Traps raid failures"
::= { systems 9 }

vrt enclosurefanTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Traps enclosure fan failures"
::= { systems 10 }

vrt enclosurepowerTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Traps enclosure power failures"
::= { systems 11 }

vrt enclosuretemperatureTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Traps enclosure temperature failures"
```

```
::= { systems 12 }

vrtsclosurediskTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Traps enclosure disk failures"
::= { systems 13 }

vrtsadapterTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Traps adapter failures"
::= { systems 14 }

vrtsfirmwareTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Traps firmware failures"
::= { systems 15 }

vrtspciTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Traps pci failures"
::= { systems 16 }

vrtsnetworkcardTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Traps network card failures"
::= { systems 17 }

vrtsvolumeTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Traps volume failures"
::= { systems 18 }

vrtsbbaTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Traps BBU failures"
::= { systems 19 }
```

```
vrtscconnectionTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Traps connection failures"
::= { systems 20 }

vrtspartitionTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Partition alert traps"
::= { systems 21 }

vrtssstoragestatusTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Traps StorageArray HealthStatus failures"
::= { systems 22 }

vrtsdimmTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Traps Dimm failures"
::= { systems 23 }

-- software traps

vrtsfailureJobsTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Job failures Trap"
::= { software 1 }

vrtsprocessTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Processes stopped traps"
::= { software 2 }

vrtsdiskSpaceTrap NOTIFICATION-TYPE
    OBJECTS { vrtssystemName }
    STATUS current
    DESCRIPTION "Low disk space traps"
```



```
::= { software 3 }
```

```
vrtssoftwareUpdateSuccessTrap NOTIFICATION-TYPE
```

```
    OBJECTS { vrtssystemName }
```

```
    STATUS current
```

```
    DESCRIPTION "Software update success trap"
```

```
::= { software 4 }
```

```
vrtssoftwareUpdateFailedRollbackSuccessTrap NOTIFICATION-TYPE
```

```
    OBJECTS { vrtssystemName }
```

```
    STATUS current
```

```
    DESCRIPTION "Software update failed but rollback was successful trap"
```

```
::= { software 5 }
```

```
vrtssoftwareUpdateFailedRollbackFailedTrap NOTIFICATION-TYPE
```

```
    OBJECTS { vrtssystemName }
```

```
    STATUS current
```

```
    DESCRIPTION "Software update and rollback failed trap"
```

```
::= { software 6 }
```

```
vrtsrollbackSuccessTrap NOTIFICATION-TYPE
```

```
    OBJECTS { vrtssystemName }
```

```
    STATUS current
```

```
    DESCRIPTION "Software rollback success trap"
```

```
::= { software 7 }
```

```
vrtsrollbackFailedTrap NOTIFICATION-TYPE
```

```
    OBJECTS { vrtssystemName }
```

```
    STATUS current
```

```
    DESCRIPTION "Software rollback failed trap"
```

```
::= { software 8 }
```

```
vrtscclusterStateTrap NOTIFICATION-TYPE
```

```
    OBJECTS { vrtssystemName }
```

```
    STATUS current
```

```
    DESCRIPTION "Cluster node failed trap"
```

```
::= { software 9 }
```

```
vrtsdiskPerfTrap NOTIFICATION-TYPE
```

```
    OBJECTS { vrtssystemName }
```

```
    STATUS current
```

```
    DESCRIPTION "Disk performance alert trap"
```

```
::= { software 10 }
```

```
vrtscollectorserviceTrap NOTIFICATION-TYPE
  OBJECTS { vrtssystemName }
  STATUS current
  DESCRIPTION "Collector plugin loading failed trap"
 ::= { software 11 }
```

```
vrtshaclusternametransmitTrap NOTIFICATION-TYPE
  OBJECTS { vrtssystemName }
  STATUS current
  DESCRIPTION "HA cluster name trap"
 ::= { software 12 }
```

END

Main > Settings > Notifications view commands

This appendix includes the following topics:

- [Settings > Notifications > LoginBanner](#)

Settings > Notifications > LoginBanner

Settings > Notifications > LoginBanner – Set and manage a text banner that appears before a user logs on to the appliance.

SYNOPSIS

Remove

Set

Show

SyncNetBackup

DESCRIPTION

The `LoginBanner` command lets you create a text banner message for your appliance that appears before a user logs on through one of the appliances.

When you set a login banner, it appears with the following appliance login methods:

- NetBackup Appliance Shell Menu
- IPMI console session
- NetBackup Appliance Web Console
- NetBackup Administration Console (optional)

OPTIONS

Remove

Remove the current login banner from the appliance. The option is also given to remove the login banner from the NetBackup Administration Console.

Set

Set a new appliance login banner. When you use this option, the appliance prompts you to enter a login banner heading and message to be displayed when a user tries to log on to the appliance.

The banner heading and banner message are both mandatory. Typing **return** for the heading text or the message text exits the banner configuration without saving any changes.

Login banner text parameters:

- Banner heading maximum characters: 250

- Banner message maximum characters: 29,000
- Standard English alphabet

Show

View the current login banner.

SyncNetBackup

Set the existing appliance login banner in the NetBackup Administration Console. This command overwrites the existing NetBackup login banner content with the appliance login banner content. If you run this command when there is no existing appliance login banner, the NetBackup login banner is removed.

EXAMPLES

Example 1 - set a new login banner for the appliance and NetBackup using the LoginBanner Set command:

```
appliance123.Notifications> LoginBanner Set
Enter a heading for the login banner (250 characters limit) or type
'return' to exit:
```

This is a test banner heading

```
Enter the message text for the login banner (type 'end' on a new
line to indicate the end of message text):
```

This is a test banner message.
end

Preview:

```
*****
This is a test banner heading
*****
```

This is a test banner message.

```
The existing banner will be overwritten and the SSH daemon
will be restarted. Do you want to proceed? [y,n]: (y) y
Setting the login banner... done
```

Do you want to use this banner for the NetBackup Administration Console as well? (Any existing NetBackup login banner will

```
be overwritten.) [y,n]: (y) y  
Setting the login banner in NetBackup... done
```

Once the login banner is set, it displays for any user that tries to access the appliance using SSH. See the following example:

Once the login banner is set, it displays for any user that tries to access the appliance using SSH and IPMI. See the following example:

```
ssh admin@appliance123.com  
*****  
This is a test banner heading  
*****
```

```
This is a test banner message.
```

```
Password:
```

Example 2 - remove the login banner from the appliance and NetBackup using the LoginBanner Remove command:

```
appliance123.Notifications> LoginBanner Remove  
The existing banner will be removed and the SSH daemon  
will be restarted. Do you want to proceed? [y,n]: (y) y  
Removing the login banner... done
```

```
Do you want to remove the banner from the NetBackup  
Administration Console as well? [y,n]: (y) y  
Removing the login banner from NetBackup... done
```

Example 3 - Set the current appliance login banner to the NetBackup Administration Console using the LoginBanner SyncNetBackup command:

```
appliance123.Notifications> LoginBanner SyncNetBackup  
Are you sure you want to use the current appliance login banner  
for the NetBackup Administration Console as well?  
(Any existing NetBackup login banner will be overwritten.) [y, n]: (y) y  
Setting the login banner in NetBackup... done
```

Main > Settings > Security commands

This appendix includes the following topics:

- [Settings > Security > Authorization](#)
- [Settings > Security > Authentication > ActiveDirectory](#)
- [Settings > Security > Authentication > Kerberos](#)
- [Settings > Security > Authentication > LDAP](#)
- [Settings > Security > Authentication > LocalUser](#)
- [Main > Settings > Security > Certificate](#)
- [Main > Settings > Security > FIPS](#)
- [Main > Settings > Security > Ports](#)
- [Main > Settings > Security > STIG](#)

Settings > Security > Authorization

Settings > Security > Authorization – authorize users to access the appliance by assigning them various roles (permissions).

SYNOPSIS

```
Grant  
List  
Revoke  
SyncGroupMembers
```

DESCRIPTION

The `Authorization` commands let you manage permissions for appliance users and user groups. The users include local users, LDAP users, Active Directory (AD) users, and NIS users. The user groups include LDAP user groups, AD user groups, and NIS user groups.

You can use the `Authorization` commands to do the following:

- Grant access privileges to the users and user groups that have been added to the appliance.
- List all of the users and user groups that have been added to the appliance, along with their designated permissions.
- Revoke access privileges from the users and user groups that have been added to the appliance.

OPTIONS

```
Grant Administrator Group groups
```

Grant the Administrator role to a user group. Here, *groups* is a comma-separated list of registered user groups that have been added to the appliance from a configured remote directory service (such as LDAP, AD, or NIS).

```
Grant Administrator Users users
```

Grant the Administrator role to a user. Here, *users* is a comma-separated list of local users, or registered users that have been added to the appliance from a configured remote directory service (such as LDAP, AD, or NIS).

Grant AMS Group *groups*

Grant the AMS role to a user group. Here, *groups* is a comma-separated list of registered user groups that have been added to the appliance from a configured remote directory service (such as LDAP, AD, or NIS).

Grant AMS Users *users*

Grant the AMS role to a user. Here, *users* is a comma-separated list of local users, or registered users that have been added to the appliance from a configured remote directory service (such as LDAP, AD, or NIS).

Grant NetBackupCLI Group *groups*

Grant the NetBackupCLI role to a user group. Here, *groups* is a comma-separated list of registered user groups that have been added to the appliance from a configured remote directory service (such as LDAP, AD, or NIS).

Grant NetBackupCLI Users *users*

Grant the NetBackupCLI role to a user. Here, *users* is a comma-separated list of registered users that have been added to the appliance from a configured remote directory service (such as LDAP, AD, or NIS).

Note: You cannot grant the NetBackupCLI role to an existing local user. However, you can create a local NetBackupCLI user by using the `Main_Menu > Manage > NetBackupCLI > Create` command from the NetBackup Appliance Shell Menu.

Note: NetBackupCLI users are solely restricted to run the NetBackup CLI and do not have access outside the scope of NetBackup software directories. Once these users log in, they are provided restricted access to the shell menu for managing NetBackup. These users do not have access to NetBackup Appliance Web Console or the other menus of the shell menu.

List

List all of the users and user groups that have been added to the appliance, along with their designated roles. The users include local users, or the registered users that have been added to the appliance from a configured remote directory service (such as LDAP, AD, or NIS). The user groups include those that have been added to the appliance from a configured remote directory service (such as LDAP, AD, or NIS).

Revoke Administrator Group *groups*

Revoke the Administrator role from a user group. Here, *groups* is a comma-separated list of registered user groups that have been added to the

appliance from a configured remote directory service (such as LDAP, AD, or NIS).

Revoke Administrator Users *users*

Revoke the Administrator role from a user. Here, *users* is a comma-separated list of local users, or registered users that have been added to the appliance from a configured remote directory service (such as LDAP, AD, or NIS).

Revoke AMS Group *groups*

Revoke the AMS role from a user group. Here, *groups* is a comma-separated list of registered user groups that have been added to the appliance from a configured remote directory service (such as LDAP, AD, or NIS).

Revoke AMS Users *users*

Revoke the AMS role from a user. Here, *users* is a comma-separated list of local users, or registered users that have been added to the appliance from a configured remote directory service (such as LDAP, AD, or NIS).

Revoke NetBackupCLI Group *groups*

Revoke the NetBackupCLI role from a user group. Here, *groups* is a comma-separated list of registered user groups that have been added to the appliance from a configured remote directory service (such as LDAP, AD, or NIS).

Revoke NetBackupCLI Users *users*

Revoke the NetBackupCLI role from a user. Here, *users* is a comma-separated list of local users, or registered users that have been added to the appliance from a configured remote directory service (such as LDAP, AD, or NIS).

SyncGroupMembers AddTask *HHMM*

Use this command to add a daily task that is synchronized for registered groups. Here, *HHMM* is the time of the day in hours and minutes.

SyncGroupMembers DeleteTask

Delete the daily tasks that are synchronized for registered groups.

SyncGroupMembers Now

Force synchronization for registered groups now.

SyncGroupMembers ShowTask

View the daily tasks that are synchronized for registered groups.

Settings > Security > Authentication > ActiveDirectory

Settings > Security > Authentication > ActiveDirectory – configure and manage Active Directory (AD) user registration and authentication on the appliance.

SYNOPSIS

