

Veritas NetBackup™ Virtual Appliance Documentation

Release 4.1



Veritas NetBackup™ Virtual Appliance 4.1 Documentation

Last updated: 2021-07-19

Legal Notice

Copyright © 2021 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	Getting to know the NetBackup Virtual Appliance	
		16
	NetBackup Virtual Appliance product description	16
	About the NetBackup Virtual Appliance primary server role	17
	About the NetBackup Virtual Appliance combined primary and media server role	18
	About the NetBackup Virtual Appliance media server role	18
	NetBackup Virtual Appliance supported features	19
	About the NetBackup Virtual Appliance documentation	22
	NetBackup Virtual Appliance 4.1 new features, enhancements, and changes	23
	Known limitations of the NetBackup Virtual Appliance 4.1 release	25
	Operational Notes for the NetBackup Virtual Appliance 4.1 release	26
Chapter 2	Preparing to deploy the appliance	29
	NetBackup Virtual Appliance product files (OVF templates)	29
	NetBackup Virtual Appliance deployment methods	32
	NetBackup Virtual Appliance deployment guidelines	34
	Configuration overview for NetBackup Virtual Appliance MSDP cloud applications	36
	NetBackup Virtual Appliance initial deployment checklist	37
Chapter 3	Deploying and configuring the appliance	40
	How to deploy and configure a NetBackup Virtual Appliance combined primary and media server	40
	Using the vSphere Client to deploy a combined primary and media server appliance	41
	Using the OVF Tool to deploy a combined primary and media server appliance	46
	Performing the initial configuration on a NetBackup Virtual Appliance combined primary and media server	48
	Completing the initial configuration of the NetBackup Virtual Appliance combined primary and media server	53

	How to deploy and configure a NetBackup Virtual Appliance media server	58
	Using the vSphere Client to deploy a media server appliance	59
	Using the OVF Tool to deploy a media server appliance	60
	Configuring a primary server to communicate with an appliance media server	62
	Performing the initial configuration on a NetBackup Virtual Appliance media server	64
	How to deploy and configure a NetBackup Virtual Appliance primary server	72
	Using the vSphere Client to deploy a NetBackup Virtual Appliance primary server	72
	Using the OVF Tool to deploy a primary server	74
	Performing the initial configuration on a NetBackup Virtual Appliance primary server	75
Chapter 4	Post initial configuration procedures	81
	About modifying the NetBackup Virtual Appliance settings	81
	Adding a permanent license key if an evaluation license key expires	82
	Managing license keys on the NetBackup Virtual Appliance	84
Chapter 5	Appliance common tasks	86
	Common tasks in NetBackup Virtual Appliance	86
Chapter 6	Storage management	89
	About NetBackup Virtual Appliance storage configuration	89
	About viewing storage space information using the <code>Show</code> command	92
	Resizing a partition	101
	Troubleshooting resize-related issues	102
	Moving a partition	102
	Creating an NDMP log partition	103
	Monitoring the progress of storage manipulation tasks	104
	Scanning storage devices using the NetBackup Virtual Appliance Shell Menu	105
	Adding storage space for the NetBackup Virtual Appliance	105
	Removing an existing storage disk	107
	About Universal Shares	107
	About OpenStorage plugin installation	109

	Installing the OpenStorage plugin	111
	Uninstalling the OpenStorage plugin	112
Chapter 7	Deduplication pool catalog backup and recovery	113
	About the NetBackup Virtual Appliance deduplication pool catalog backup policy	113
	Automatic configuration of the NetBackup Virtual Appliance deduplication pool catalog backup policy	114
	Manually configuring the NetBackup Virtual Appliance deduplication pool catalog backup policy	115
	Manually updating the NetBackup Virtual Appliance deduplication pool catalog backup policy	116
	Recovering the NetBackup Virtual Appliance deduplication pool catalog	117
Chapter 8	Network connection management	120
	About IPv4-IPv6-based network support	120
	Network settings for the NetBackup Virtual Appliance	121
	Configuring DNS and host name mapping for the NetBackup Virtual Appliance	122
	Setting the date and time on a NetBackup Virtual Appliance	123
	Configuring static routes on the NetBackup Virtual Appliance	124
	Expanding the bandwidth on the NetBackup Virtual Appliance	125
Chapter 9	Managing users	126
	About managing NetBackup Virtual Appliance users	127
	About NetBackup Virtual Appliance account types	128
	Adding NetBackup Virtual Appliance users	131
	Deleting NetBackup Virtual Appliance users	133
	Adding NetBackup Virtual Appliance user groups	134
	Deleting NetBackup Virtual Appliance user groups	137
	Granting roles to NetBackup Virtual Appliance users and user groups	138
	Revoking roles from NetBackup Virtual Appliance users and user groups	139
	About user name and password specifications	140
	About STIG-compliant password policy rules	144
	Changing NetBackup Virtual Appliance user passwords	145
	About password management and recovery	146
	About authenticating LDAP users	147

Adding or modifying an LDAP server configuration on the NetBackup Virtual Appliance	149
Importing an LDAP server configuration for the NetBackup Virtual Appliance	152
Setting the SSL certification for LDAP on the NetBackup Virtual Appliance	153
Exporting an LDAP server configuration from the NetBackup Virtual Appliance	154
Unconfiguring LDAP user authentication on the NetBackup Virtual Appliance	156
Disabling LDAP user authentication on the NetBackup Virtual Appliance	157
Enabling LDAP user authentication on the NetBackup Virtual Appliance	157
Adding an LDAP attribute mapping on the NetBackup Virtual Appliance	158
Deleting an LDAP attribute mapping on the NetBackup Virtual Appliance	159
About authenticating Active Directory users	159
Adding an Active Directory server configuration	161
Unconfiguring Active Directory user authentication on the NetBackup Virtual Appliance	162
About authentication using smart cards and digital certificates	163
About authenticating Kerberos-NIS users	165
Adding a Kerberos-NIS authentication configuration on the NetBackup Virtual Appliance	166
Unconfiguring Kerberos-NIS user authentication on the NetBackup Virtual Appliance	168
Generic user authentication guidelines	168
About user authorization on the NetBackup Virtual Appliance	170
NetBackup Virtual Appliance user role privileges	171
About the Administrator user role	173
About the NetBackupCLI user role	174
Creating NetBackup administrator user accounts	176
Logging on as a NetBackup administrator	177
Managing NetBackup administrator user account passwords	177
Viewing NetBackup administrator user accounts	179
Auditing NetBackup administrator accounts	179
Deleting NetBackup administrator user accounts	180

Chapter 10	Using the appliance	181
	About configuring Host parameters for your appliance on the NetBackup Virtual Appliance	181
	Configuring data buffer options on the NetBackup Virtual Appliance	182
	Configuring lifecycle parameters on the NetBackup Virtual Appliance	184
	Managing NetBackup Virtual Appliance deduplication	187
	About BMR integration	189
	About Copilot functionality and Share management	191
	Creating a Share	192
	Editing a Share	193
	Deleting a Share	195
	Moving a Share	195
	Viewing Share information from the NetBackup Virtual Appliance	
	Shell Menu	196
	NFS export options	196
	About NetBackup Virtual Appliance as a VMware backup host	197
	NetBackup Virtual Appliance as backup host: component overview	198
	Notes on NetBackup Virtual Appliance as a VMware backup host	198
	About running NetBackup commands from the appliance	199
	Running NetBackup commands from the NetBackup Virtual Appliance	199
	Creating a NetBackup touch file from the NetBackup Virtual Appliance	200
	Best practices for running NetBackup commands from the NetBackup Virtual Appliance	201
	About NetBackup operating system commands	202
	Known limitations of running NetBackup commands from the NetBackup Virtual Appliance	202
	About mounting a remote NFS	203
	Mounting a remote NFS drive	204
	Unmounting an NFS drive	206
	About Auto Image Replication from a NetBackup Virtual Appliance	208
	Prerequisites for Auto Image Replication	208
	Configuring a replication target	208
	Determining the appliance deduplication password	210
	Generating certificates	211

Chapter 11	Monitoring the appliance	212
	About NetBackup Virtual Appliance alerts	212
	Setting up email notifications for a NetBackup Virtual Appliance	213
	Setting up SNMP notifications for a NetBackup Virtual Appliance	214
	Enabling and disabling Call Home from the appliance shell menu	216
	Configuring a Call Home proxy server from the NetBackup Virtual Appliance Shell Menu	217
	About SNMP	218
	About the Management Information Base (MIB)	219
	About Call Home	219
	Understanding the Call Home workflow	221
	About the Product Improvement Program	221
	About AutoSupport	222
	About storage email alerts	223
Chapter 12	Appliance security	224
	About Symantec Data Center Security on the NetBackup Virtual Appliance	225
	Auditing the SDCS logs on the NetBackup Virtual Appliance	226
	Viewing SDCS audit log details	228
	Changing the SDCS log retention settings on the NetBackup Virtual Appliance	230
	About SDCS event type codes and severity codes on the NetBackup Virtual Appliance	231
	About data security	233
	About data integrity	234
	About data classification	234
	About data encryption	235
	KMS support	235
	About SSL usage	239
	About implementing ECA certificates	240
	About the NetBackup Virtual Appliance intrusion detection system	242
	About the NetBackup Virtual Appliance intrusion prevention system	243
	Major components of the NetBackup Virtual Appliance OS	244
	OS STIG hardening for NetBackup Virtual Appliance	245
	FIPS 140-2 conformance for NetBackup Virtual Appliance	246
	Disable user access to the NetBackup appliance operating system	247
	Manage support access to the maintenance shell	249
	About the appliance login banner	250

Setting the appliance login banner	250
Creating the appliance login banner	251
Removing the appliance login banner	251
Log Forwarding feature overview	252
Chapter 13 Upgrading the appliance	255
About upgrading to NetBackup Virtual Appliance software version 4.1	255
Supported upgrade paths	255
Preflight check before the upgrade	256
Appliance behavior during upgrades	256
About corresponding NetBackup software versions	257
About the Appliance Install Manager	257
Requirements and best practices for upgrading NetBackup appliances	258
Upgrade time estimation	259
Pre-upgrade tasks for appliance upgrades	259
Methods for downloading appliance software release updates	261
Downloading software updates directly to a NetBackup appliance	261
Downloading software updates to a NetBackup appliance using a client share	262
Installing a NetBackup Virtual Appliance software update using the NetBackup Virtual Appliance Shell Menu	264
Troubleshooting upgrade issues	267
Chapter 14 NetBackup client upgrades with VxUpdate	268
About VxUpdate	268
VxUpdate repository management	269
Deployment policy management	272
Manually initiating upgrades from the primary server using VxUpdate	276
Manually initiating upgrades from the client using VxUpdate	281
Deployment job status	282
Chapter 15 Appliance restore	285
About appliance restore	285
Creating an appliance checkpoint from the appliance shell menu	286
Rollback to an appliance checkpoint from the appliance shell menu	288
About NetBackup Virtual Appliance factory reset	290