```
Configure
Groups
List
Status
Unconfigure
Users
```

DESCRIPTION

You can use the `ActiveDirectory` command to perform the following tasks:

- Configure the appliance for AD user authentication.
- Add or remove one or more AD user groups.
- List all AD users and user groups.
- Add or remove one or more AD users.
- Unconfigure AD user authentication for the appliance.

OPTIONS

The following commands and options are available under `Authentication > ActiveDirectory`:

`Configure`

Configure the appliance for AD user authentication. When prompted for the **Domain** *<Hostname or IP address>*, enter either the fully qualified domain name (FQDN) or the IP address of the Active Directory server. When prompted for the **user**, enter the user name of the AD server Administrator. When prompted for a **Password**, enter a password for that user.

Note: At the `Domain <Hostname or IP address>` prompt, it is recommended that you use the FQDN.

If the appliance host name contains more than 15 characters, a message appears to inform you that the host name cannot be used as the NetBIOS name for Active Directory configuration. To complete the Active Directory configuration, you must specify a NetBIOS name for the appliance as follows:

- Maximum of 15 characters.
- The name cannot include any of the following special characters: \ * + = | ; ; " ? < > ,
- The name must be different than other names on the network.

Groups

Add or remove one or more AD user groups. Only the user groups that already exist on the AD server can be added to the appliance.

- Use the `Groups Add <groupname>` command to add a comma-separated list of AD user groups.
- Use the `Groups Remove <groupname>` command to delete a comma-separated list of AD user groups.

List

List all of the AD users and user groups that have been added to the appliance.

Status

View the status of AD authentication on the appliance.

Unconfigure

Unconfigure AD user authentication for the appliance.

Note: Before you unconfigure the AD server, you must revoke the roles from all of the AD users that have been added to the appliance. Otherwise the operation fails.

Warning: Unconfiguring AD user authentication disables and deletes the current AD configuration. The AD users are deleted from the appliance, but not from the AD server.

Users

Add or remove one or more AD users. Only the users that already exist on the AD server can be added to the appliance.

- Use the `Users Add <username>` command to add a comma-separated list of AD users.
- Use the `Users Remove <username>` command to delete a comma-separated list of AD users.

Note: As a matter of best practice, you should delete a registered user or user group from the appliance before deleting it from the LDAP server, AD server, or NIS server. If a user is removed from the remote directory service first (and not removed from the appliance), the user is listed as a registered user on the appliance but will not be able to log on.

Settings > Security > Authentication > Kerberos

Settings > Security > Authentication > Kerberos – configure and manage Network Information Service (NIS) user registration with Kerberos authentication on the appliance.

SYNOPSIS

Configure
Groups
List
Status
Unconfigure
Users

DESCRIPTION

You can use the `Kerberos` command to perform the following tasks:

- Configure the appliance for NIS-Kerberos user authentication.
- Add or remove one or more NIS user groups.
- List all NIS users and user groups.
- Add or remove one or more NIS users.
- Unconfigure NIS-Kerberos user authentication for the appliance.

OPTIONS

The following commands and options are available under `Authentication > Kerberos`:

Configure NIS `<NisServer> <NisDomain> <KdcServer> <Realm> [Domain]`

Configure the appliance for NIS-Kerberos user authentication.

Add and configure NIS-Kerberos user authentication with the following parameters.

- `NisSever` - NIS server FQDN or IP.
- `NisDomain` - NIS Domain.
- `KdcServer` - KDC server FQDN or IP.

- *Realm* - Kerberos default realm.
- *[Domain]* - KDC domain(optional). The default value is none.

Groups

Add or remove one or more NIS user groups. Only the user groups that already exist on the NIS server can be added to the appliance.

- Use the `Groups Add <groupname>` command to add a comma-separated list of NIS user groups.
- Use the `Groups Remove <groupname>` command to delete a comma-separated list of NIS user groups.

List

List all of the NIS users and user groups that have been added to the appliance.

Status

View the status of NIS-Kerberos authentication on the appliance.

Unconfigure

Unconfigure NIS-Kerberos user authentication for the appliance.

Note: Before you unconfigure the NIS-Kerberos server, you must revoke the roles from all of the NIS users that have been added to the appliance. Otherwise the operation fails.

Warning: Unconfiguring NIS-Kerberos user authentication disables and deletes the current NIS-Kerberos configuration. The NIS users are deleted from the appliance, but not from the NIS server.

Users

Add or remove one or more NIS users. Only the users that already exist on the NIS server can be added to the appliance.

- Use the `Users Add <username>` command to add a comma-separated list of NIS users.
- Use the `Users Remove <username>` command to delete a comma-separated list of NIS users.

Note: As a matter of best practice, you should delete a registered user or user group from the appliance before deleting it from the LDAP server, AD server, or NIS server. If a user is removed from the remote directory service first (and not removed from appliance), the user is listed as a registered user on the appliance but won't be able to log on.

Settings > Security > Authentication > LDAP

Settings > Security > Authentication > LDAP – configure and manage Lightweight Directory Access Protocol (LDAP) user registration and authentication on the appliance.

SYNOPSIS

Attribute
Certificate
ConfigParam
Configure
Disable
Enable
Export
Groups
Import
List
Map
Show
Status
Unconfigure
Users

DESCRIPTION

You can use the `LDAP` command to perform the following tasks:

- Add or delete LDAP configuration attributes.
- Set or show the trusted LDAP server certificate.
- Set, unset, or show the various LDAP configuration parameters.
- Configure the appliance for LDAP user authentication.
- Disable LDAP user authentication.
- Enable LDAP user authentication.

- Export LDAP configuration as an XML file.
- Add or remove one or more LDAP user groups.
- Import LDAP configuration from an XML file.
- List all LDAP users and user groups.
- Add, delete, or show NSS map attributes or object classes.
- Show the LDAP configuration.
- Show the status of LDAP authentication.
- Unconfigure LDAP user authentication for the appliance.
- Add or remove one or more LDAP users.

OPTIONS

The following commands and options are available under `Authentication > LDAP`:

Attribute

Add or delete LDAP configuration attributes.

- Use the `Attribute Add <parameter_name> <attribute>` command to add a new attribute.
- Use the `Attribute Delete <attribute_name>` command to delete an existing attribute.

Certificate

Set, view, or disable the SSL certificate.

- Use the `Certificate Set <filename>` command to enable and add the SSL certificate. The SSL certificate must be stored in the `/inst/patch/incoming` directory.

Note: When you use the `ssl=StartTLS` and `ssl=Yes` options during LDAP or AD configuration on the appliance, the initial setup is done over a non-SSL channel. After the LDAP connection and initial discover phase is over, the SSL channel is turned on. Even at this phase, establishing the SSL channel does not perform the server-side certificate validation. This validation starts after the server's root certificate is explicitly set using the **LDAP > Certificate Set <path>** option.

- Use the `Certificate Show` command to view the certificate applicable for the LDAP server.

- Use the `Certificate Unset` command to disable the SSL certificate.

ConfigParam

Set, view, and unset the LDAP configuration parameters.

Note: The `ConfigParam` command is only used to set the various LDAP configuration parameters. Once you set all of the necessary parameters, use the `Configure` command to enable the LDAP configuration and establish a connection with the LDAP server.

- Use the `ConfigParam Set` command to add or change the following LDAP configuration parameters:

* Required parameters

- `*ConfigParam Set base <base_DN>`

Enter the base directory name which is the top level of the LDAP directory tree.

- `ConfigParam Set binddn <bind_DN>`

Enter the bind directory name. The bind DN is used as an authentication to externally search the LDAP directory within the defined search base.

- `ConfigParam Set bindpw <password>`

Enter the password to access the LDAP server.

- `ConfigParam Set directoryType <directoryType>`

Enter the LDAP directory type. The available options are: OpenLDAP, ActiveDirectory, and Others.

Select **OpenLDAP** if you use a typical OpenLDAP directory service.

Select **ActiveDirectory** if you use AD as an LDAP directory service.

Select **Others** if you use a different type of LDAP directory service.

- `ConfigParam Set groupList <group_name(s)>`

Enter the name of an existing LDAP user group that resides on the LDAP server. To enter multiple groups, separate each group name with a comma (,).

The appliance does not handle ID mapping for LDAP configuration.

Veritas recommends that you reserve a group ID range of 1000 to 1999 for appliance users only.

Note: As a best practice, do not enter group names that are already used for appliance local users or NetBackupCLI users.

- `*ConfigParam Set host <server_name or IP>`

Enter the FQDN or IP address of the LDAP server.

Note: The specified LDAP server should comply with RFC 2307bis. The RFC2307bis specifies that hosts with IPv6 addresses must be written in their preferred form, such that all components of the address are indicated and leading zeros are omitted.

- `*ConfigParam Set ssl <No|Yes|StartTLS>`

Enable SSL certificate for the LDAP server.

Note: When you use the `StartTLS` and `Yes` options during LDAP configuration, the initial setup is done over a non-SSL channel. After the LDAP connection and initial discover phase is over, the SSL channel is turned on. Even at this phase, the established SSL channel doesn't do the server-side certificate validation. This validation starts after the server's root certificate is explicitly set using the `LDAP > Certificate Set` command.

- `ConfigParam Set userList <user_name(s)>`

Enter the name of an existing LDAP user that resides on the LDAP server. To enter multiple users, separate each user name with a comma (,).

The appliance does not handle ID mapping for LDAP configuration. Veritas recommends that you reserve a user ID range of 1000 to 1999 for appliance users only.

Note: As a best practice, do not enter user names that are already used for appliance local users or NetBackupCLI users. Additionally, do not use the appliance default names **admin** or **maintenance** for LDAP users.

- Use the `ConfigParam Show` command to view the existing LDAP configuration parameters.
- Use the `ConfigParam Unset <parameters>` command to unset the LDAP configuration parameters.

Configure

After setting the LDAP parameters using the `ConfigParam` command, run the `Configure` command to complete the configuration and enable LDAP authentication on the appliance.

The `ValidateIDs` option determines whether the appliance checks the LDAP server and the local server for conflicts when creating LDAP user IDs, group IDs, user names, or group names. By default, the appliance is set to validate IDs by checking for conflicts. Any conflict is reported immediately and stops LDAP configuration.

- Use the `Configure Yes` command to enable `ValidateIDs`.
- Use the `Configure No` command to disable `ValidateIDs`.

Disable

Disable LDAP user authentication on the appliance. This command does not remove the configuration and you can reenable it using the `Enable` command.

Enable

Enable a disabled LDAP configuration on the appliance.

Export <file_name>

Export the existing LDAP configuration as an XML file. The file is saved at `/inst/patch/incoming/<file_name>`. This file can be imported to configure LDAP on other appliances.

Groups

Add or remove one or more LDAP user groups. Only the user groups that already exist on the LDAP server can be added to the appliance.

- Use the `Groups Add <groupname>` command to add a comma-separated list of LDAP user groups.
- Use the `Groups Remove <groupname>` command to delete a comma-separated list of LDAP user groups.

Import <path>

Import the LDAP configuration from an XML file. The XML file must reside at `/inst/patch/incoming/<file_name>`.

List

List all of the LDAP users and user groups that have been added to the appliance.

Map

Add, delete, or show NSS map attributes.

- Use the `Map Add Attribute <attribute type> <attribute value>` command to set an NSS map attribute.
- Use the `Map Delete Attribute <attribute type>` command to delete an NSS map attribute.
- Use the `Map Show` command to view the NSS map attributes.

Show

View the LDAP configuration details.

Status

View the status of LDAP authentication on the appliance.

Unconfigure

Unconfigure LDAP user authentication for the appliance.

Note: Before you unconfigure the LDAP server, you must revoke the roles from all of the LDAP users that have been added to the appliance. Otherwise the operation fails.

Warning: Unconfiguring LDAP user authentication disables and deletes the current LDAP configuration. The LDAP users are deleted from the appliance, but not from the LDAP server.

Users

Add or remove one or more LDAP users. Only the users that already exist on the LDAP server can be added to the appliance.

- Use the `Users Add <username>` command to add a comma-separated list of LDAP users.
- Use the `Users Remove <username>` command to delete a comma-separated list of LDAP users.

Note: As a matter of best practice, you should delete a registered user or user group from the appliance before deleting it from the LDAP server, AD server, or NIS server. If a user is removed from the remote directory service first (and not removed from appliance), the user is listed as a registered user on the appliance but won't be able to log on.

EXAMPLES

Example 1 - Configure an association between the appliance and an LDAP directory server to enable the appliance to import users and user groups.