	Factory reset best practices	291
	How to factory reset the NetBackup Virtual Appliance	292
Chapter 16	Decommissioning and Reconfiguring	295
	About decommissioning a NetBackup Virtual Appliance	295
	Decommissioning a NetBackup Virtual Appliance with the media server role	296
Chapter 17	Troubleshooting	297
	About troubleshooting the NetBackup Virtual Appliance	297
	About contacting Technical Support	300
	Determining the NetBackup Virtual Appliance serial number	301
	About disaster recovery	302
	Recovering a NetBackup appliance primary server using NetBackup catalog restore	303
	About NetBackup support utilities	306
	NetBackup Domain Network Analyzer (NBDNA)	306
	NetBackup Support Utility (NBSU)	308
	Troubleshooting NetBackup Virtual Appliance initial deployment issues	308
	Error messages displayed on the NetBackup Virtual Appliance Shell Menu	312
	NetBackup status codes applicable for NetBackup Virtual Appliance	317
	Installing an EEB	318
	Rolling back an EEB using the NetBackup Virtual Appliance Shell Menu	319
Chapter 18	Appliance logging	321
	About NetBackup Virtual Appliance log files	321
	Viewing log files using the Support command	323
	Where to find NetBackup Virtual Appliance log files using the Browse command	324
	Enabling and disabling VxMS logging	325
	Gathering device logs on a NetBackup virtual appliance	326
	About forwarding logs to an external server	327
	Uploading certificates for TLS	328
	Enabling log forwarding	329
	Changing the log forwarding interval	330
	Viewing the log forwarding configuration	330
	Disabling log forwarding	331

Chapter 19	Commands overview	332
	About the NetBackup Virtual Appliance Shell Menu	332
	Logging in to the NetBackup Virtual Appliance Shell Menu	332
	Using the NetBackup Virtual Appliance Shell Menu	333
	About the NetBackup Virtual Appliance Shell Menu command views	334
Appendix A	Appliance commands	336
	Main > Appliance > Primary	337
	Main > Appliance > Media	338
	Main > Appliance > ShowDedupPassword	340
	Main > Appliance > Status	341
	Main > Appliance > Configure	342
Appendix B	Manage commands	344
	Main > Manage > Software > Delete	346
	Main > Manage > Software > Download	347
	Main > Manage > Software > List	348
	Main > Manage > Software > Install	350
	Main > Manage > Software > Share	351
	Main > Manage > Software > Readme	352
	Main > Manage > Software > Rollback	354
	Main > Manage > Software > Cancel	355
	Main > Manage > Software > DownloadAnalyzer	356
	Main > Manage > Software > DownloadProgress	357
	Main > Manage > Software > UpgradeStatus	358
	Main > Manage > Software > VxUpdate	359
	Main > Manage > Storage > Show	361
	Main > Manage > Storage > Add	363
	Main > Manage > Storage > Create	365
	Main > Manage > Storage > Delete	366
	Main > Manage > Storage > Edit	367
	Main > Manage > Storage > Monitor	370
	Main > Manage > Storage > Move	371
	Main > Manage > Storage > Remove	373
	Main > Manage > Storage > Resize	375
	Main > Manage > Storage > Scan	377
	Main > Manage > OpenStorage > Install	378
	Main > Manage > OpenStorage > List	380
	Main > Manage > OpenStorage > Readme	382
	Main > Manage > OpenStorage > Share	384

Main > Manage > OpenStorage > Uninstall	386
Main > Manage > MountPoints > List	388
Main > Manage > MountPoints > Mount	389
Main > Manage > MountPoints > Unmount	391
Main > Manage > License > Add	393
Main > Manage > License > List	394
Main > Manage > License > ListInfo	395
Main > Manage > License > Remove	396
Main > Manage > Certificates > Generate	397
Main > Manage > Certificates > Delete	398
Main > Manage > NetBackupCLI > Create	399
Main > Manage > NetBackupCLI > Delete	400
Main > Manage > NetBackupCLI > List	401

Appendix C Monitor commands 402

Main > Monitor > Uptime	403
Main > Monitor > Who	404
Main > Monitor > NetworkStatus	405
Main > Monitor > Top	407
Main > Monitor > MemoryStatus	409
Main > Monitor > SDCS	411
Main > Monitor > NetBackup	413
Main > Monitor > Hardware	414

Appendix D Network commands 416

Main > Network > Configure	417
Main > Network > Date	419
Main > Network > DNS	420
Main > Network > Gateway	422
Main > Network > Hostname	424
Main > Network > Hosts	425
Main > Network > IPv4	426
Main > Network > IPv6	427
Main > Network > LinkAggregation	428
Main > Network > NetStat	432
Main > Network > NTPServer	433
Main > Network > Ping	434
Main > Network > SetProperty	435
Main > Network > Show	436
Main > Network > TimeZone	437
Main > Network > TraceRoute	438
Main > Network > Unconfigure	439

	Main > Network > WANOptimization	440
Appendix E	Reports commands	445
	Main > Reports > Deduplication	446
	Main > Reports > Process	447
Appendix F	Settings commands	448
	Main > Settings > Deduplication	450
	Main > Settings > LifeCycle	459
	Main > Settings > LogForwarding	463
	Main > Settings > NetBackup	466
	Main > Settings > NetBackup DNAT	471
	Main > Settings > NetBackup NATServers	473
	Main > Settings > Password	474
	Main > Settings > SystemLocale	475
	Main > Settings > Share	478
	Main > Settings > Sysctl	479
	Main > Settings > Notifications > LoginBanner	481
	Main > Settings > Security > Authentication > AccountStatus	484
	Main > Settings > Security > Authentication > LDAP	486
	Main > Settings > Security > Authentication > ActiveDirectory	493
	Main > Settings > Security > Authentication > Kerberos	495
	Main > Settings > Security > Authentication > LocalUser	498
	Main > Settings > Security > Authentication > CIFSShare	501
	Main > Settings > Security > Authorization	504
	Main > Settings > Security > Certificate	507
	Main > Settings > Security > STIG	508
	Main > Settings > Security > FIPS	509
	Main > Settings > Security > SecurityLevel	511
	Main > Settings > Alerts > CallHome	513
	Main > Settings > Alerts > SNMP	517
	Main > Settings > Alerts > Email	520
	Main > Settings > Alerts > Hardware	522
Appendix G	Support commands	523
	Main > Support > Checkpoint	525
	Main > Support > DataCollect	528
	Main > Support > Disk	530
	Main > Support > Errors	531
	Main > Support > FactoryReset	532
	Main > Support > InfraServices	533

Main > Support > InstantAccess	535
Main > Support > iostat	536
Main > Support > LogBrowser	539
Main > Support > Logs	540
Main > Support > Maintenance	546
Main > Support > Messages	548
Main > Support > NBDNA	549
Main > Support > nbperfchk	551
Main > Support > NBSU	555
Main > Support > Processes	556
Main > Support > Reboot	557
Main > Support > Service	558
Main > Support > Shutdown	560
Main > Support > Storage Create NDMPLogPartition	561
Main > Support > Storage SanityCheck	562
Main > Support > Storage Reset	563
Main > Support > System	565
Main > Support > Test	567

Getting to know the NetBackup Virtual Appliance

This chapter includes the following topics:

- [NetBackup Virtual Appliance product description](#)
- [NetBackup Virtual Appliance supported features](#)
- [About the NetBackup Virtual Appliance documentation](#)
- [NetBackup Virtual Appliance 4.1 new features, enhancements, and changes](#)
- [Known limitations of the NetBackup Virtual Appliance 4.1 release](#)
- [Operational Notes for the NetBackup Virtual Appliance 4.1 release](#)

NetBackup Virtual Appliance product description

The NetBackup Virtual Appliance product is a scalable data protection solution that is designed to integrate NetBackup solutions into your virtual environment. It provides an alternative to existing NetBackup physical appliance solutions to let you use your own hardware and leverage your existing NetBackup expertise.

The NetBackup Virtual Appliance product provides the following solutions:

- **NetBackup Virtual Appliance primary server**
The NetBackup Virtual Appliance provides a dedicated NetBackup primary server solution for deployment in a virtual environment. It provides the capabilities of a regular NetBackup primary server, but requires minimal on-site infrastructure management expertise.

See [“About the NetBackup Virtual Appliance primary server role”](#) on page 17.

- **NetBackup Virtual Appliance combined primary and media server for remote offices and branch offices (ROBO)**

The NetBackup Virtual Appliance provides a combined primary and media server solution for a remote office or branch office. It provides a lower-cost alternative to existing NetBackup Appliance solutions for environments with smaller data protection requirements, and requires minimal on-site infrastructure management expertise. You can configure the NetBackup Virtual Appliance to link back to NetBackup in the data center for replication of remote office or branch office data.

Note: The NetBackup Virtual Appliance with the combined primary and media server role does not support adding an additional media server.

See [“About the NetBackup Virtual Appliance combined primary and media server role”](#) on page 18.

- **NetBackup Virtual Appliance media server for data centers (DC)**

The NetBackup Virtual Appliance provides a media server solution for data centers. It can scale up in the number of instances and storage capacity to meet the growing requirement of data protection in data centers. You can use NetBackup to replicate data from the NetBackup Virtual Appliance to other sites for disaster recovery.

See [“About the NetBackup Virtual Appliance media server role”](#) on page 18.

The NetBackup Virtual Appliance provides a simplified solution for NetBackup configuration and the daily management of your backup environment. The goal is to provide a solution that eliminates the need to provide dedicated individuals to manage their backup environment.

See [“About the NetBackup Virtual Appliance documentation”](#) on page 22.

About the NetBackup Virtual Appliance primary server role

In this role, the NetBackup Virtual Appliance operates as dedicated NetBackup primary server. You configure and use this appliance much like you would use a regular NetBackup primary server with no attached storage.

This appliance role provides a simplified administrative interface for the local network and storage management. However, the majority of NetBackup administration such as backup management must be performed through the traditional NetBackup Administration Console.

For complete NetBackup administration information, see the *NetBackup Administrator's Guide for UNIX and Linux, Volume I and Volume II*.

See [“NetBackup Virtual Appliance product description”](#) on page 16.

See [“About the NetBackup Virtual Appliance combined primary and media server role”](#) on page 18.

See [“About the NetBackup Virtual Appliance media server role”](#) on page 18.

See [“About the NetBackup Virtual Appliance documentation”](#) on page 22.

About the NetBackup Virtual Appliance combined primary and media server role

In this role, the NetBackup Virtual Appliance is a combined primary and media server with its own virtual storage. You configure and use this appliance much like you would use a regular NetBackup primary server with attached storage or a NetBackup 52xx Appliance that is configured as a primary server. You can schedule backups or start a backup manually. Users with the appropriate privileges can perform restores.

You can also configure the NetBackup Virtual Appliance combined primary and media server for MSDP cloud applications. See [“Configuration overview for NetBackup Virtual Appliance MSDP cloud applications”](#) on page 36.

This appliance role provides a simplified administrative interface for the local network and storage management. However, the majority of NetBackup administration such as backup management must be performed through the traditional NetBackup Administration Console.

For complete NetBackup administration information, see the *NetBackup Administrator's Guide for UNIX and Linux, Volume I and Volume II*.

See [“NetBackup Virtual Appliance product description”](#) on page 16.

See [“About the NetBackup Virtual Appliance primary server role”](#) on page 17.

See [“About the NetBackup Virtual Appliance media server role”](#) on page 18.

See [“About the NetBackup Virtual Appliance documentation”](#) on page 22.

About the NetBackup Virtual Appliance media server role

In this role, a NetBackup Virtual Appliance operates as a media server with user-added disk storage.

After the deployment, the virtual appliance contains only the internal storage that is used for storing the operating system, checkpoints, and system logs. The internal storage cannot be used for storing any data or taking any backups. For backup and restore, you must first add disk storage to this virtual machine from the virtualization software(VMware).

You can also configure the NetBackup Virtual Appliance media server for MSDP cloud applications. See [“Configuration overview for NetBackup Virtual Appliance MSDP cloud applications”](#) on page 36.

This appliance role provides a simplified administrative interface for the local network and for disk storage management. However, the majority of NetBackup administration such as backup management is performed on the primary server.

When you perform the initial configuration on the appliance, specify the associated primary server:

- **For use with a traditional NetBackup primary server**
- **For use with a NetBackup physical appliance primary server**
- **For use with a NetBackup Virtual Appliance primary server**

See [“NetBackup Virtual Appliance product description”](#) on page 16.

See [“About the NetBackup Virtual Appliance primary server role”](#) on page 17.

See [“About the NetBackup Virtual Appliance combined primary and media server role”](#) on page 18.

See [“About the NetBackup Virtual Appliance documentation”](#) on page 22.

NetBackup Virtual Appliance supported features

Review the following for a full list of the features that are supported by your deployment.

Basic features

The appliance software supports all of the basic features.

- The NetBackup Virtual Appliance Shell Menu.
The shell menu is a command line interface for appliance configuration and management.
- NetBackup preinstalled.
NetBackup Enterprise Server software is already installed and configured to work with the operating system. This feature simplifies the deployment and integration into an existing NetBackup environment.

Note: The Enhanced Auditing feature that was released in NetBackup version 7.7 is not currently supported for use on NetBackup Virtual Appliance. This feature should not be configured or enabled on an appliance.

- Support for the core NetBackup software agents.
The NetBackup agents optimize the performance of critical databases and applications.
See the *NetBackup Administrator's Guide Volume I* for more information about the policy types that are supported for each software agent. For the latest appliance compatibility information, refer to the Hardware Compatibility List on the Veritas Support website:
www.netbackup.com/compatibility
- Symantec Data Center Security (SDCS) integration.
The SDCS agent is installed and configured when you initially deploy your appliance. By default, SDCS helps secure the appliance using host-based intrusion prevention and detection technology.
See “[About Symantec Data Center Security on the NetBackup Virtual Appliance](#)” on page 225.
- AutoSupport.
The appliance can monitor key components and provide proactive monitoring and messaging. Veritas Support uses this information to resolve any issues that you might report.
See “[About AutoSupport](#)” on page 222.
- Bare Metal Restore (BMR) integration.
BMR is the server recovery option of NetBackup. BMR automates and streamlines the server recovery process.
See “[About BMR integration](#)” on page 189.
- Link Aggregation
See “[Expanding the bandwidth on the NetBackup Virtual Appliance](#)” on page 125.

Additional features

The appliance software supports the following additional features depending on the virtual appliance type.

Primary server

- Adding media servers to the NetBackup domain.
You can add media servers to this primary server. The primary server manages backups, archives, and restores.

Combined primary and media server

- Media Server Deduplication Pool (MSDP) storage.
MSDP is an embedded deduplication technology that reduces the amount of space that is needed for backups.
- AdvancedDisk storage.

Advanced disk can provide faster restore operation but is not space-optimized like MSDP.

Note: AdvancedDisk storage does not support Auto Image Replication. To replicate the data on the AdvancedDisk storage, you can first duplicate the data to MSDP, and then use MSDP for replication.

- Checkpoint creation and rollback.
Checkpoint enables you to restore the appliance to a specific state. That state is determined through the use of checkpoints.
- Backup of VMware virtual machines.
The appliance supports direct backup of VMware virtual machines. The appliance can back up virtual machines without a separate backup host.
See [“About NetBackup Virtual Appliance as a VMware backup host”](#) on page 197.
- MSDP cloud.
You can configure the appliance for MSDP cloud applications. See [“Configuration overview for NetBackup Virtual Appliance MSDP cloud applications”](#) on page 36.
- Instant Access.
The Instant Access feature allows you to create an Instant Access VM from a NetBackup backup image. The VM is available almost instantaneously, achieving a near-zero recovery time objective. For more information about how to use this feature, see the *NetBackup Web UI VMware Administrator's Guide*.

Media server

- Media Server Deduplication Pool (MSDP) storage.
MSDP is an embedded deduplication technology that reduces the amount of space that is needed for backups.
- AdvancedDisk storage.
Advanced disk can provide faster restore operation but is not space-optimized like MSDP.

Note: AdvancedDisk storage does not support Auto Image Replication. To replicate the data on the AdvancedDisk storage, you can first duplicate the data to MSDP, and then use MSDP for replication.

- Copilot (Standard Shares only).
Copilot enables Oracle database administrators to work with Veritas appliance administrators to perform a streamlined backup and restore process of Oracle databases.

- Checkpoint creation and rollback.
Checkpoint enables you to restore the appliance to a specific state. That state is determined through the use of checkpoints.
- Factory reset.
Factory reset enables you to restore the appliance to the original factory state.
- Backup of VMware virtual machines.
The appliance supports direct backup of VMware virtual machines. The appliance can back up virtual machines without a separate backup host.
See [“About NetBackup Virtual Appliance as a VMware backup host”](#) on page 197.
- MSDP cloud.
You can configure the appliance for MSDP cloud applications. See [“Configuration overview for NetBackup Virtual Appliance MSDP cloud applications”](#) on page 36.
- Instant Access.
The Instant Access feature allows you to create an Instant Access VM from a NetBackup backup image. The VM is available almost instantaneously, achieving a near-zero recovery time objective. For more information about how to use this feature, see the *NetBackup Web UI VMware Administrator's Guide*.

About the NetBackup Virtual Appliance documentation

The NetBackup Virtual Appliance documentation helps to ensure that you can successfully install, configure, and use your appliance. The documentation includes the *NetBackup Virtual Appliance Getting Started Guide* and the *NetBackup Virtual Appliance Documentation* web topics that are available from the following sites:

[Appliance documentation page](#) on the Veritas Support website.

[Services and Operations Readiness Tools \(SORT\)/documents](#)

The *NetBackup Virtual Appliance Getting Started Guide* includes all of the information you need to deploy and start using your appliance, as well as important notes relevant to the current release.

All appliance documentation content is also searchable using your favorite web search engine.

See [“NetBackup Virtual Appliance product description”](#) on page 16.

NetBackup Virtual Appliance 4.1 new features, enhancements, and changes

The following list describes the new features, enhancements, and changes in the NetBackup Virtual Appliance 4.1 release:

- Terminology changes for NetBackup Virtual Appliance
Starting with this release, the NetBackup Virtual Appliance interfaces and documentation are changing the following terms:
 - "primary server" replaces master server
 - "allowed list" replaces whitelist/white list
 - "blocked list" replaces blacklist/black list

Most of these changes have been implemented, however, it is possible that the previous terms may still appear in some messages, interface screen captures, and line art or graphic images. Any remaining updates will be addressed in the next software release.

Note: Some system messages may contain the word "slave". These occurrences are not in the NetBackup Virtual Appliance code, but reside in third party packages/ applications that are included with the product. For example, Linux and Samba. These occurrences are minimal and appear mostly in system messages, along with the option or variable name used in the `Main > Network > LinkAggregation` command. Those vendors are responsible for making the necessary changes in their packages/applications. Veritas does not currently have a time line from its third party vendors with regard to terminology changes.

- VmWare vSphere 7U1 support
VMware vSphere version 7U1 is now supported for deployment.
- Factory reset support for the NetBackup Virtual Appliance combined primary and media server
Factory reset is now supported on the NetBackup Virtual Appliance combined primary and media server. It is not supported on a NetBackup Virtual Appliance primary server.
- Change to Appliance Install Manager availability
You can no longer use the Appliance Install Manager to view the upgrade progress between the first and second restarts of the operation. During that time, use the VMware Remote Console to monitor the upgrade progress. You can use the Appliance Install Manager after the second restart.
- RBAC default privileges change for NetBackup CLI users

Starting with this release, NetBackup CLI users are no longer granted any NetBackup RBAC privileges by default. This includes new 4.1 or later appliance deployments or appliance upgrades to version 4.1 or later with existing NetBackup CLI users. If any of these users require access to the NetBackup web UI or REST APIs, you must manually grant them the appropriate NetBackup RBAC privileges. For complete details, see the *NetBackup Web UI Administrator's Guide*.