```
appliance123.LDAP > ConfigParam Set host ldap.example.com
appliance123.LDAP > ConfigParam Set base dc=sample,dc=com
appliance123.LDAP > ConfigParam Set ssl no
appliance123.LDAP > Configure
- [Info] Configure Successful. Continuing with Post-Configure Processing!
Configure Successful. Continuing with Post-Configure Processing!
```

Command was successful!

Example 2 - Register a user or user group from the LDAP directory server so that those users can be authorized and authenticated on the appliance.

```
appliance123.LDAP> Users Add ldapuser1,ldapuser2
Command was successful!
appliance123.LDAP> Groups Add ldapgroup01
Command was successful!
appliance123.Authorization> List
```

```
+-----+
|Principal Type|Name/login |Access | Role |Principal Source|
|-----+-----+-----+-----+-----+
|User          |ldapuser1  |Allowed|NoRole|Ldap             |
|-----+-----+-----+-----+-----+
|User          |ldapuser2  |Allowed|NoRole|Ldap             |
|-----+-----+-----+-----+-----+
|Group         |ldapgroup01|Allowed|NoRole|Ldap             |
|-----+-----+-----+-----+-----+
| -Member      |ldapuser3  |Allowed|      |                  |
+-----+-----+-----+-----+-----+
```

Command was successful!

Example 3 - Export the current LDAP configuration into an XML file that can be imported on other appliances.

```
appliance123.LDAP> Export ldapconfig1
- [Info] Exporting LDAP configuration
Exporting LDAP configuration
```

Command was successful!

Example 4 - Import an LDAP configuration from an XML file.

```
appliance123.LDAP> Export ldapconfig1  
- [Info] Exporting LDAP configuration  
Exporting LDAP configuration
```

Command was successful!

Settings > Security > Authentication > LocalUser

Settings > Security > Authentication > LocalUser – create and manage local users on the appliance.

SYNOPSIS

Clean

List

Password *UserName*

Users

DESCRIPTION

You can use the `LocalUser` command to perform the following tasks:

- Delete all local users.
- List all local users.
- Change local user password.
- Add or remove one or more local users.

OPTIONS

The following commands and options are available under `Authentication > LocalUser`:

Clean

Delete all of the local users.

List

List all of the local users that have been added to the appliance.

Password *UserName*

Change the password of a local user.

Note: Only the system Admin user can change other users' passwords.

Users

Add or remove one or more local users.

- Use the `Users Add <users>` command to add one local user or a comma-separated list of local users.
- Use the `Users Remove <users>` command to delete one local user or a comma-separated list of local users..

Note: Only the system Admin user can add and delete other users.

Main > Settings > Security > Certificate

Main > Settings > Security > Certificate – Import an external certificate or show current certificate details.

DESCRIPTION

The `Certificate` command allows you to import an external certificate or show the details of the certificate that is currently in use.

OPTIONS

Import

Import an external certificate to the appliance.

Show

Shows the details of the certificate that is currently in use on the appliance.

Main > Settings > Security > FIPS

Main > Settings > Security > FIPS – Enable the FIPS 140-2 standard for NetBackup MSDP.

DESCRIPTION

The `FIPS` command allows you to increase security on the appliance by enforcing the FIPS 140-2 standard for NetBackup MSDP. For more information about FIPS 140-2, see the *NetBackup Appliance Security Guide*.

Note: In a NetBackup Appliance high availability (HA) setup, you must configure the FIPS options on both nodes and the configurations must match.

OPTIONS

Enable MSDP

Enforces the FIPS 140-2 standard for NetBackup MSDP. This command prompts you to enter the maintenance password to enable the feature.

Enabling with the `MSDP` option terminates all jobs that are currently in progress and restarts the NetBackup services. As a best practice, it is recommended that you first stop all jobs manually before you enable this feature.

Enable VxOS

Enforces the FIPS 140-2 standard for VxOS (Veritas Operating System). This command prompts you to enter the maintenance password to enable the feature.

Enabling with the `VxOS` option reboots the appliance and disconnects all logged in users from their sessions. As a best practice, it is recommended that you provide advanced notice to all users before you enable this feature.

Enable All

Enforces the FIPS 140-2 standard for NetBackup MSDP and for VxOS. This command prompts you to enter the maintenance password to enable the feature.

Enabling with the `All` option reboots the appliance and disconnects all logged in users from their sessions. As a best practice, it is recommended that you provide advanced notice to all users before you enable this feature.

Disable MSDP

Disables enforcement of the FIPS 140-2 standard for NetBackup MSDP. This command prompts you to enter the maintenance password to disable the feature.

Disabling with the `MSDP` option terminates all jobs that are currently in progress and restarts the NetBackup services. As a best practice, it is recommended that you first stop all jobs manually before you disable this feature.

Disable VxOS

Disables enforcement of the FIPS 140-2 standard for VxOS. This command prompts you to enter the maintenance password to disable the feature.

Disabling with the `VxOS` option reboots the appliance and disconnects all logged in users from their sessions. As a best practice, it is recommended that you provide advanced notice to all users before you disable this feature.

Disable All

Disables enforcement of the FIPS 140-2 standard for MSDP and for VxOS. This command prompts you to enter the maintenance password to disable the feature.

Disabling with the `All` option reboots the appliance and disconnects all logged in users from their sessions. As a best practice, it is recommended that you provide advanced notice to all users before you disable this feature.

Status

Shows the current status of the feature.

Main > Settings > Security > Ports

Main > Settings > Security > Ports – Synchronize appliance ports with the open NetBackup ports or view the currently open NetBackup ports on the appliance.

DESCRIPTION

The `Ports` view allows you to synchronize or view the currently open NetBackup ports in the firewall rules on the appliance.

`ModifyNBUPortRange`

Synchronizes the appliance ports with the open NetBackup ports.

Before you run this command, you must first modify the open NetBackup ports using the `SERVER_PORT_WINDOW` option in the NetBackup Java console. Then, run this command to synchronize the appliance ports with the open NetBackup ports.

`Show`

Shows the NetBackup ports that are currently open on the appliance.

Main > Settings > Security > STIG

Main > Settings > Security > STIG – Enable OS STIG hardening rules.

DESCRIPTION

The `STIG` command lets you increase security on the appliance by enforcing OS STIG hardening rules. This command enables a specific set of STIG rules and does not allow individual rule control. When the feature is enabled, a list of the enforced rules appears. The command output may also show exceptions for any specific rules that cannot be enforced. For more information about STIG, see the *NetBackup Appliance Security Guide*.

For appliances (nodes) in a high availability (HA) setup, this feature must be enabled manually on each node to ensure correct operation in switchover or failover scenarios.

Note: Once the feature is enabled, a factory reset is required to disable it.

OPTIONS

Enable

Enforce OS STIG hardening rules. This command prompts you to enter the maintenance password to enable the option.

Show

See the current status of the option.

Main > Support commands

This appendix includes the following topics:

- [Support > Checkpoint](#)
- [Support > Cleanup > RemoveShelfEntries](#)
- [Support > Cleanup > ResetDIMMErrors](#)
- [Support > Collect](#)
- [Support > DataCollect](#)
- [Support > Disk](#)
- [Support > Errors](#)
- [Support > FactoryReset](#)
- [Support > FibreTransport](#)
- [Support > InfraServices](#)
- [Support > iostat](#)
- [Support > IPMI](#)
- [Support > KillRemoteCall](#)
- [Support > Logs](#)
- [Support > Maintenance](#)
- [Support > Messages](#)

- Support > NBDNA
- Support > nbperfchk
- Support > NBSU
- Support > Processes
- Support > RAID
- Support > Reboot
- Support > RecoverStorage
- Support > Service
- Support > ServiceAllowed
- Support > Show
- Support > Shutdown
- Support > Storage ClearReservations
- Support > Storage Reset
- Support > Storage SanityCheck
- Support > Test

Support > Checkpoint

Support > Checkpoint – Used to manage system checkpoints

SYNOPSIS

Checkpoint Create

Checkpoint Rollback

DESCRIPTION

This command exists under the `Main_Menu > Support` view. Use this command to create a new checkpoint or roll back the host to an existing appliance checkpoint.

OPTIONS

Checkpoint Create

Use this command to create a user-defined checkpoint.

Checkpoint Rollback

Use this command to rollback an appliance to a specific checkpoint that you select.

You can chose from the following checkpoints:

- Pre-upgrade checkpoint
A checkpoint that is created before you perform a software upgrade.
- Post-upgrade checkpoint
A checkpoint that is created after you have upgraded your appliance to a newer version.
- User-directed checkpoint
A checkpoint that you created.

EXAMPLES

The following examples demonstrate how to create a new user-defined checkpoint and roll back to a specified checkpoint.

To create a new checkpoint from the NetBackup Appliance Shell Menu:

- 1 Log on to the appliance as an administrator and open the NetBackup Appliance Shell Menu.

- 2 Enter the following command to create a user-directed checkpoint:

```
Main_Menu > Support > Checkpoint Create
```

The following interactive process begins. The NetBackup Appliance Shell Menu informs you of any existing checkpoints before you can create a new checkpoint.

- 3 Enter **Yes** to proceed with the creation of the new checkpoint.
- 4 Enter a description for your checkpoint. That is an optional field.
- 5 Enter **Yes** to begin the Create checkpoint process.

To roll back to an existing checkpoint from the NetBackup Appliance Shell Menu

- 1 Log on to the appliance as an administrator and open the NetBackup Appliance Shell Menu.
- 2 Enter the following command to roll back to a checkpoint:

```
Main_Menu > Support > Checkpoint Rollback
```

The following interactive process begins. The NetBackup Appliance Shell Menu informs you of the components that are reverted during this process. It also lists all of the existing checkpoints.

Rolling back to an Appliance Checkpoint will restore the system back to the checkpoint's point-in-time. This can help undo any misconfiguration or system failures that might have occurred.

Rolling back to an Appliance Checkpoint will revert the following components:

- 1) Appliance Operating System
- 2) Appliance Software
- 3) NetBackup Software
- 4) Clustering Software
- 5) Networking Configuration
- 6) Any previously applied patches
- 7) Backup data is not reverted

The existing Appliance Checkpoints in the system are:

```
-----  
(1) Checkpoint Name: User directed checkpoint  
Date Created: Fri Oct 5 09:27:32 2012  
Description: User checkpoint after configuring network  
-----
```

Please enter the checkpoint to rollback to (Available options: 1 only):

- 3 Enter the number of the checkpoint that you want to use for the Rollback operation.
- 4 Enter **Yes**, if you want to automatically restart all appliances after the rollback completes.
- 5 Enter **Yes** a second time to confirm that you want to restart appliances automatically after the rollback operation completes.
- 6 Enter **Yes** to begin the rollback to a checkpoint operation.

Support > Cleanup > RemoveShelfEntries

`Support > Cleanup > RemoveShelfEntries` – Remove hardware monitoring data that is associated with the decommissioned storage shelves on 52xx platforms (Must be under the guidance of Technical Support).

SYNOPSIS

`RemoveShelfEntries`

DESCRIPTION

This command applies to 52xx platforms (5230 and later).

This command exists under the `Main_Menu > Support > Cleanup` view. After the storage shelves have been decommissioned, this command must be run to clear the hardware monitoring data that is associated with the storage shelves. This command removes the storage shelf entries from the database.

Note: This command must be run under the guidance of Technical Support.

OPTIONS

`RemoveShelfEntries`

After the storage shelves have been decommissioned, this command must be run to clear the hardware monitoring data that is associated with the storage shelves. This command removes the storage shelf entries from the database.

EXAMPLES

The following example demonstrates how to run the `Support > Cleanup > RemoveShelfEntries` command:

```
abcxxx.Cleanup> RemoveShelfEntries
>> Do you want to remove hardware monitoring data for
    the decommissioned storage shelves?[yes, no](no): yes
    12 records deleted
    Successfully deleted storage shelf entries.
```

Support > Cleanup > ResetDIMMErrors

Support > Cleanup > ResetDIMMErrors – Resets the uncorrectable error count of specific failed DIMMs (dual in-line memory modules) to zero.

SYNOPSIS

```
ResetDIMMErrors
```

DESCRIPTION

This command exists under the `Main_Menu > Support > Cleanup` view. You may need to run this command after a failed DIMM has been replaced. After you replace some DIMMs, the uncorrectable error count may not be reset (to zero) automatically. In this scenario, you need to run the `ResetDIMMErrors` command.

After replacing a DIMM, you can verify the uncorrectable error count by running the `Monitor > Hardware ShowHealth Appliance DIMM` command.

Note: This command must be run under the guidance of Technical Support.

OPTIONS

```
ResetDIMMErrors
```

After the failed DIMMs have been replaced, this command may be needed to reset the uncorrectable error count of the specific DIMMs.

By default, the command resets the uncorrectable error count of all the failed DIMMs that are shown in the output. You can specify specific IDs to reset the uncorrectable error count for specific failed DIMMs.

Once the uncorrectable error count is reset, you will receive one or more alerts indicating that the DIMM error is resolved (if alerts are configured).

EXAMPLES

The following example demonstrates how to run the `Support > Cleanup > ResetDIMMErrors` command:

```
appliance.Cleanup> ResetDIMMErrors
```

Showing the DIMMs (dual in-line memory modules) with a failed state:

ID	Name	Status	Manufacturer	Part	Serial	Type	Size	Speed	Uncorrectable	Status
----	------	--------	--------------	------	--------	------	------	-------	---------------	--------

				Number	Number				Error Count	
1	ChannelA	Uncorrectable	Samsung	M393A1G4	313C62CB	DDR4	8192	2133	2	Failed
	Slot1	Error		0DB0-CPB			MB	MHz		
11	ChannelB	Uncorrectable	Samsung	M393A1G4	313C53CA	DDR4	8192	2133	2	Failed
	Slot2	Error		0DB0-CPB			MB	MHz		

To reset the uncorrectable error count of specific DIMMs from the table, enter the IDs separated by commas. To reset the uncorrectable error count for all the DIMMs shown in the table, type all(default): 1,11

Are you sure you want to reset the uncorrectable error count for 1 and 11?[yes, no](no): yes
The reset has been initiated. It may take some time to complete.
If alerts are configured, you will receive one or more alerts indicating that the DIMM error is resolved.

Support > Collect

Support > Collect – Collect appliance details and transmit to Veritas.

SYNOPSIS

Collect

DESCRIPTION

Use this command to collect detailed information of your appliance manually and transmit to Veritas.

OPTIONS

Collect Inventory

Use this command to collect all component-specific metadata including model information, serial number, etc. and transmit to Veritas.

EXAMPLES

The following procedure is executed after you run the `Collect Inventory` command.

```
abc123.Support> Collect inventory
```

Collecting inventory data. The data collecting process may take several minutes.

Inventory collection completed. It may take 10 to 30 seconds to transmit the data to Veritas.

Support > DataCollect

Support > DataCollect – Gather device logs.

SYNOPSIS

DataCollect

DESCRIPTION

Use this command to gather appliance device logs.

OPTIONS

DataCollect

Use to gather appliance device logs.

EXAMPLES

The following procedure is executed after you run the `DataCollect` command.

The log files collected from the appliance are sent to AutoSupport servers. The data transmission completes in several minutes or longer due to file size, network status, appliance performance and other reasons.

```
abc123.Support> DataCollect
Gathering release information
Gathering disk performance logs
Gathering command output logs
Gathering dmidecode logs
Gathering ipmitool sel list logs
Gathering ipmitool sel writeraw logs
Gathering fwtermlog logs
Gathering AdpEventLog logs
Gathering smartctl logs
Gathering ipmiutil command output
Gathering iSCSI logs
Gathering cpu information
Gathering memory information
Gathering os logs
Gathering dfinfo logs
Gathering vxprint logs
Gathering patch logs
```

```
Gathering autosupport logs
Gathering sysinfo logs
Gathering sdr logs
Gathering adpallinfo logs
Gathering encinfo logs
Gathering cfgdsply logs
Gathering ldpdinfo logs
Gathering pdlist logs
Gathering fru logs
Gathering adpbucmd logs
Gathering adpalilog logs
Gathering Test Hardware logs
```

```
All logs have been collected in /tmp/DataCollect.zip
Log file can be collected from the appliance shared folder - \\abc123.example.com\logs\APPLIANCE
Share can be opened using Main->Support->Logs->Share Open
The Log files DataCollect-SYMXXXXXX-XXXXXXXXXX.tar.gz collected from the appliance are sent to A
The data transmission may complete in several minutes or longer due to file size, network status
```

```
=====End of DataCollect=====
All logs have been collected in /tmp/DataCollect.zip
```

Support > Disk

Support > Disk – Gather disk information

SYNOPSIS

Disk info

DESCRIPTION

Use this command to gather and display information about the local disk layout and usage.

OPTIONS

Disk info

Use to gather disk information and display the disk layout and usage information.

Support > Errors

`Support > Errors` – Display NetBackup error logs.

SYNOPSIS

`Errors HoursAgo`

DESCRIPTION

The `Errors` command displays all the recorded problem entries in the NetBackup logs for the previous day. You can designate the number of hours that you want to go back and display.

OPTIONS

`Errors`

Displays the NetBackup error logs of the previous day. Here, *HoursAgo* specifies the number of hours in the past from the current time. *HoursAgo* is an integer. The default is 24 hours before the current time.

Support > FactoryReset

Support > FactoryReset – Reset the appliance to factory default settings.

SYNOPSIS

```
FactoryReset
```

```
FactoryReset ResetAll
```

DESCRIPTION

Use this command to reset the appliance to the factory default settings. If you changed the default factory-set password, this command resets it back to the default value.

For appliance nodes in a high availability (HA) setup, you must first remove the node from the HA setup and disconnect its Ethernet and Fibre Channel (FC) cables before a factory reset.

Note: If you attempt to run a factory reset or initiate a rollback to a non-HA checkpoint on a node in an HA setup, the HA setup can malfunction.

Before a factory reset on any HA node, perform the following tasks in the order as they appear:

- On the node that you do not want to remove, run the following command to remove the other node from the HA setup:

```
Manage > High Availability > Remove Node HostName
```


Where *HostName* is the host name of the node you want to remove.
- Disconnect the Ethernet cables and the FC cables from the removed node.
- After completing the previous tasks, you can run the `FactoryReset` command.

Note: If you do not remove the node from the HA setup and disconnect the Ethernet and FC cables before a factory reset, the command fails. An error message appears to remind you to perform the previous tasks and then try the factory reset again.

OPTIONS

`FactoryReset`

Use this command to reset the appliance to the factory default settings.

`FactoryReset ResetAll`

Use this command to reset the appliance factory installed image in non-interactive mode.

EXAMPLES

To begin a factory reset from the appliance shell menu

- 1 Open an SSH session and log on to the appliance as an administrator.

- 2** Enter `Main_Menu > Support > FactoryReset`. This command shows the following messages and requires you to answer the questions that follow, before the factory reset begins:

[Info] Disable interrupt (CTRL-C), quit, and suspend signals.

[Info] The IPMI sysadmin user and its associated password, status, and permissions have been reset to the default values.

Appliance factory reset will reset the entire system to the factory installed image. The appliance will have the following components reset to the factory restored settings/image:

- 1) Appliance Operating System
- 2) Appliance Software
- 3) NetBackup Software
- 4) Tape media configuration on the master server
- 5) Networking configuration (optionally retain)
- 6) Storage configuration and backup data (optionally retain)

- [Info] Running factory reset validation...please wait (approx 2 mins)
- [Info] Factory reset validation successful.

RESET NETWORK CONFIGURATION [Optional]

- Resets the IP and routing configuration.
- Resets the DNS configuration.

>> Do you want to reset the network configuration? [yes/no] (yes) no

RESET STORAGE CONFIGURATION and BACKUP DATA [Optional]

- Removes all the images on the AdvancedDisk and MSDP storage pools.
- Resets the storage partitions.
- Resets storage expansion units, if any.

>> Do you want to delete images and reset backup data? [yes/no] (yes)

>> Resetting the storage configuration will remove all backup data on the storage partitions and any connected expansion units. This is not reversible. Are you sure you want to reset storage configuration? [yes/no] (yes)

>> A reboot of the appliance is required to complete the factory reset. Reboot automatically after reset? [yes/no] (no) yes

>> Automatically rebooting after the reset will not provide you with an opportunity to review the progress/final status of the reset. Are you sure you would like to automatically reboot? [yes/no] (no) yes

3 After you respond to these questions, the following summary information is shown:

```
FACTORY RESET SUMMARY
-----
Reset Appliance OS, software configuration      : [YES]
Reset Appliance network configuration          : [NO]
Reset Appliance storage configuration (REMOVE DATA) : [YES]
Auto reboot after reset?                       : [YES]

Appliance will make the following version changes:

+-----+
| Appliance | Current Version | Reverted Version |
+-----+-----+-----+
|v49        |NetBackup 7.6.0.1 Appliance |NetBackup 7.6.0.1 Appliance |
|           |2.6.0.1          |2.6.0.1          |
+-----+-----+-----+
```

- 4 The following warning appears. If you want to begin the factory reset operation, enter **Yes**.

The following summary messages appear as the factory reset continues:

```
- [Info] PERFORMING APPLIANCE RESET TO FACTORY STATE ON : abc123.example.com
- [Info] Delete checkpoints (type: NON_FACT) succeeded
- [Info] Reset of the appliance to FACTORY STATE successful.
- [Info] Stopping NetBackup processes... (6 mins approx)
- [Info] Moving NetBackup Appliance Directory to ce-win21-urmil...
- [Info] Acquired lock on the storage.
- [Info] Resetting the storage configuration...
- [Info] Checking whether the 'MSDP' storage partition exists...
- [Info] Initiating deletion of 'MSDP' storage partition...
- [Info] Unmounting the 'MSDP' partition '0'...
- [Info] Deleting the 'MSDP' partition '0'...
- [Info] Checking whether the 'Catalog' storage partition exists...
- [Info] Initiating deletion of 'Catalog' storage partition...
- [Info] Unmounting the 'Catalog' partition '0'...
- [Info] Deleting the 'Catalog' partition '0'...
- [Info] Checking whether the 'Configuration' storage partition exists...
- [Info] Initiating deletion of 'Configuration' storage partition...
- [Info] Unmounting the 'Configuration' partition '0'...
- [Info] Deleting the 'Configuration' partition '0'...
- [Info] Checking whether the 'AdvancedDisk' storage partition exists...
- [Info] Initiating deletion of 'AdvancedDisk' storage partition...
- [Info] Unmounting the 'AdvancedDisk' partition '0'...
- [Info] Deleting the 'AdvancedDisk' partition '0'...
- [Info] Removing the storage configuration...
- [Warning] Failed to query SCSI device '/dev/system/root'.

- [Warning] Failed to query SCSI device '/dev/system/root'.
>> A reboot of the appliance is required to complete the factory reset.
    Reboot now?[yes/no] (no)yes
Rebooting the appliance now...
- [Info] Rebooting abc123.example.com...
```

Broadcast message from root (Mon Nov 25 11:56:39 2013):

The system is going down for reboot NOW!

```
- [Info] Rebooting appliance to complete the reset.
```

Please reconnect to the Appliance shell menu to continue using this appliance

Support > FibreTransport

Support > FibreTransport – Use to manage the Fibre Transport (FT) advanced settings.

SYNOPSIS

```
FibreTransport ChunkSize Show
```

```
FibreTransport ChunkSize Set ChunkSize
```

DESCRIPTION

You can use the `FibreTransport` command to do the following:

- Show the chunk size for optimized duplication and replication to other NetBackup appliances over FT.
- Set the chunk size for optimized duplication and replication other NetBackup appliances over FT

OPTIONS

```
FibreTransport ChunkSize Show
```

Use this command to show the current chunk size for optimized duplication and replication to other NetBackup appliances over FT.

```
FibreTransport ChunkSize Set ChunkSize
```

Use this command to set the chunk size in KB.

The default value for chunk size is "0", which means the chunk size is not specified, and not used. If you set the chunk size to a value equal or greater than "1", you specify the size of each data chunk that is sent to the FC network. The available chunk size value is 1-2048 in KB. The recommended values are 128 KB, 256 KB, 512 KB, 1024 KB, and 2048 KB. You may also need to set other values.

Note: The chunk size setting is not required for optimized duplication and replication over FT. It is highly dependent on user deployment and network status. If you find it necessary to use the chunk size, you can adjust the chunk size as needed to determine a proper value for your environment and the current network status.

For more information about how to use the FT chunk size, see the *NetBackup Appliance Fibre Channel Guide*.

EXAMPLES

The following is an example of information when you run the `FibreTransport ChunkSize Show` command.

```
appliance.support> FibreTransport ChunkSize Set 2  
[Info] Current deduplication chunk size is 0 KB.
```

The following is an example of information when you run the `FibreTransport ChunkSize Set Value` command.

```
appliance.support> FibreTransport ChunkSize Set 2  
[Info] New deduplication chunk size is 2 KB.
```

Support > InfraServices

Support > InfraServices – Display and control the infrastructure services.

SYNOPSIS

```
Show All
Start All
Stop All
Show Database
Start Database
Stop Database
Show MessageQueue
Start MessageQueue
Stop MessageQueue
Show Webserver
Start Webserver
Stop Webserver
```

DESCRIPTION

These commands exist under the `Main > Support > InfraServices` view. You can use these commands to monitor, start, and stop the infrastructure services.

Note: The infrastructure service commands are mainly used for troubleshooting and support. These should be used under the guidance of Technical Support. Stopping the infrastructure services may lead to failure of running operations.

OPTIONS

```
Show All
```

Show the status of all the infrastructure services. The infrastructure services include the database, message queue, and the web server service.

Start All

Start all the infrastructure services. The infrastructure services include the database, message queue, and the web server service.

Stop All

Stop all the infrastructure services. The infrastructure services include the database, message queue, and the web server service.

Show Database

Show the status of the database.

Start Database

Start the database.

Stop Database

Stop the database.

Show MessageQueue

Show the status of the message queue service.

Start MessageQueue

Start the message queue service.

Stop MessageQueue

Stop the message queue service.

Show Webserver

Show the status of the web server and the web console.

Start Webserver

Start the web server and the web console.

Stop Webserver

Stop the web server and the web console.

Support > iostat

Support > iostat – Monitor system input and output device loading

SYNOPSIS

```
iostat help
```

```
iostat run
```

```
iostat [options] [interval] [count]
```

DESCRIPTION

The `iostat` command is a Linux command that you can use to monitor system input and output devices. The command enables you to observe the time that the devices are active in relation to their average transfer rates. This command generates reports that you can use to change the system configuration to better balance the input and the output load between physical disks. The `iostat` command generates reports continuously.

Note: You must run the `iostat run` command before you can use the available options that are supported for the `iostat` command.

OPTIONS

```
iostat help
```

View the help information of the command.

```
iostat run
```

Prompts you to enter the available options that are supported.

```
[options]
```

The following list describes the available options that are supported:

- `-c`
Display the CPU utilization report.
- `-d`
Display the device utilization report.
- `-N`
Display the registered device mapper names for any device mapper devices.
- `-n`

Display the network file system (NFS) report. This option works only with kernel 2.6.17 and later.

- `-h`
Make the NFS report that is displayed by option `-n` easier to read.
- `-k`
Display statistics in kilobytes per second instead of blocks per second.
- `-m`
Display statistics in megabytes per second instead of blocks or kilobytes per second.
- `-t`
Print the time for each report displayed.
- `-V`
Print the version number then exit.
- `-x`
Display the extended statistics.
- `-p [{ device [,...] | ALL }]`
The `-p` option displays the statistics for block devices and all their partitions that the system uses. If a device name is entered on the command line, then the statistics for it and all of its partitions are displayed. The `ALL` keyword indicates that statistics have to be displayed for all the block devices and partitions defined by the system. That includes those that have never been used.
- `[device [,...] | ALL]`
If a device name is entered on the command line, then the statistics for it and all of its partitions are displayed. The `ALL` keyword indicates that statistics have to be displayed for all the block devices and partitions defined by the system. That includes those that have never been used.

[interval]

- The *interval* parameter specifies the amount of time in seconds between each report.
- The first report contains statistics for the time since system startup. Each subsequent report contains statistics that are collected during the interval since the previous report.

[count]

- The *count* parameter can be specified with the *interval* parameter.

- If the *count* parameter is specified, the value of *count* determines the number of reports that are generated at *interval* seconds apart.

EXAMPLES

The following example shows how to use the `iostat` command:

```
abc123.Support> iostat run
Please enter options:
iostat -c
```

The following example shows how to use the `interval` parameter:

```
abc123.Support> iostat run
Please enter options:
iostat -c 1
```

Support > IPMI

Support > IPMI – Use these commands to manage the IPMI configuration.

SYNOPSIS

```
IPMI Network Configure<IPAddress> <Netmask> <GatewayIPAddress>
```

```
IPMI Network Show
```

```
IPMI Reset
```

```
IPMI User Add <User_name>
```

```
IPMI User Delete <User_name>
```

```
IPMI User List
```

DESCRIPTION

The IPMI commands let you configure the IPMI network and manage users accessing the appliance using the IPMI connection. Use the IPMI commands to:

- Configure IPMI sub-system
- View the current IPMI settings
- Reset the IPMI
- Add users
- Delete users
- List users

OPTIONS

IPMI Network Configure

This command is used to configure the IPMI sub-system using the IPMI port.

IPMI Network Show

This command is used to view the current IPMI port information.

IPMI Reset

This command is used to reset the IPMI. You must reset IPMI only if the IPMI interface stops responding or hangs.

IPMI User Add

This command is used to add new users to access the IPMI sub-system.

IPMI User Delete

This command is used to delete existing users that can access the IPMI sub-system.

IPMI User List

This command is used to view the list of users who can access the IPMI sub-system.

The following procedure is executed after you run the `IPMI Network Configure` command.

```
Support> IPMI Network Configure 10.182.8.70 255.255.240.0 10.182.1.1
Network is configured successfully.
```

The following information is displayed when you run the `IPMI Network Show` command.

```
Support> IPMI Network Show
IP Address Source      : STATIC
IP Address              : 10.182.8.70
Subnet Mask             : 255.255.240.0
Gateway IP Address     : 10.182.1.1
```

The following information is displayed when you run the `IPMI Reset` command.