- New command options to manage NFS, NMB, SMB services
Starting with this release, new `Main > Support > Service` command options let you fully manage the NFS, NMB, and SMB services on the appliance. The new options are `[Service Disable]`, `[Service Enable]`, and `[Service Show]`. See [Support > Service](#) on page 558.
- CIFS and NFS share folder location changes for Log Forwarding and OpenStorage plugins
Starting with this release, the folder locations for Log Forwarding and OpenStorage plugins have changed as follows:
 - Log Forwarding/CIFS - from `\server_name\logforwarding` to `\server_name\general_share`
 - Log Forwarding/NFS - from `server_name:/inst/logforwarding` to `server_name:/inst/share`
 - OpenStorage/CIFS - from `\\server_name\incoming_plugins` to `\\server_name\general_share`
 - OpenStorage/NFS - from `server_name:/inst/plugin/incoming` to `server_name:/inst/share`
- STIG lists available on Veritas Support site
Starting with this release, the STIG rule lists have been removed from the *NetBackup Virtual Appliance Documentation*. All STIG rule lists are now available in separate documents on the Veritas Support site. Two checklists are currently available, one for the OS and one for Application Security STIG. For instructions about how to obtain these documents, go to the **Latest releases** page on the [Veritas Download Center](#), navigate to **NetBackup Virtual Appliance** and click **Learn more**.
- New RBAC requirements for enabling KMS encryption
Starting with this release, the NetBackupCLI user used to enable KMS encryption must be assigned the Default Security Administrator role. See [“KMS support”](#) on page 235.
- New commands to manage locked accounts on the appliance

Starting with this release, new `Settings > Security > Authentication > AccountStatus` commands view lets you view and reinstate locked accounts. The new command-line options are `ListLockedAccounts` and `UnlockAccounts`. See [Settings > Security > Authentication > AccountStatus](#) on page 484.

- New commands to register an external certificate authority (ECA) on the appliance.
 Starting with this release, the `Settings > Security > Certificate` commands view lets you manage external certificates on an appliance. The `Import` command-line option is modified to register and enable the ECA on NetBackup and NetBackup Virtual Appliance layers.
 See [Main > Settings > Security > Certificate](#) on page 507.

Known limitations of the NetBackup Virtual Appliance 4.1 release

The NetBackup Virtual Appliance contains similar software as NetBackup Appliance. However, some of the features that are supported on the physical appliances are not currently supported on the virtual appliance.

The following list describes the known limitations for the NetBackup Virtual Appliance 4.1 release:

- The appliance software is currently available in English only.
- The NetBackup Virtual Appliance Web Console and the Veritas Remote Management interface (IPMI) are not supported. Use the NetBackup Virtual Appliance Shell Menu or the NetBackup Administration Console to log on and manage the appliance.
- Factory reset is not available on a NetBackup Virtual Appliance combined primary and media server. You cannot return your appliance to the factory state. If you encounter any severe issues, contact Veritas Support for assistance. You may need to redeploy the appliance if the issue cannot be resolved.
- Tape devices and libraries are not supported.
- The following network features are not available:
 - Fibre Channel
 - Fibre Transport
 - SAN Client
 - VLAN
 - IPsec

- iSCSI
- The Copilot feature is only available on the NetBackup Virtual Appliance media server for data centers (DC). Standard shares are supported. Optimized shares are not supported.
- The self-test feature is limited to the NetBackup Virtual Appliance software.
- Appliance monitoring for AutoSupport is limited to the following:
 - Partition information
 - MSDP statistics
 - NetBackup Virtual Appliance software version
 - NetBackup version
 - Appliance model
 - Appliance configuration

Note: NetBackup Virtual Appliance is not currently supported for registration.

- The Symantec Data Center Security (SDCS) managed mode is not currently available. SDCS operates in unmanaged mode on the appliance.

See [“Operational Notes for the NetBackup Virtual Appliance 4.1 release”](#) on page 26.

See [“NetBackup Virtual Appliance product description”](#) on page 16.

Operational Notes for the NetBackup Virtual Appliance 4.1 release

This chapter contains the topics that explain important aspects of NetBackup Virtual Appliance 4.1 operations that may not be documented elsewhere in the documentation.

Because NetBackup Virtual Appliance 4.1 installs NetBackup 9.1 software, the operational notes that apply to NetBackup 9.1 also apply to NetBackup Virtual Appliance 4.1. For more information on the operational notes for NetBackup, refer to the *NetBackup 9.1 Release Notes*. The *NetBackup Release Notes* are available from the [NetBackup Documentation page](#) on the Veritas Support website.

The following list contains the notes and the known issues that apply for this release:

- Customized STIG login banner is not retained after upgrade on STIG-enabled appliances

If STIG is enabled and you have customized the login banner prior to an upgrade, the login banner is reset to the default STIG login banner after the upgrade. To resolve this issue, you must reconfigure the customized STIG login banner manually.

- Failed Instant Access (IA) workload when ECA is enabled on NetBackup Virtual Appliance and not on NetBackup

An IA workload fails while attempting to access NGINX on an MSDP server, if ECA is enabled on NetBackup Virtual Appliance and not on NetBackup. To resolve this issue re-import the ECA certificates on the appliance using the `Settings > Security > Certificate > Import` command. The `Import` command registers and enables the same ECA on NetBackup and NetBackup Virtual Appliance layers.

- Intermittent test email notification after upgrade
After upgrading to version 4.0, the test email may not always succeed. To workaround this issue, delete all of the SMTP server configuration information and then re-enter all of the information.
- After an upgrade to software version 4.1, NetBackup CLI users may not be able to log in to the appliance. To resolve this issue, log in to the appliance as the administrator and run the following command:

```
Support->Service Restart nbapp-nbcli.
```

- When you attempt to copy a software update to the share directory, do not initiate any other commands until the copy finishes. If you run a command during the copy process, you may see that the software update is listed and available. However, if you install that software update, it can fail.
- If you receive an email stating "No license exists" during the initial configuration of a media server, you can safely disregard the email. The email is sent during host name configuration. The license key file is renamed when it is modified with the new host name, and the alert mechanism cannot locate the license temporarily. When the configuration completes, the license is set correctly. You can check the license key with the `Main > Manage > License > List` command in the NetBackup Virtual Appliance Shell Menu.
- Windows 7/8.1 clients cannot automatically access the appliance CIFS shares. To work around this issue, run the following command from a Windows command prompt on the client:

```
net use /user:admin \\appliance-name *, where appliance-name is the fully qualified domain name (FQDN) of the appliance.
```

Enter your appliance administrator password at the prompt.
Once you have run this command, the client is able to access the CIFS shares.

- The functionality of Active Directory (AD) user names is inconsistent, as described in the following scenarios:
 - NetBackup Virtual Appliance Shell Menu
This interface does not recognize Active Directory (AD) user names as case sensitive.
 - NetBackup Java Console
This interface does recognize Active Directory (AD) user names as case sensitive. When you enter these user names with all lowercase letters, access to the NetBackup Administrator's Console is granted. If you enter these user names with any or all uppercase letters, access to the NetBackup Backup, Archive, and Restore interface is granted.

See [“Known limitations of the NetBackup Virtual Appliance 4.1 release”](#) on page 25.

See [“NetBackup Virtual Appliance product description”](#) on page 16.

Preparing to deploy the appliance

This chapter includes the following topics:

- [NetBackup Virtual Appliance product files \(OVF templates\)](#)
- [NetBackup Virtual Appliance deployment methods](#)
- [NetBackup Virtual Appliance deployment guidelines](#)

NetBackup Virtual Appliance product files (OVF templates)

This section describes the NetBackup Virtual Appliance product files (OVF templates) for deployment. The product files are different in appliance roles and initial storage capacity.

You can download the NetBackup Virtual Appliance product file from the [Download Center](#) on the Veritas Support website.

Primary server

Table 2-1 NetBackup Virtual Appliance primary server product file

Product file	Description
Only one product file	■ CPU and memory 8 vCPUs, 16 GB memory ■ Storage capacity The primary server appliance does not have its own virtual storage. ■ Disks One System disk at 512 GB for the OS (does not come out of your NetBackup license). One Base disk at 900 GB for the NetBackup catalog. ■ Network interfaces Up to 8 virtual NICs ■ Virtual machine hardware Version 13

See [“About the NetBackup Virtual Appliance primary server role”](#) on page 17.

Combined primary and media server for remote offices and branch offices (ROBO)

For the combined primary and media server, Veritas provides the automatic initial configuration option. By using a product file that supports this option, the deployment wizard passes in the appliance network and storage configuration as OVF properties during the deployment process. When the deployment is complete, the appliance network and storage are configured based on these values. Then, you need to perform the remaining steps from the appliance shell menu to complete the initial configuration.

Table 2-2 NetBackup Virtual Appliance combined primary and media server product files

Product file	Description
Product file 1: NetBackup_VA_ROBO_ Vmware_GUI_ <version>_EN.ova	Note: This product file requires a VMware vCenter Server. - How to perform initial configuration Automatic initial configuration - CPU and memory 8 vCPUs, 16 GB memory - Storage capacity Flexible. When you deploy the appliance, the initial capacity is 0.5 TB. After deployment, you can resize the storage up to 16 TB. - Disks One System disk at 512 GB for the OS (does not come out of your NetBackup license). One Base disk at 614 GB for the storage. 102 GB of the disk space is used for storage metadata. - Network interfaces Up to 8 virtual NICs - Virtual machine hardware Version 13
Product file 2: NetBackup_VA_ROBO_ Vmware_<version>_ EN.ova	Note: This product file requires a VMware vCenter Server. - How to perform initial configuration Initial configuration from the shell menu - CPU and memory 8 vCPUs, 16 GB memory - Storage capacity Flexible. When you deploy the appliance, the initial capacity is 0.5 TB. After deployment, you can resize the storage up to 16 TB. - Disks One System disk at 512 GB for the OS (does not come out of your NetBackup license). One Base disk at 614 GB for the storage. 102 GB of the disk space is used for storage metadata. - Network interfaces Up to 8 virtual NICs - Virtual machine hardware Version 13

See [“About the NetBackup Virtual Appliance combined primary and media server role”](#) on page 18.

Media server for data centers (DC)

Table 2-3 NetBackup Virtual Appliance media server product file

Product file	Description
Only one product file	- CPU and memory 8 vCPUs, 16 GB memory - Storage capacity No initial disk storage. After the deployment, you can create virtual disks to add to the virtual appliance from the virtualization software (VMware vSphere). - Disks One System disk at 512 GB for the OS (does not come out of your NetBackup license). No Base disk for the storage. Note: Create at least one virtual disk to add to the appliance after the deployment is complete. Otherwise you cannot perform the initial configuration. - Network interfaces Up to 8 virtual NICs - Virtual machine hardware Version 13

See [“About the NetBackup Virtual Appliance media server role”](#) on page 18.

See also

See [“How to deploy and configure a NetBackup Virtual Appliance combined primary and media server”](#) on page 40.

See [“How to deploy and configure a NetBackup Virtual Appliance media server”](#) on page 58.

See [“How to deploy and configure a NetBackup Virtual Appliance primary server”](#) on page 72.

NetBackup Virtual Appliance deployment methods

You can choose to deploy a NetBackup Virtual Appliance using GUI or CLI.

- GUI deployment

Use the VMware vSphere Client or the browser-based VMware vSphere Web Client. A wizard guides you through the deployment steps.

- **CLI deployment**

Use the VMware OVF Tool. You need to specify the required deployment properties.

For example:

```
ovftool
--name=<nbva_name>
--acceptAllEulas
--net:"VM Network=<vm_network>"
--allowAllExtraConfig
--datastore=<vm_datastore>
--powerOn
<nbva_ova>
vi://<vCenter_username>:<vCenter_password>/?ip=<hostIPAddress>
```

For the combined primary and media server, Veritas provides the automatic initial configuration option. By using a product file that supports this option, the deployment wizard passes in the appliance network and storage configuration as OVF properties during the deployment process. When the deployment is complete, the appliance network and storage are configured based on these values. If you use the OVF tool to deploy this product file, you need to specify the desired properties for appliance initial configuration.

For example, the following is a list of the OVF properties for appliance network configuration:

```
--prop:va.hostname=<nbva_hostname>
--prop:va.ip=<nbva_ip>
--prop:va.netmask=<nbva_netmask>
--prop:va.gateway=<nbva_gateway>
--prop:va.dns1=<nbva_dns1>
--prop:va.dns2=<nbva_dns2>
--prop:va.ipv6Address=<nbva_ipv6addr>
--prop:va.ipv6PrefixLength=<nbva_ipv6Prefix>
--prop:va.ipv6Gateway=<nbva_ipv6Gateway>
--prop:va.dnsDomain=<nbva_domain>
```

NetBackup Virtual Appliance deployment guidelines

Use the following configuration guidelines when you deploy a new NetBackup Virtual Appliance:

Table 2-4 Appliance deployment guidelines

Parameter	Description
Deployment requirements	To deploy a NetBackup Virtual Appliance, you need a VMware vCenter Server user account and access to the VSphere Client or vSphere Web Client. The appliance supports vSphere versions 6.5, 6.7, 7.0, and 7U1. Your vCenter Server account must have at least the minimum privileges required to deploy an OVF template. For how to deploy an OVF package directly on an ESXi host, see the following technical article. https://www.veritas.com/support/en_US/article.100038949 Refer to the VMware documentation for more information.
Connectivity during deployment	When you perform the appliance deployment, Veritas recommends that you take precautions to avoid loss of connectivity. Any loss of connectivity during deployment results in failure. The computer that you use to deploy the appliance should be set up to avoid the following events: ■ Conditions that cause the computer to go to sleep ■ Conditions that cause the computer to shut down or to lose power ■ Conditions that cause the computer to lose its network connection
Environment requirements	Depending on the product file (OVF template) you use, the appliance can use one of the following CPU and memory combination. ■ 16 GB of memory and 8 virtual CPUs (vCPUs) ■ 8 GB of memory and 4 vCPUs ■ 64 GB of memory and 32 vCPUs See “NetBackup Virtual Appliance product files (OVF templates)” on page 29. Make sure that both the CPU and memory requirements are met before you deploy the appliance.

Table 2-4 Appliance deployment guidelines (*continued*)

Parameter	Description
Performance	Veritas recommends that you adhere to the following best practices: ■ Do not overcommit the vCPUs on the ESX host. The number of vCPUs that are assigned to all virtual machines on the host should be equal to or less than the number of cores on that host. ■ Set a memory reservation to provide the appliance with full utilization of the available memory. ■ Do not overcommit the memory on the ESX host. The amount of memory that is assigned to all virtual machines on the host should be equal to or less than the amount of memory on that host. ■ Use thick provisioning for the appliance virtual disks. ■ The NetBackup Virtual Appliance has a heavy I/O workload, so it should be isolated from shared storage as much as possible. At a minimum, make sure that the appliance uses a different datastore than other virtual machines with a heavy I/O workload. ■ NetBackup Virtual Appliance supports hyper-threading and usually performs better when hyper-threading is enabled. VMware vSphere recommends that you enable hyper-threading as a performance best practice. VMware vSphere 6.5 and later enable hyper-threading by default to increase hypervisor performance. Note that hyper-threading performance improvements are highly application-dependent, and some applications might see performance degradation. Additionally, there are various microprocessor flaws that may introduce security vulnerabilities when hyper-threading is enabled. Consult your hardware vendor documentation to learn about hyper-threading and possible security vulnerabilities.
Required names and addresses	Before the initial deployment, gather the following information: ■ Data center and storage details ■ Appliance host name and IP address ■ Netmask and Gateway IP address ■ DNS information ■ Names for AdvancedDisk and MSDP disk pools and storage units Note: You do not need to provide the storage details for a primary server appliance. ■ New passwords for the admin and maintenance accounts New password for the nbsecadmin account (primary server and combined primary and media server only) Note: You cannot access the NetBackup web UI until you have changed the nbsecadmin user password. The default password for all default accounts is P@ssw0rd. See “NetBackup Virtual Appliance initial deployment checklist” on page 37.

Table 2-4 Appliance deployment guidelines (*continued*)

Parameter	Description
Licenses	The appliance comes with a not for resale (NFR) license key that expires after a specific period of time. The appliance does not provide a warning message that this license key is about to expire. Therefore, Veritas recommends that you change this key to a permanent key after you deploy the appliance. Make sure that you replace the NFR key with a permanent key before it expires. Warning: If the correct license key is not installed, the appliance services stop functioning after the evaluation key expires. Make sure that the NetBackup license you add includes support for NetBackup Virtual Appliance.

Review the initial deployment checklist and make sure that you have all of the necessary information to complete the deployment procedure.

See [“NetBackup Virtual Appliance initial deployment checklist”](#) on page 37.

Configuration overview for NetBackup Virtual Appliance MSDP cloud applications

Starting with release 3.3.0.1, you can configure the NetBackup Virtual Appliance media server or the NetBackup Virtual Appliance combined primary and media server for MSDP cloud applications.

MSDP cloud is a cloud solution with deduplication technology. Data is stored directly to cloud targets with deduplication. One MSDP storage server can support both local storage and multiple cloud storage targets. After you have configured the appliance MSDP storage server (during the initial configuration), you can add a cloud storage target to that storage server. Then, the appliance MSDP storage server can store data to the cloud target.

MSDP cloud storage requires 60 GB of storage for the local cache, which comes out of your MSDP storage allocation. 50 GB is used for the storage data, and 10 GB is used for the metadata.

If you need to expand the cache, first verify that there is enough unused space in the MSDP storage and add additional disks if needed. Then, adjust the **CloudDataCacheSize** and the **CloudMetaCacheSize** parameters in the `contentrouter.cfg` file. See the NetBackup Deduplication Guide for more information.

The following describes a summary of the required steps to configure an appliance for MSDP cloud applications:

- Step 1: Perform the initial configuration on the appliance using the NetBackup Virtual Appliance Shell Menu (shell menu).
- Step 2: Log in to the NetBackup web UI as the **nbaseadmin** user and configure the MSDP cloud storage as follows:
 - Create a disk pool.
 - Create a storage unit.
 For details, see the *NetBackup Web UI Administrator's Guide*.

Note: Once the appliance initial configuration has been completed, you can configure MSDP cloud storage anytime later.

NetBackup Virtual Appliance initial deployment checklist

This checklist is intended to help you plan for the initial configuration of your appliance. Use the checklist together with the initial deployment procedure.

For a new appliance, use the following tables to record the initial deployment settings for the appliance. When using a printed version of this checklist, make sure to place the completed checklist in a secure location.

Data center details

Table 2-5 Data center details

Parameter	Setting
Appliance name	
Data center name	
ESX/ESXi host name	
Destination datastore	

Network configuration

Table 2-6 Network configuration

Parameter	Setting
Appliance host name (Veritas recommends FQDN)	
DNS domain name	

Table 2-6 Network configuration (*continued*)

Parameter	Setting
Appliance IPv4 address	
(Optional) Appliance IPv6 address	
(Optional) Appliance IPv6 prefix length	
Netmask	
Gateway IPv4 address	
(Optional) Gateway IPv6 address	
Primary DNS server IPv4 address	
(Optional) Additional DNS server IPv4	
(Optional) Additional DNS server IPv6	

Primary server and NTP

Table 2-7 Primary server and NTP

Parameter	Setting
Primary server name (required if it is a media server)	
(Optional) NTP	

Storage configuration

You do not need to provide the storage details for a primary server appliance.

Table 2-8 Storage configuration

Parameter	Setting
AdvancedDisk disk pool name	
AdvancedDisk storage unit name	
AdvancedDisk storage size (media server only)	
MSDP disk pool name	
MSDP storage unit name	

Table 2-8 Storage configuration (*continued*)

Parameter	Setting
MSDP storage size (media server only)	

Password change

Table 2-9 Password change

Parameter	Setting
New <code>admin</code> password	
New <code>maintenance</code> password	
New <code>nbasecadmin</code> password (primary server and combined primary and media server only)	

See [“NetBackup Virtual Appliance deployment guidelines”](#) on page 34.

Deploying and configuring the appliance

This chapter includes the following topics:

- [How to deploy and configure a NetBackup Virtual Appliance combined primary and media server](#)
- [How to deploy and configure a NetBackup Virtual Appliance media server](#)
- [How to deploy and configure a NetBackup Virtual Appliance primary server](#)

How to deploy and configure a NetBackup Virtual Appliance combined primary and media server

Use this process to deploy and configure a NetBackup Virtual Appliance combined primary and media server.

Table 3-1 How to deploy the NetBackup Virtual Appliance combined primary and media server

Step	Task
Step 1	Review the available product files (OVF templates) for deployment. See “NetBackup Virtual Appliance product files (OVF templates)” on page 29.
Step 2	Download the desired NetBackup Virtual Appliance product file from the Download Center on the Veritas Support website.
Step 3	Review the deployment guidelines and prepare the checklist. See “NetBackup Virtual Appliance deployment guidelines” on page 34.