```
Resetting the IPMI disconnects all current IPMI users.
Are you sure you want to reset the IPMI? [yes, no]: yes
```

In case other users are not affected, type **yes** and press **Enter** to continue. The following message is displayed:

```
-[Info] The IPMI is being reset...
-[Info] Wait for two minutes before attempting to reconnect to the
IPMI console. If you cannot access the IPMI console, the appliance
must be shut down and then restarted. First schedule a convenient time
for the shutdown, alert all users and shut down the appliance.
Then disconnect all appliance power cables for 15 seconds, reconnect
them and turn on power to the appliance.
```

Type **no** in case other users are affected. Alert all users and schedule a convenient time for reset. Run the `IPMI Reset` command again at the scheduled time.

The following procedure is executed after you run the `IPMI User Add <User_name>` command.

```
Support> IPMI User Add abc
New password:
```

Confirm password:
Operation successful

The following procedure is executed after you run the IPMI User Delete
<User_name> command.

```
Support> IPMI User Delete abc
User abc has been deleted successfully.
```

The following information is displayed after you run the IPMI User List command.

```
Support > IPMI User List

User name      : Anonymous User
User privilege : ADMIN

User name      : sysadmin
User privilege : ADMIN

User name      : root
User privilege : ADMIN
```

Support > KillRemoteCall

Support > KillRemoteCall – Use to terminate remote calls on peer appliances.

SYNOPSIS

KillRemoteCall

DESCRIPTION

You can use this command to terminate remote calls on peer appliances. The remote calls that are terminated can be in a running or hung state.

OPTIONS

KillRemoteCall

Use this command to terminate remote calls on peer appliances.

Support > Logs

Support > Logs – Manage logging setting, view and share logs files.

SYNOPSIS

```
Browse  
Delete Date LogType  
GetLevel  
SetLevel Option Level  
Share  
VxLogView JobID job_id  
VxLogView Minutes minutes_ago  
VxLogView Module module_name  
Upload JobID jobid case_num  
Upload Time start end case_num
```

DESCRIPTION

Use this command to do the following functions:

- Browse the appliance log directories and files.
You can use the `Browse` command to view the log directories and log files that are configured in your appliance. When you run the `Browse` command the command prompt changes to `LOGROOT/>`. From the `LOGROOT/` command prompt you can run the following commands to list, view, and change directories:
 - `ls` - List the directories and files
 - `tree` - Provides a tree-view of the directories and files.
 - `cd DIR` - Use to change the directory, where *DIR* is the directory name. For example, you can use `cd .`, `cd ..`, and `cd -`.
 - `less FILE` - Provides a read-only view of a file. You must enter the letter `q` or `quit` to exit this view.
 - `exit|quit` - Enables you to exit the log shell.
 - `help|?` - Use either of these two commands to display help.

From the `LOGROOT/>` command prompt, you can use the `ls` command to see the following log directories on the host:

- `APPLIANCE`
- `NBU`
- `OS`
- `PD`
- `WEBGUI`

To see the log files from within a log directory, you must change directories to the log directory that contains the log files that you want to view. After you change directories, the same commands that were available under the `LOGROOT/` view are available for each of the log directories.

For example, to see the operating system (OS) log files, you must first enter `cd OS` at the `LOGROOT/>` command prompt. The command prompt changes to `LOGROOT/OS>/. Then you can enter ls to see the file names. Finally, you can use the less filename command to view a read-only version of the log file.`

- **Set the level of debug logs**

Use the `SetLevel` command to set the NetBackup log level for an appliance component that you choose. The range begins with zero and can differ for each component. A value of zero means that logging is at its lowest level. In addition, you can use the `GetLevel` command to get the NetBackup log level.
- **Export or remove CIFS and NFS shares for the logs.**

Use the `Share Open` command to export the CIFS and the NFS shares for the logs. The `Share Close` command removes the CIFS and the NFS shares for the logs.
- **Display debug information from the VxLog files.**

Use the `VxLogView` command to display log files for specific job or by a set duration of time.
- **Upload the NetBackup log files for your appliance to Support.** The files that you send can be based on the job ID, the time that the log files were taken, or the default-based duration.

If an issue occurs and you decide you need additional support, you should call Veritas Technical Support and open a customer case. The customer support contact assigns a unique customer case number that identifies you, your company information, and your issue. To further help you diagnose the issue, the customer support contact needs to obtain a copy of your appliance log files. You can use the `Upload` command to send all of the log files that are associated with your appliance to Support.

The following procedure describes the process that you use to send the log files from your appliance to Technical Support.

To configure your appliance to upload log files using the Logs Upload command

- 1 Make sure that you have a customer case number assigned to your issue. If you do not have a case number, contact Technical Support and have a customer case opened and a unique customer case number assigned to your issue. The customer case number is used to create the name of the file that you send to Support. That helps the technical support contact identify the file that you sent.
- 2 Log on to your appliance as the administrator.
- 3 Enter the **Main > Support** view.
- 4 Type one of the following commands to create a log set for technical support. Depending on the nature of your issue, technical support may ask you to use one of the following commands to create the log set. Each of these commands creates a `.tar` file that is based on the job ID, a specific start and end time, or a default duration of four hours.
 - **Type** `Logs Upload Jobid jobid case_num`.
This command creates a `.tar` file that contains log files that are based on the job ID.
 - **Type** `Logs Upload Time start End case_num`.
This command creates a `.tar` file that contains log files that are based on the default duration of four hours
Where *case_num* is the customer case number that was issued to you by your NetBackup Support contact. This number becomes a part of the `.tar` file name so your Technical Support contact can identify the files that came from your appliance.
Where *jobid* is the job ID number that is used to collect the logs.
Where *start* and *End* are the start date and the end date of the logs to collect.

OPTIONS

Browse

Use the show the appliance logs.

Delete *Date LogType*

Use this command to delete archived log files. Here, *Date* defines the date until which you want to delete archived log files. *LogType* is the product name for which you want to delete the archived log files.

The available *LogType* options are the following:

CoreDump/NetBackup/Puredisk/WEBGUI/ALL

GetLevel

Use to view the NetBackup log levels

SetLevel *Option Level*

Use to set the NetBackup log levels. Where *Option* is the appliance component. For example, an appliance component can be NetBackup or PureDisk. In addition, *Level* is the appliance logging level. For NetBackup, you can select a level from 0 to 5 and for PureDisk, you can select a level from 0 to 10. Zero provides the lowest level of logging that is available.

Share

Use to extract the CIFS and the NFS shares for the logs.

For CIFS, you must map the share using the appliance "admin" user's credentials.

VxLogView JobID *job_id*

Display debug information from the log files by designating a specific job ID as the criteria by which the information is parsed.

Where *job_id* is the NetBackup job that you determine you want to view from the debug information.

VxLogView Minutes *minutes_ago*

Display debug information from the log files using time (in minutes) as the criteria by which the information is parsed.

Where *minutes_ago* is the amount of time, in minutes, used to determine how much of the past debug information to display.

VxLogView Module *module_name*

Display debug information from the log files by designating a specific logging module as the criteria by which the information is parsed.

Where *module_name* is the module from which you want to view log files. You can select from the following modules:

All/CallHome/Checkpoint/Common/Config/Database/Hardware/HWMonitor
/Network/RAID/Seeding/SelfTest/Storage/SWUpdate/Commands/CrossHost
/Trace/FTMS/FTDedupTarget/AuthService/TaskService

Upload JobID *jobid case_num*

Upload log files for the appliance to Support. This command creates a .tar file of the logs using the job ID. Use FTP to upload the file to Support.

Where *jobid* contains the job ID number that is used to collect the logs. The *case_num* variable is a unique number filed with Support that identifies the customer and their corresponding log files. The format of this number is ###-###-###

Upload Time *start end case_num*

Upload the logs based on the default duration. The default duration is four hours. This command creates a .tar file of the logs using the time. Use FTP to upload the file to Support.

Where *start* is the start date of the log files to send to Support. *end* is the end date of the log files to send to Support. And *case_num* is a unique number filed with Support that identifies the customer and their corresponding log files. The format of this number is ###-###-###

Support > Maintenance

Support > Maintenance – Enables the user to open an interactive shell menu.

SYNOPSIS

Maintenance

DESCRIPTION

Your appliance is pre-configured with a **Maintenance** user account. When you log into this account, you open an interactive shell menu that you can use to troubleshoot or manage underlying operating system tasks.

The default password is, P@ssw0rd. Veritas recommends that you change this password at your earliest convenience. Use the following command to reset the password.

```
Main > Settings > Password UserName
```

In this case, the user name is `maintenance`.

If you require customer support to resolve an issue, you may be required to provide this password to your support representative. In addition, if you change this password and then run the `FactoryReset` command, this password is reset to the initial default value.

OPTIONS

Maintenance

Used to enter an interactive shell menu that you can use to troubleshoot or manage underlying operating system tasks.

EXAMPLES

To enter your Maintenance account, run the following command, and provide the password when you receive a prompt.

```
NBAppl.Support> Maintenance
<!--Maintenance Mode--!>
maintenance's password:
```

Support > Messages

Support > Messages – Display the message file.

SYNOPSIS

Messages *lines*

DESCRIPTION

Use this command to display the messages file. With this command, you can designate the number of lines that you want to display from that file. If you do not define the number of lines the entire messages file is displayed.

OPTIONS

Messages *lines*

Display the message file. Here, *lines* is the number of lines that are to be displayed in the message. You can enter a value between zero and 99999.

Support > NBDNA

Support > NBDNA – Create and remove network traces with the NBDNA utility.

SYNOPSIS

NBDNA Create *phase*

NBDNA Remove

DESCRIPTION

Use this command in conjunction with the NetBackup Domain Network Analyzer(NBDNA) utility on an appliance. The NBDNA utility analyzes the following information:

- The NetBackup domain and its configuration for network issues
- NetBackup performance
- Behavior with regard to hostname lookup and connectivity between NetBackup hosts and their role within the NetBackup domain

OPTIONS

NBDNA Create *phase*

Used to create and remove network traces with the NBDNA utility.

Where *phase* is used to specify which test phase to run, phase 0, phase 1, or phase 2.

Phase 0: Default mode. Name lookup test and socket connection test.

Phase 1: Includes Phase 0. Add basic NetBackup service test for the SERVER list.

Phase 2: Includes Phase 0. Add basic NetBackup service test for SERVER and CLIENT list.

NBDNA Remove

Used to remove all existing trace files that the NBDNA utility generates.

Support > nbperfchk

Support > nbperfchk – Measures a disk array's read and write speeds.

SYNOPSIS

```
nbperfchk -i inputpath -o outputpath [-s filesize] [-syncend] [-bs buffersize]
```

DESCRIPTION

The `nbperfchk` command measures the read speed and write speed of a disk array. You can use this command to test the read speed and the write speed of the disks that host deduplicated data. For example, you can measure the speeds of the disks that host deduplicated data as follows:

- In a PureDisk storage pool, use this command to measure the speed of disks attached to the content router.
- In a NetBackup media server deduplication pool (MSDP), use this command to measure the speed of the disks attached to the media server. The media server can be running any operating system that Veritas supports for media servers and MSDPs.

Note: Veritas recommends that you work with a Veritas Technical Support staff member when you run this command and interpret its results. Veritas recommends a minimum disk performance level of 130 MB/sec for deduplicated read and write operations.

The `nbperfchk` command is functionally equivalent to the obsolete `camel` command that was available from Veritas as a downloadable program but was not associated with any specific product release. The `camel` command is available internally from the Veritas Technical Support website as HOWTO47457.

The `nbperfchk` utility enables you to write a test file to a disk, read back that test file, and observe the read speeds attained during the read operation. You can use the results from `nbperfchk` to make sure that the `ReadBufferSize` parameter is set appropriately in your backup environment. The `ReadBufferSize` parameter resides in the `[CRDataStore]` section of the `contentrouter.cfg` file. You can use this command as follows:

- Use the following command to write data to the disks:

```
nbperfchk -i inputpath -o outputpath -s filesize -syncend
```

- Use the following command to read data from the disks:

```
nbperfchk -i inputpath -o outputpath -bs buffersize
```

OPTIONS

-i *inputpath*

For *inputpath*, specify the full path to an input file. The `nbperfchk` command reads this file and generates information about the read speed when this file is read to disk.

For example, you can specify the following to read in a file that contains all zero characters (0x00) from the `/dev/zero`:

-o *outputpath*

For *outputpath*, specify the full path to an output file. The `nbperfchk` command creates this file.

For example, on writes, specify the path to the output file that you want to create. On reads, specify `-o NUL` to discard all the output as it is generated.

-s *filesize*

For *filesize*, specify a file size that is equal to or larger than than combined memory size of your computer plus the amount in the disk array. A file of this size ensures that the data is written to disk and not to a buffer.

-syncend

The `syncend` parameter flushes the buffer and writes all data to disk.

-bs *buffersize*

For *buffersize*, specify the read buffer size to use when `nbperfchk` runs. For example, 64k or 128k.

PROCEDURES

To analyze nbperfchk results and adjust the ReadBufferSize parameter setting

- 1 Log in as the root user (UNIX) or the administrator (Windows) on the computer that hosts the content router.

In PureDisk environments, log into the storage pool authority node or storage pool authority appliance.

In NetBackup environments, log into the media server.

- 2 Change to a test directory.

- 3 Type the `nbperfchk` command in the following format to write a large test file to the content router:

```
nbperfchk -i inputpath -o outputpath -s filesize -syncend
```

For example, the following command writes a 64 GB data file that contains all zeros to the `e` drive:

```
nbperfchk -i zero: -o e:\datal -s 64g -syncend
```

- 4 Type the `nbperfchk` command in the following format to read the test file and observe the read speeds in the `nbperfchk` output:

```
nbperfchk -i inputpath -o NUL -bs buffersize
```

Example 1. To observe several read speeds with several buffer sizes, type the following series of commands:

```
nbperfchk -i e:\datal -bs 64k -o NUL
nbperfchk -i e:\datal -bs 128k -o NUL
nbperfchk -i e:\datal -bs 256k -o NUL
```

Example 2. The following `nbperfchk` command reads back the data in file `datal` and uses a buffer size of 1024 K:

```
C:\Users\administrator.mymediaserver\Desktop>nbperfchk -i e:\datal -bs 1024k -o NUL
195 MB @ 65.3 MB/sec, 194 MB @ 64.9 MB/sec
295 MB @ 49.4 MB/sec, 100 MB @ 33.5 MB/sec
403 MB @ 44.8 MB/sec, 108 MB @ 35.8 MB/sec
505 MB @ 42.1 MB/sec, 102 MB @ 34.1 MB/sec
599 MB @ 40.0 MB/sec, 94 MB @ 31.3 MB/sec
705 MB @ 39.2 MB/sec, 106 MB @ 35.5 MB/sec
821 MB @ 39.2 MB/sec, 116 MB @ 38.8 MB/sec
943 MB @ 39.4 MB/sec, 122 MB @ 40.8 MB/sec
1024 MB @ 40.1 MB/sec
```

Observe the following when you analyze the data:

- The left two columns show the amount of data read and the average read speed.
- The final line shows the overall read speed. This is the most important line in this output because it shows you how fast the total read occurred with the buffer size you specified.

- The right two columns show the average read speed in the last 3 seconds of each read. Unless these numbers vary drastically from read to read, you can disregard the right two columns.
- 5 Analyze your read speeds and adjust the `ReadBufferSize` parameter if necessary.

Your operating system, your disk speeds, and the `ReadBufferSize` parameter setting all affect restore and rehydration performance.

Veritas recommends that you type several `nbperfchk` commands and increase the size of the argument to the `-bs` parameter each time. Example 1 in step 4 shows this method. If you can enter ever-increasing arguments to the `-bs` parameter, you can probably increase the size of the `ReadBufferSize` parameter in the `[CRDataStore]` section of the `contentrouter.cfg` file.

By default, `ReadBufferSize=65536`, which is 64K. Veritas testing shows that `ReadBufferSize=1048576`, which is 1024 X 1024, or 1M, offers good performance on most Windows systems. On most UNIX systems, Veritas testing shows that `ReadBufferSize=65536` (the default) offers good performance.

For information about how to edit NetBackup configuration files, see your NetBackup documentation.

For information about how to edit PureDisk configuration files, see the *PureDisk Administrator's Guide*.

Support > NBSU

Support > NBSU – Manage NetBackup support data files

SYNOPSIS

NBSU Create

NBSU Remove

DESCRIPTION

The NetBackup Support Utility (NBSU) is a Veritas utility used to gather diagnostic information about the system on which the utility is run. By default, NBSU gathers appropriate diagnostic information based on the operating system and NetBackup environment.

You can use this command to create or remove the NetBackup configuration support files that the NBSU utility uses.

OPTIONS

NBSU Create

Use to create NetBackup configuration support files.

NBSU Remove

Use to remove any NetBackup configuration support files.

Support > Processes

`Support > Processes` – Display and control the NetBackup processes.

SYNOPSIS

```
Processes NetBackup Show
Processes NetBackup Start
Processes NetBackup Stop
```

DESCRIPTION

You can use this command to monitor, start, and stop the NetBackup processes.

OPTIONS

```
Processes NetBackup Show
    Shows the NetBackup processes that are currently active.

Processes NetBackup Start
    Used to start the NetBackup processes.

Processes NetBackup Stop
    Used to stop the NetBackup processes.
```

Support > RAID

`Support > RAID` – Used to clear data on the storage disks and to reset the disk RAID configuration.

SYNOPSIS

`RAID Clear`

`RAID ClearReservations`

DESCRIPTION

The RAID commands are available only on a 53xx appliance and only when it is newly out-of-box or has been re-imaged or factory reset.

Use the `RAID Clear` command to remove external RAID storage that includes only the LUNs and volume groups.

Use the `RAID ClearReservations` command to remove any outstanding persistent reservations on the external RAID storage that block initialization operations.

OPTIONS

`RAID Clear`

This command removes all data on the storage and resets the disk RAID configuration. It also reassigns all the host-spare disks. The RAID volume groups are completely cleared out and then re-created. The complete operation results in an initialization overhead.

This operation may fail if any persistent reservations remain on the RAID storage. If the operation fails, run the `RAID ClearReservations` command to clear the persistent reservations. Then, try the `RAID Clear` command again.

Note: This command is available only on an unconfigured 53xx compute node, and only before role configuration.

`RAID ClearReservations`

This command removes all persistent reservations on the RAID storage. These reservations can exist if a configured 53xx appliance is re-imaged, or factory reset.

Note: This command is available only on an unconfigured 53xx compute node, and only before role configuration.

Support > Reboot

Support > Reboot – Reboot the system

SYNOPSIS

```
Reboot [Force]
```

DESCRIPTION

Use this command to reboot the current system. You cannot use this command to restart another system remotely.

OPTIONS

```
Reboot [Force]
```

Use this command to restart the system.

The `Force` parameter forces the system to restart even if services are not able to be stopped. Use this parameter if a previous attempt failed.

Support > RecoverStorage

Support > RecoverStorage – View or purge any storage recovered during a reimage

SYNOPSIS

```
RecoverStorage PurgeBackups
```

```
RecoverStorage ViewBackups
```

DESCRIPTION

This command exists under the `Main_Menu > Support` view. Use this command to view or purge the data sets that were saved during the reimage.

OPTIONS

```
RecoverStorage PurgeBackups
```

Use this command to purge the storage that was recovered during the Appliance reimage operation.

```
RecoverStorage UniversalShares
```

Mount and export any existing Universal Shares.

```
RecoverStorage ViewBackups
```

Use this command to view the storage that was recovered during the Appliance reimage operation.

EXAMPLES

The following prompt is displayed after you run the `RecoverStorage PurgeBackups` command.

```
Are you sure you want to delete data found on disk during reimage? (yes/no)
```

Type **yes** to delete the data recovered during reimage.

Support > Service

`Support > Service` – You can use this command to restart a service on a host. When you use this command you designate the name of the service that you want to restart and the target host name.

SYNOPSIS

```
Service Restart
```

```
Service Stop
```

DESCRIPTION

You can use this command to stop or restart a service on a host. You must provide the name of the service that you want to stop or restart.

OPTIONS

```
Service Restart ServiceName
```

Use this command to restart a service on your appliance. Here, *ServiceName* is the name of the service that you want to restart. For example, network.

```
Service Stop ServiceName
```

Use this command to stop a service on your appliance. Here, *ServiceName* is the name of the service that you want to stop. For example, smb.

Support > ServiceAllowed

Support > ServiceAllowed – Use the `ServiceAllowed` commands to set specific components of a Primary or an Expansion Storage Shelf to the Service Allowed mode so that service can be performed on those units.

SYNOPSIS

```
ServiceAllowed Set PrimaryShelf
```

```
ServiceAllowed Set ExpansionShelf
```

DESCRIPTION

The `ServiceAllowed` command options let you set specific components of a Primary or an Expansion Storage Shelf to the Service Allowed mode so that service can be performed on those units.

Veritas requires that you perform this procedure only with assistance from Veritas Technical Support. Before you attempt to run these commands, refer to the following documents:

NetBackup Appliance Administrator's Guide

NetBackup Appliance Troubleshooting Guide

OPTIONS

The following command options are available for the `ServiceAllowed Set PrimaryShelf` command:

```
ServiceAllowed Set PrimaryShelf Controller location flag
```

Use this command to set the Service Allowed flag for a Primary Shelf controller.

Where *location* is A or B, and *flag* is on or off.

```
ServiceAllowed Set PrimaryShelf FanCanister location flag
```

Use this command to set the Service Allowed flag for a Primary Shelf fan canister.

Where *location* is Left or Right, and *flag* is on or off.