Table 3-1 How to deploy the NetBackup Virtual Appliance combined primary and media server *(continued)*

Step	Task
Step 4	Deploy the NetBackup Virtual Appliance combined primary and media server. See “Using the vSphere Client to deploy a combined primary and media server appliance” on page 41. See “Using the OVF Tool to deploy a combined primary and media server appliance” on page 46.
Step 5	Configure the appliance from the NetBackup Virtual Appliance Shell Menu. If you use a product file that supports automatic initial configuration, you only need to complete the remaining step of the initial configuration. See “Performing the initial configuration on a NetBackup Virtual Appliance combined primary and media server” on page 48. See “Completing the initial configuration of the NetBackup Virtual Appliance combined primary and media server” on page 53.

Using the vSphere Client to deploy a combined primary and media server appliance

The section describes how to deploy and configure a NetBackup Virtual Appliance combined primary and media server. This server role is for deployment in remote offices and branch offices.

To ensure a successful deployment, make sure that you meet all of the deployment guidelines before you begin these procedures.

See [“NetBackup Virtual Appliance deployment guidelines”](#) on page 34.

For how to deploy an OVF package directly on an ESXi host, use the following technical article.

https://www.veritas.com/support/en_US/article.100038949

Note: The following procedure is based on the VMware vSphere Client. It also applies to the browser-based VMware vSphere Web Client. Note that the order of the steps are slightly different with the web client.

To deploy a combined primary and media server appliance using the VMware vSphere Client

- 1 Using the VMware vSphere Client, log on to the vCenter Server where you want to deploy your appliance.

Note: Your vCenter Server user account must have at least the minimum privileges required to deploy an OVF template. Refer to the VMware documentation for more information.

- 2 Select **File > Deploy OVF Template** to start the deployment wizard.
- 3 On the **Source** page of the deployment wizard, click **Browse** to navigate to the NetBackup Virtual Appliance product file. If you split the file when you downloaded it, make sure that all of the pieces are saved in the same folder and navigate to that folder.

Verify the path and click **Next**.

- 4 Review the **OVF Template Details** page and click **Next**.
- 5 On the **End User License Agreement** page, read through the EULA and click **Accept**, and then **Next**.
- 6 Enter the destination details as follows:
 - **Name:** Enter a unique name for your appliance.
 - **Inventory Location:** Select the folder or the data center where you want the appliance to be located. The options are autopopulated based on what is available to that vCenter Server.

Click **Next**.

- 7 Select the resource location where you want the deployed template to run.
Click **Next**.
- 8 Select the destination storage where you want to store the appliance files.
Click **Next**.

Caution: If you select a storage cluster, make sure that one of the datastores in the cluster has enough storage space for the entire appliance. If none of the individual datastores in the cluster has enough space, the deployment fails.

- 9 Select **Thick Provision Lazy Zeroed** as the provisioning format for the appliance disks, and make sure that the **Disk Mode** is set to **Independent - Persistent** for all disks other than the OS disk. For more information on provisioning or the disk mode, refer to the VMware documentation.

Click **Next**.

- 10 Select the destination networks to map the networks used in the OVF template.

Click **Next**.

- 11 Depending on the virtual appliance product file you use, choose the following to proceed:

- If the virtual appliance product file supports deployment properties, continue to Step 12.

In the following steps the deployment wizard guides you to provide the deployment properties for the automatic initial configuration of the appliance. The automatic initial configuration happens immediately after the deployment is complete.

- If the virtual appliance product file does not support deployment properties, you are ready to complete the deployment.

Do the following:

- Read through and verify the deployment options that you entered. If everything is correct, click **Finish** to start the deployment.
The amount of time that it takes for the deployment process to complete varies depending on your network connection. The process can take up to 30 minutes to complete.
- After the deployment is complete, proceed to perform the initial configuration steps in the following topic.
[See "Performing the initial configuration on a NetBackup Virtual Appliance combined primary and media server" on page 48.](#)

- 12 On the **Properties** page, fill in the following information:

- Network configuration:

- **Host name**

Enter a short host name or a fully qualified domain name (FQDN) for this appliance. The host name can contain up to 256 characters, any letters, numbers, and the following special characters: . - _ . Do not start a name with a special character.

As a best practice, Veritas recommends that you use an FQDN.

Caution: After the initial deployment has completed successfully, the only way to change the host name is to redeploy the appliance.

Note: If you plan to configure Active Directory (AD) authentication on this appliance, the host name must be 15 characters or less. Otherwise, AD configuration can fail.

- **DNS domain name**
Enter a DNS domain name for this appliance.
- **IP address**
Enter the IPv4 address to be used for this appliance.
- **Netmask**
Enter the netmask that corresponds to the IP address.
- **Gateway**
Enter the IPv4 address of the gateway (network point) that acts as an entrance to another network.
- **DNS server**
Enter the IPv4 address of the primary DNS server for this appliance.
- **DNS server (optional)**
Enter the IPv4 address of the secondary DNS server for this appliance.
- **Host name resolution**
The host name must be resolvable with a DNS server or a HOSTS file for the automatic initial configuration to be successful. If DNS is not available during the deployment, use the HOSTS file to resolve the host name.
Select the checkbox to add the host name and IP address to the HOSTS file.
- IPv6 Network Configuration (optional)
 - **IPv6 address**
Enter the IPv6 address for this appliance.
 - **IPv6 prefix length**
Enter the IPv6 prefix length for this appliance.
 - **IPv6 gateway**
Enter the IPv6 gateway for this appliance.
- Usage Insights customer registration key
To obtain a key, follow the onscreen prompts.

- Storage configuration:

Note: The NetBackup disk pool and storage unit names can contain up to 256 characters. The names can contain any letters, numbers, and the following special characters: + . - _ . Do not start a name with the minus (-) character.

- **AdvancedDisk disk pool name**
Enter a name for the AdvancedDisk disk pool on the appliance.
- **AdvancedDisk storage unit name**
Enter a name for the AdvancedDisk storage unit on the appliance.
- **MSDP disk pool name**
Enter a name for the MSDP disk pool on the appliance.
- **MSDP storage unit name**
Enter a name for the MSDP storage unit on the appliance.

13 When you have filled in all of the required information, click **Next**.

14 Read through and verify the deployment properties that you entered. If everything is correct, click **Finish** to deploy the appliance.

The amount of time that it takes for the deployment process to complete varies depending on your network connection. If you have selected to power on the appliance after the deployment, NetBackup Virtual Appliance boots up and configures the network, the role, and the storage. This configuration process can take up to 30 minutes to complete.

15 Once the deployment process is complete, proceed to the remaining configuration steps in the following procedure.

See [“Completing the initial configuration of the NetBackup Virtual Appliance combined primary and media server”](#) on page 53.

After the appliance is configured and operational, you are ready to install NetBackup client software on the computers that you want to back up.

See the *NetBackup Installation Guide* for how to install NetBackup clients.

See [“Common tasks in NetBackup Virtual Appliance”](#) on page 86.

See [“About modifying the NetBackup Virtual Appliance settings”](#) on page 81.

Using the OVF Tool to deploy a combined primary and media server appliance

The section describes how to deploy and configure a NetBackup Virtual Appliance combined primary and media server. This server role is for deployment in remote offices and branch offices.

To ensure a successful deployment, make sure that you meet all of the deployment guidelines before you begin these procedures.

See [“NetBackup Virtual Appliance deployment guidelines”](#) on page 34.

Note: This procedure requires a vCenter Server. For how to deploy an OVF package directly on an ESXi host, see the following technical article.

https://www.veritas.com/support/en_US/article.100038949

To deploy a combined primary and media server appliance using the VMware OVF Tool

- 1 Log on to the vCenter Server where you want to deploy your appliance.

Note: Your vCenter Server user account must have at least the minimum privileges required to deploy an OVF template. Refer to the VMware documentation for more information.

- 2 Use the VMware OVF Tool to deploy the OVF package.

OVF descriptors can contain configuration properties for the deployed OVF package. The `--prop` option is used to set a property. The appliance uses the configuration properties for the automatic initial configuration. Replace the variables with the environment information you gathered, and use a blank to separate the options and property mappings.

Choose one of the following to proceed according to the product file you use.

- If the product file supports configuration properties, run the following command:

```
ovftool
--name=<nbva_name>
--acceptAllEulas
--net:"VM Network=<vm_network>"
--allowAllExtraConfig
--datastore=<vm_datastore>
--prop:va.hostname=<nbva_hostname>
```

```

--prop:va.ip=<nbva_ip>
--prop:va.netmask=<nbva_netmask>
--prop:va.gateway=<nbva_gateway>
--prop:va.dns1=<nbva_dns1>
--prop:va.dns2=<nbva_dns2>
--prop:va.ipv6Address=<nbva_ipv6addr>
--prop:va.ipv6PrefixLength=<nbva_ipv6Prefix>
--prop:va.ipv6Gateway=<nbva_ipv6Gateway>
--prop:va.dnsDomain=<nbva_domain>
--prop:va.addhosts=true|false
--prop:va.smartmeterText='<copy_entire_key_file_content_here>'
--prop:va.adPoolName=<ad_name>
--prop:va.adStuName=<ad_stu_name>
--prop:va.msdpPoolName=<msdp_name>
--prop:va.msdpStuName=<msdp_stu_name>
--powerOn
<nbva_ova>
vi://<vCenter_username>:<vCenter_password>/?ip=<hostIPAddress>

```

Once the deployment and the automatic configuration are complete, proceed to the remaining configuration steps in the following procedure.

See [“Completing the initial configuration of the NetBackup Virtual Appliance combined primary and media server”](#) on page 53.

- If the product file does not support configuration properties, you must deploy the virtual appliance first.

Run the following OVF tool command to deploy the virtual appliance:

```

ovftool
--name=<nbva_name>
--acceptAllEulas
--net:"VM Network=<vm_network>"
--allowAllExtraConfig
--datastore=<vm_datastore>
--powerOn
<nbva_ova>
vi://<vCenter_username>:<vCenter_password>/?ip=<hostIPAddress>

```

Once the deployment is complete, proceed to perform the initial configuration steps in the following topic.

See [“Performing the initial configuration on a NetBackup Virtual Appliance combined primary and media server”](#) on page 48.

Performing the initial configuration on a NetBackup Virtual Appliance combined primary and media server

This section describes how to perform the initial configuration on a NetBackup Virtual Appliance with the combined primary and media server role.

You do not need this procedure if the product file supports automatic initial configuration after the deployment.

To perform the initial configuration on a NetBackup Virtual Appliance with the combined primary and media server role

- 1 After you have deployed a new virtual appliance, log on to the NetBackup Virtual Appliance Shell Menu.

The logon is `admin`, and the default password is `P@ssw0rd`.

- 2 Use the following command to start the initial configuration:

```
Main > Appliance > Configure
```

A message about the **Virtual Appliance Initial Configuration Wizard** appears. This wizard will walk you through the process to configure this appliance.

- 3 The wizard prompts you to change the default passwords.

Change each user account password as prompted.

Review the following password policy before setting a new password:

- Passwords must contain at least eight characters.
- Passwords must contain at least one lowercase letter (a-z) and one number (0-9).
- Dictionary words are considered weak passwords and are not accepted.
- The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.

Note: If you enter five consecutive invalid passwords for any user account, the appliance aborts the initial configuration process automatically. You must start the initial configuration process again.

Note: If you enable the STIG feature after completing the initial configuration, you may be prompted to change the new passwords you entered here to meet the requirements of the STIG password policy.

- 4 The wizard takes you to the network configuration.

Specify the following:

- **Hostname**

Enter a short host name or a fully qualified domain name (FQDN) for this appliance. As a best practice, Veritas recommends that you use an FQDN.

Caution: After the initial deployment has completed successfully, the only way to change the host name is to redeploy the appliance.

Note: If you plan to configure Active Directory (AD) authentication on this appliance, the host name must be 15 characters or less. Otherwise, AD configuration can fail.

- **DNS domain name**

Enter a DNS domain name for this appliance.

- **IPv4 address**

Enter the IPv4 address to be used for this appliance.

- **Netmask**

Enter the netmask that corresponds to the IP address.

- **Gateway IP address**

Enter the IPv4 address of the gateway (network point) that acts as an entrance to another network.

- **DNS server 1 IP address**

Enter the IPv4 address of the primary DNS server for this appliance.

- **DNS server 2 IP address(Optional)**

Enter the IPv4 address of the secondary DNS server for this appliance.

When you are prompted with the following message, choose whether you want to add the host name and IP address to the HOSTS file.

```
The host name must be resolvable with a DNS or a HOSTS file for
the initial configuration to be successful. Do you want to write
the host name resolution information to the HOSTS file? [yes,
no] (no)
```

Note: The host name must be resolvable with a DNS server or a HOSTS file for the initial configuration to be successful. If DNS is not available, you can add the host name and IP address to the HOSTS file.

- 5 After the network configuration is completed, the wizard takes you to the next step for the Veritas Usage Insights customer registration key. You cannot complete the configuration until you provide the registration key. To obtain a key, follow the onscreen prompts.
- 6 Once the file is uploaded, the wizard takes you to final step for storage configuration.

Specify the following:

- **AdvancedDisk disk pool name**
Enter a name for the AdvancedDisk disk pool on the appliance.
- **AdvancedDisk storage unit name**
Enter a name for the AdvancedDisk storage unit on the appliance.
- **MSDP storage unit name**
Enter a name for the MSDP storage unit on the appliance.
- **MSDP disk pool name**
Enter a name for the MSDP disk pool on the appliance.

The storage configuration may take several minutes.

- 7 Use the following command to verify that the automatic configuration completed successfully:

```
Main > Appliance > Status
```

The command output should contain a message similar to the following:

```
Appliance Version is 4.1.
```

```
Appliance is configured as primary appliance.
```

If the output does not show that the appliance is configured as a primary appliance, you need to redeploy the appliance or perform other troubleshooting steps to fix the issue before you proceed to the next step. See [“Troubleshooting NetBackup Virtual Appliance initial deployment issues”](#) on page 308.

- 8 Use the following command to change the **nbasecadmin** account password from the known default password (**P@ssw0rd**):

```
Main > Settings > Password nbasecadmin
```

Note: You cannot access the NetBackup web UI until you have changed the **nbasecadmin** user password.

- 9 Use the following command to set the time zone:

```
Main > Network > TimeZone Set
```

Select the appropriate time zone from the displayed list.

- 10 Use the following command to add a Network Time Protocol (NTP) server:

```
Main > Network > NTPServer Add <Server>
```

Where <Server> is the name of the NTPServer.

- 11 Add a permanent license key before the evaluation key expires with the following command:

```
Main > Manage > License > Add
```

You can locate your permanent license key from the Veritas Entitlement Management System (VEMS). To access VEMS, click **Licensing** on the [Veritas Support website](#).

Warning: If the correct license key is not installed, the appliance services stop functioning after the evaluation key expires. Make sure that the NetBackup license you add includes support for NetBackup Virtual Appliance.

See [“Managing license keys on the NetBackup Virtual Appliance”](#) on page 84.

- 12 (Optional)

If you want to configure an IPv6 address for the appliance, run the following command:

```
Main > Network > IPv6 <IPAddress> <Prefix> InterfaceName
```

Where <IPAddress> is the IPv6 address and <Prefix> is the prefix length.

See [“About IPv4-IPv6-based network support”](#) on page 120.

- 13 (Optional)

If you want to configure an IPv6 DNS server on the appliance, run the following command:

```
Main > Network > DNS Add NameServer <IPAddress>
```

Where <IPAddress> is the IPv6 address of the additional DNS server. Only global-scope and unique-local IPv6 addresses are allowed.

See [“Configuring DNS and host name mapping for the NetBackup Virtual Appliance”](#) on page 122.

14 (Optional)

If you want to use an external Certificate Authority (CA) for communication between the appliance and your other NetBackup hosts, run the following command:

```
Main > Settings > NetBackup CertificateUsage Enable ECA
```

15 (Optional)

If you plan to connect this combined primary and media server to another media server in a NAT network, perform the following tasks:

- Enable the NetBackup DNAT feature on this combined primary and media server as follows:

```
Main > Settings > NetBackup DNAT Enable
```

- Add the name of the other media server to the NetBackup Servers list on this combined primary and media server as follows:

```
Main > Settings > NetBackup NATServers Add
```

16 (Optional)

If you deployed a product file with an initial storage capacity of .5 TB and want to add storage up to a total of 16 TB, use the following steps to add additional disks:

- Use the VMware vSphere Client to create new virtual disks with sizes that are multiples of 0.5 TB, or 512 GB.
- From the NetBackup Virtual Appliance Shell Menu, run the following command:

```
Main > Manage > Storage > Scan
```

This command refreshes the storage disks and device information to locate available disks.

- Run the following command:

```
Main > Manage > Storage > Add
```

This command launches a wizard that displays the available disks. Follow the prompts to add the disks. To add multiple disks at one time, use a comma-separated list.

See [“Adding storage space for the NetBackup Virtual Appliance”](#) on page 105.

- 17 Log on to the appliance from the NetBackup Administration Console and activate the NetBackup catalog backup policy.

By default, the appliance creates an inactive backup policy that uses a Storage Lifecycle Policy (SLP) to protect the NetBackup catalog. The SLP backs up the data to AdvancedDisk and then duplicates it to MSDP. You are then able to use Auto Image Replication to save your catalog backup off site. Veritas recommends that you use this replication-based strategy for disaster recovery (DR) due to the combined primary and media server role of the appliance.

To activate the policy, navigate to the **NetBackup Management > Policies** tab in the Administration Console, right-click on the `nbu-catalog` policy, and select **Activate**.

Note: You must set a encryption passphrase for the disaster recovery package for the catalog to be successful. Catalog backups continue to fail until the passphrase is set.

For more information about the security requirements for disaster recovery , see the *NetBackup Security and Encryption Guide*.

If you plan to use AdvancedDisk to back up your clients, note that the AdvancedDisk does not support Auto Image Replication. If you want to save the data off site, create an SLP to duplicate the backup data on AdvancedDisk to MSDP. You are then able to use Auto Image Replication to transfer the data off site.

- 18 If you want to configure the appliance for MSDP cloud, log in to the NetBackup web UI as the **nbasecadmin** user and configure the MSDP cloud storage as follows:

- Create a disk pool.
- Create a storage unit.

For details, see the *NetBackup Web UI Administrator's Guide*.

After the appliance is configured and operational, you are ready to install NetBackup client software on the computers that you want to back up.

See the *NetBackup Installation Guide* for how to install NetBackup clients.

Completing the initial configuration of the NetBackup Virtual Appliance combined primary and media server

This section describes the remaining configuration steps after the automatic initial configuration is complete.

Note: Use this procedure to complete the initial configuration only when the product file you use supports automatic initial configuration.

To complete the initial configuration of a NetBackup Virtual Appliance

- 1 After you have deployed a new virtual appliance, open a console session from the VMware vSphere Client to log on to the NetBackup Virtual Appliance Shell Menu.

The logon is `admin`, and the default password is `P@ssw0rd`.

Note: You cannot log in to the shell until the automatic initial configuration is complete. Wait for about 20-30 minutes after deployment before you attempt to log in.

- 2 The first time you log in, you are prompted to change the default passwords. Change each user account password as prompted.

Review the following password policy before setting a new password:

- Passwords must contain at least eight characters.
- Passwords must contain at least one lowercase letter (a-z) and one number (0-9).
- Dictionary words are considered weak passwords and are not accepted.
- The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.

Note: If you enter five consecutive invalid passwords for any user account, the appliance aborts the shell session. You must log back in and try again.

Note: If you enable the STIG feature after completing the initial configuration, you may be prompted to change the new passwords you entered here to meet the requirements of the STIG password policy.

- 3 Use the following command to verify that the automatic configuration completed successfully:

```
Main > Appliance > Status
```

The command output should contain a message similar to the following:

```
Appliance Version is 4.1.
```

```
Appliance is configured as primary appliance.
```

If the output does not show that the appliance is configured as a primary appliance, you need to redeploy the appliance or perform other troubleshooting steps to fix the issue before you proceed to the next step. See [“Troubleshooting NetBackup Virtual Appliance initial deployment issues”](#) on page 308.

- 4 Use the following command to change the **nbasecadmin** account password from the known default password (**P@ssw0rd**):

```
Main > Settings > Password nbasecadmin
```

Note: You cannot access the NetBackup web UI until you have changed the **nbasecadmin** user password.

- 5 Use the following command to set the time zone:

```
Main > Network > TimeZone Set
```

Select the appropriate time zone from the displayed list.

- 6 Use the following command to add a Network Time Protocol (NTP) server:

```
Main > Network > NTPServer Add <Server>
```

Where **<Server>** is the name of the NTPServer.

- 7 Add a permanent license key before the evaluation key expires with the following command:

```
Main > Manage > License > Add
```

You can locate your permanent license key from the Veritas Entitlement Management System (VEMS). To access VEMS, click **Licensing** on the [Veritas Support website](#).

Warning: If the correct license key is not installed, the appliance services stop functioning after the evaluation key expires. Make sure that the NetBackup license you add includes support for NetBackup Virtual Appliance.