```
ServiceAllowed Set PrimaryShelf HDD DrawerID SlotNo Flag
```

Use this command to set the Service Allowed flag for a Primary Shelf hard disk drive.

Where *DrawerID* is 1-5, *SlotNo* is 1-12, and *flag* is on or off.

`ServiceAllowed Set PrimaryShelf PowerCanister location flag`

Use this command to set the Service Allowed flag for a Primary Shelf power canister.

Where *location* is Top or Bottom, and *flag* is on or off.

The following command options are available for the `ServiceAllowed Set ExpansionShelf` command:

`ServiceAllowed Set ExpansionShelf ExpansionCanister location flag`

Use this command to set the Service Allowed flag for an Expansion Shelf canister.

Where *location* is Top or Bottom, and *flag* is on or off.

`ServiceAllowed Set ExpansionShelf FanCanister location flag`

Use this command to set the Service Allowed flag for an Expansion Shelf fan canister.

Where *location* is Left or Right, and *flag* is on or off.

`ServiceAllowed Set ExpansionShelf HDD ExpansionShelfID DrawerID SlotNo Flag`

Use this command to set the Service Allowed flag for an Expansion Shelf hard disk drive.

Where *ExpansionShelfID* is 0 - 98, *DrawerID* is 1-5, *SlotNo* is 1-12, and *flag* is on or off.

`ServiceAllowed Set ExpansionShelf PowerCanister location flag`

Use this command to set the Service Allowed flag for an Expansion Shelf power canister.

Where *location* is Top or Bottom, and *flag* is on or off.

Support > Show

Support > Show – Displays reference table for hardware diagnosis.

SYNOPSIS

Show HW-DiagnosisHelp

DESCRIPTION

Use this command to view the reference table for hardware diagnosis. Using the reference table, you can identify the potential causes of various error states, such as critical warnings or failures of a hardware.

OPTIONS

Show HW-DiagnosisHelp

Use this command to display the reference table for hardware diagnosis.

EXAMPLES

The following is an example of the information that is displayed when you run the Main > Support > Show HW-DiagnosisHelp command.

Reference Chart			
ID	Device	State	Diagnosis
1	Power Supply	Warning	Check if both the Power Supply Units are cabled and is receiving power * If PS is cabled and receiving power, call Veritas support to replace the Power Supply Unit
2	CPU	Failed	Check the status column. * If the status is "Disabled", run the test again. (ipmitool may sometimes report incorrect CPU status) * If the failure persists, call Veritas support to replace the CPU

			Check the status column
			* "Device Absent" indicates that the fan is either
			not inserted correctly or the power supply cable
3	Fan	Failed	for the fan is loose.
			* If the fan is inserted correctly or the power
			supply cable is inserted correctly on the
			motherboard, call Veritas support to replace the
			fan.

			Check the Speed column.
			* Speed will be above the high water mark levels.
			Check if any other fan is in failed state. If yes,
			call Veritas support to replace the failed fan.
4	Fan	Warning	Once replaced, the speed will stay within water
			mark level.
			* If none of the other fans have failed, check the
			temperature table. If the temperature of appliance
			rises, then fan speed increases unless proper
			cooling is provided to the machine.

			Check the "Slot number" column
5	Disk	Failed	
			* Call Veritas support to replace the drive in
			that slot

			Check the "Status" column
			* Drive in that slot was supposed to be in
			"Hotspare" state. It might have changed the state
6	Disk	Warning	due to a drive failure in another slot.
			* If none of the other drives are in failed state,
			copyback needs to be initiated so that the drive
			in this particular slot becomes a "hotspare"

7	Fiber	Failed	* Call Veritas support to replace the FC card
	Channel		

8	Temperature	Warning	* Make sure enough cooling is provided so that the temperature does not cross the high threshold limit

			Check the "status" column
9	RAID	Failed	* Multiple drive failure can result in RAID volume going offline

			Check the "Write Policy" column
			* If it is in "WriteThrough" mode, check the "RAID adapter" table. If either the "BBU learn cycle active" field for that RAID adapter is "yes" OR if the "BBU charge" field is less than 60%, the write policy will temporarily remain in WriteThrough mode.
10	RAID	Warning	* If "BBU learn cycle active" is not "yes" AND "BBU charge" is more than 60%, change the write policy for RAID-6 to "WriteBack with BBU" using MegaCli
			* Status can be "Degraded" or "Partially degraded". One or more drives might have failed. Call Veritas support to replace the failed drive (s) and wait for the rebuild and copyback operation to complete.

			Check "Adapter status" and "BBU status" column
			* Either adapter NVRAM, Memory, or Flash of the adapter is absent or bad. Call Veritas support to replace the RAID card
11	Adapter	Failed	* Either BBU, BBU voltage or BBU temperature is not OK, call Veritas support to replace the BBU on that adapter.

12	Adapter	Warning	* This is a temporary state when either the BBU learn cycle is active or the BBU charge is less than 60%

			* Warning indicates that either the PCI card in	
13	PCI	Warning	not inserted in the compatible slot or an	
			unsupported card is inserted.	
+-----+				

Support > Shutdown

Support > Shutdown – Turn off the system

SYNOPSIS

Shutdown

DESCRIPTION

Use this command to turn off the current system.

OPTIONS

Shutdown

Use to turn off the current system.

Support > Storage ClearReservations

Support > Storage ClearReservations – Clear the existing storage reservations for the high availability (HA) functions on the storage disks.

SYNOPSIS

```
Storage ClearReservations
```

DESCRIPTION

This command is available only on the NetBackup 53xx appliance and only before you perform the initial configuration on the appliance. Use this command to remove the existing storage reservations that are related to the HA functions when it blocks the appliance initialization operation.

OPTIONS

```
Storage ClearReservations
```

Use this command to clear the existing storage reservations that are related to the HA functions on the storage disks. Veritas recommends that you run this command only when the node is re-imaged or performed with the factory reset.

EXAMPLES

The following is an example of the information that is displayed when you run the Main > Support > Storage ClearReservations command:

```
Support> Storage ClearReservations
[Warning] Do not clear the reservations if a compute node is configured
with the media server role.
>>Do you want to continue? [yes, no]
```


Support > Storage Reset

Support > Storage Reset – Reset the appliance storage.

SYNOPSIS

Storage Reset

DESCRIPTION

Use the `Storage Reset` command to delete the backup data and partitions from the appliance, and configures the disk status for all the disks as New Available.

This command is available when the appliance is in a factory install state. An appliance is in a factory install state when it has not been configured as a master or media server (or the role is not configured). This command stops the NetBackup processes, deletes the backup data and partitions from the appliance, and configures the disk status for all the disks as New Available.

EXAMPLES

The following procedure is executed after you run the `Reset` command from the Support > Storage menu.

```
Support> Storage Reset
```

```
=====StorageReset=====
```

```
Resetting storage will delete any existing data and configuration.
```

```
>> Do you want to continue? (yes,no): yes
```

```
- [Info] Stopping NetBackup services ...please wait.
- [Info] Resetting the storage configuration...
- [Info] Stopping NetBackup processes... (6 mins approx)
- [Info] Checking whether the 'MSDP' storage partition exists...
- [Info] The 'MSDP' storage partition does not exist.
- [Info] Checking whether the 'Catalog' storage partition exists...
- [Info] Initiating deletion of 'Catalog' storage partition...
- [Info] Unmounting the 'Catalog' storage '0' partition...
- [Warning] Failed to unmount the 'Catalog' storage '0' partition.
  The 'Catalog' storage '0' partition may not be mounted.
- [Info] Deleting the 'Catalog' storage '0' partition...
- [Info] Checking whether the 'Configuration' storage partition exists...
```

- [Info] Initiating deletion of 'Configuration' storage partition...
- [Info] Unmounting the 'Configuration' storage '0' partition...
- [Warning] Failed to unmount the 'Configuration' storage '0' partition.
The 'Configuration' storage '0' partition may not be mounted.
- [Info] Deleting the 'Configuration' storage '0' partition...
- [Info] Checking whether the 'AdvancedDisk' storage partition exists...
- [Info] Initiating deletion of 'AdvancedDisk' storage partition...
- [Info] Unmounting the 'AdvancedDisk' storage '0' partition...
- [Warning] Failed to unmount the 'AdvancedDisk' storage '0' partition.
The 'AdvancedDisk' storage '0' partition may not be mounted.
- [Info] Deleting the 'AdvancedDisk' storage '0' partition...
- [Info] Removing the storage configuration...
- [Info] Succeeded.
- [Info] Starting NetBackup services ...
- [Info] Successfully started NetBackup services.

Support > Storage SanityCheck

Support > Storage SanityCheck – Use the Storage SanityCheck command if you want to disable or enable storage sanity checks.

SYNOPSIS

```
Storage SanityCheck Disable
```

```
Storage SanityCheck Enable
```

DESCRIPTION

Storage sanity check runs everyday and also runs as a part of storage manipulation operations. The Storage sanity check helps to fix some of the storage issues or reports them. The storage sanity check is enabled by default. Use the `Support> Storage SanityCheck Disable` command to disable the storage sanity check. This command can be used for debugging by Support engineers. Use the `Support> Storage SanityCheck Enable` command to enable the storage sanity check.

Support > Test

Support > Test – Test the current status of the various appliance components.

SYNOPSIS

Test Hardware

Test Software

DESCRIPTION

The appliance runs a test at regular intervals to check the status of its components. This ability of the appliance is referred to as self test. Use the `Test` command to verify the current status of the various appliance components.

OPTIONS

Test Hardware

Use this command to view the enhanced hardware monitoring page that displays the status of various hardware components.

Test Software

Use this command to test the current status of the various appliance software components.

EXAMPLES

The following is an example of information that is displayed when you run the `Main > Support > Test Hardware` command.

```
abc123.Support> Test Hardware
```

```
Compute Node abc123.example.com
```

```
Time Monitoring Ran: Wed Jul 20 2016 00:25:43 PDT
```

```
+-----+
|                                     Power Supply Information                                     |
|+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+|
|| ID | Status               | Wattage | HighWaterMark | State   |
|+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+|
```

2	Power Supply AC lost	0 Watts	940 Watts	Warning	
	+	+	+	+	+
	PCI Information				
	+	+	+	+	+
ID	Slot	Details	Firmware	State	
	+	+	+	+	+
5	5	Intel_X710	4.25 0x8000143f 0.0.0	Failed	
	+	+	+	+	+
	Disk Information				
	+	+	+	+	+
ID	Slot	Status	Foreign	HotSpare	Firmware
		Number	State	Type	Version
	+	+	+	+	+
-	2	Unconfigured Good, Spun Up	Foreign	N/A	0006
	+	+	+	+	+
-	7	Online, Spun Up	None	N/A	0006
	+	+	+	+	+
	+	+	+	+	+

The following is an example of information that is displayed when you run the [Main > Support > Test Software]command for a Master appliance.

xyz123.Support> Test Software

Running Validation tests on Master Appliance xyz123.

Checking whether serial number is present ...	[OK]
Checking whether installation is successful ...	[OK]
Checking whether critical kernel drivers exist and can work ...	[OK]
Checking whether SSH is enabled ...	[OK]
Checking whether hostname is set ...	[OK]
Checking whether IP address is set ...	[OK]
Checking whether appliance user accounts exist ...	[OK]
Checking whether required packages are installed ...	[OK]
Checking whether BIOS firmware is compatible with the software ...	[NA]
Checking whether registration information is properly set ...	[OK]
Checking whether NetBackup is configured and running ...	[OK]
Checking whether storage units and diskpools have been created ...	[OK]
Checking whether Web Server is configured and running ...	[OK]
Checking test backup and restore operations ...	[OK]
Expiring test backup images and deleting test policy ...	[OK]

Completed running tests on the appliance.

SELF TEST RESULT :

[PASS]