See [“Managing license keys on the NetBackup Virtual Appliance”](#) on page 84.

- 8 (Optional)

If you want to use an external Certificate Authority (CA) for communication between the appliance and your other NetBackup hosts, run the following command:

```
Main > Settings > NetBackup CertificateUsage Enable ECA
```

- 9 (Optional)

If you plan to connect this combined primary and media server to another media server in a NAT network, perform the following tasks:

- Enable the NetBackup DNAT feature on this combined primary and media server as follows:

```
Main > Settings > NetBackup DNAT Enable
```

- Add the name of the other media server to the NetBackup Servers list on this combined primary and media server as follows:

```
Main > Settings > NetBackup NATServers Add
```

- 10 (Optional)

If you deployed a product file with an initial storage capacity of .5 TB and want to add storage up to a total of 16 TB, use the following steps to add additional disks:

- Use the VMware vSphere Client to create new virtual disks with sizes that are multiples of 0.5 TB, or 512 GB.
- From the NetBackup Virtual Appliance Shell Menu, run the following command:

```
Main > Manage > Storage > Scan
```


This command refreshes the storage disks and device information to locate available disks.

- Run the following command:

```
Main > Manage > Storage > Add
```

This command launches a wizard that displays the available disks. Follow the prompts to add the disks. To add multiple disks at one time, use a comma-separated list.

See [“Adding storage space for the NetBackup Virtual Appliance”](#) on page 105.

- 11 Log on to the appliance from the NetBackup Administration Console and activate the NetBackup catalog backup policy.

By default, the appliance creates an inactive backup policy that uses a Storage Lifecycle Policy (SLP) to protect the NetBackup catalog. The SLP backs up the data to AdvancedDisk and then duplicates it to MSDP. You are then able to use Auto Image Replication to save your catalog backup off site. Veritas recommends that you use this replication-based strategy for disaster recovery (DR) due to the combined primary and media server role of the appliance.

To activate the policy, navigate to the **NetBackup Management > Policies** tab in the Administration Console, right-click on the `nbu-catalog` policy, and select **Activate**.

Note: You must set an encryption passphrase for the disaster recovery package for the catalog to be successful. Catalog backups continue to fail until the passphrase is set.

For more information about the security requirements for disaster recovery, see the *NetBackup Security and Encryption Guide*.

If you plan to use AdvancdDisk to back up your clients, note that the AdvancedDisk does not support Auto Image Replication. If you want to save the data off site, create an SLP to duplicate the backup data on AdvancedDisk to MSDP. You are then able to use Auto Image Replication to transfer the data off site.

- 12 If you want to configure the appliance for MSDP cloud, log in to the NetBackup web UI as the **nbasecadmin** user and configure the MSDP cloud storage as follows:

- Create a disk pool.
- Create a storage unit.

For details, see the *NetBackup Web UI Administrator's Guide*.

How to deploy and configure a NetBackup Virtual Appliance media server

Use this process to deploy and configure a NetBackup Virtual Appliance media server.

Table 3-2 Before you deploy the NetBackup Virtual Appliance combined primary and media server

Step	Task
Step 1	Review the available product files (OVF templates) for deployment. See “NetBackup Virtual Appliance product files (OVF templates)” on page 29.
Step 2	Download the NetBackup Virtual Appliance product file from the Download Center on the Veritas Support website.
Step 3	Review the deployment guidelines and prepare the checklist. See “NetBackup Virtual Appliance deployment guidelines” on page 34.

Table 3-3 Deployment and initial configuration

Step	Task
Step 4	Add the appliance media server name to the primary server. You must know the proposed host name of the appliance. The same name is used in the NetBackup Virtual Appliance Shell Menu during the initial configuration wizard. See “Configuring a primary server to communicate with an appliance media server” on page 62.
Step 5	Deploy the NetBackup Virtual Appliance media server. See “Using the vSphere Client to deploy a media server appliance” on page 59. See “Using the OVF Tool to deploy a media server appliance” on page 60.
Step 6	Configure the appliance from the NetBackup Virtual Appliance Shell Menu. See “Performing the initial configuration on a NetBackup Virtual Appliance media server” on page 64.

Using the vSphere Client to deploy a media server appliance

The section describes how to deploy a NetBackup Virtual Appliance with the media server role. This server role is for deployment in data centers.

To ensure a successful deployment, make sure that you meet all of the deployment guidelines before you begin these procedures.

See [“NetBackup Virtual Appliance deployment guidelines”](#) on page 34.

Note: The following procedure is based on the VMware vSphere Client. It also applies to the browser-based VMware vSphere Web Client. Note that the order of the steps are slightly different with the web client.

To deploy a media server appliance from the VMware vSphere Client

- 1 Using the VMware vSphere Client, log on to the vCenter Server where you want to deploy your appliance.

Note: Your vCenter Server user account must have at least the minimum privileges required to deploy an OVF template. Refer to the VMware documentation for more information.

- 2 Select **File > Deploy OVF Template** to start the deployment wizard.
- 3 On the **Source** page of the deployment wizard, click **Browse** to navigate to the NetBackup Virtual Appliance product file. If you split the file when you downloaded it, make sure that all of the pieces are saved in the same folder and navigate to that folder.

Verify the path and click **Next**.
- 4 Review the **OVF Template Details** page and click **Next**.
- 5 On the **End User License Agreement** page, read through the EULA and click **Accept** and then **Next**.
- 6 Read through and verify the deployment options that you entered. If everything is correct, click **Finish** to deploy the appliance.

The amount of time that it takes for the deployment process to complete varies depending on your network connection. This configuration process can take up to 30 minutes to complete.

- 7 A newly deployed virtual appliance with the media role does not contain virtual disks for appliance storage. Once the deployment is complete, use the VMware vSphere Client to add virtual disks to the virtual machine configuration.

When you add the disks, select **Thick Provision Lazy Zeroed** as the provisioning format, and make sure that the **Disk Mode** is set to **Independent - Persistent** for all disks other than the OS disk. For more information on provisioning or the disk mode, refer to the VMware documentation.

Note: Veritas recommends that you create virtual disks with sizes that are multiples of 512 GB, or 0.5 TB for the appliance to use as storage disks.

- 8 After you have added one or more virtual disks for use as appliance storage disks, proceed to perform the initial configuration steps in the following topic.

See [“Performing the initial configuration on a NetBackup Virtual Appliance media server”](#) on page 64.

See [“Common tasks in NetBackup Virtual Appliance”](#) on page 86.

See [“About modifying the NetBackup Virtual Appliance settings”](#) on page 81.

Using the OVF Tool to deploy a media server appliance

The section describes how to deploy a NetBackup Virtual Appliance with the media server role. This server role is for deployment in data centers.

To ensure a successful deployment, make sure that you meet all of the deployment guidelines before you begin these procedures.

See [“NetBackup Virtual Appliance deployment guidelines”](#) on page 34.

Note: This procedure requires a vCenter Server. For how to deploy an OVF package directly on an ESXi host, see the following technical article.

https://www.veritas.com/support/en_US/article.100038949

To deploy a media server appliance using the VMware OVF Tool

- 1 Log on to the vCenter Server where you want to deploy your appliance.

Note: Your vCenter Server user account must have at least the minimum privileges required to deploy an OVF template. Refer to the VMware documentation for more information.

- 2 Use the VMware OVF Tool to run the following command, substituting the environment information that you gathered for the parameters that are marked with angular brackets (<>) and in italics:

```
ovftool
--name=<nbva_name>
--acceptAllEulas
--net:"VM Network=<vm_network>"
--allowAllExtraConfig
--datastore=<vm_datastore>
--powerOn
<nbva_ova>
vi://<vCenter_username>:<vCenter_password>/?ip=<hostIPAddress>
```

For more information about the OVF Tool, refer to the [VMware OVF Tool documentation](#).

- 3 A newly deployed virtual appliance with the media role does not contain virtual disks for appliance storage. Once the deployment is complete, create new virtual disks to the virtual machine configuration. You can create a new virtual disk from the VMware vSphere Client.

Note: Veritas recommends that you create virtual disks with sizes that are multiples of 512 GB, or 0.5 TB for the appliance to use as storage disks.

- 4 After you have added disks to the appliance from the VMware vSphere (Web) Client, proceed to perform the initial configuration steps in the following topic. See [“Performing the initial configuration on a NetBackup Virtual Appliance media server”](#) on page 64.

Configuring a primary server to communicate with an appliance media server

Before you configure a new appliance for the **Media** server role, you must first update the configuration on the primary server that you plan to use with it. To ensure communication between the primary server and the new media server, the new media server host name must be added to the **Additional Servers List** on the primary server.

The following procedure describes how to configure a primary server to communicate with a new appliance media server.

To configure a primary server to communicate with a new media server

- 1 Before the appliance is configured for the media server role, verify that the software version is compatible with the primary server. The primary server must use the same or a later software version than the media server as follows:

- 2 For an appliance primary server:

From the NetBackup Virtual Appliance Shell Menu:

- From the **Main_Menu > Settings** view, run the following command:

```
Settings > NetBackup AdditionalServers
Add media-server
```

Where *media-server* is the fully qualified host name (FQHN) of the appliance media server that is not yet configured.

If the appliance has more than one host name, you must add all of the names.

For a traditional NetBackup primary server:

- Log on to the NetBackup Administration Console as the administrator.
- On the main console window, in the left pane, click **NetBackup Management > Host Properties > Primary Servers**.
- In the right pane, click on the primary server host name.
- On the **Host Properties** window, in the left pane, click **Servers**.
- In the right pane, in the **Additional Servers** section, click **Add** and enter your appliance host name. The appliance host name should appear in the top **Additional Servers** section.
If the appliance has more than one host name, you must add all of the names.
- Click **OK** and close the **Primary Server Properties** window.

- 3 If a firewall exists between the primary server and the media server, open the following ports on the primary server to allow communication with the media server:

Note: You must be logged in as the administrator to change port settings.

- `vnetd: 13724`
 - `bprd: 13720`
 - `PBX: 1556`
 - If the primary server is a NetBackup appliance that uses TCP, open the following ports:
443, 5900, and 7578.
- 4 Make sure that the date and time of the media server matches the date and time on the primary server. You can use an NTP server or set the time manually.
 - 5 If you plan to use the new media server in a NAT network, perform the following tasks before you configure the media server:

- Enable the DNAT feature on the primary server.
On an appliance primary server, log in to the shell menu and run the following command:
`Main > Settings > NetBackup DNAT Enable`
On a traditional (non-appliance) NetBackup primary server, see the *Veritas NetBackup Administrator's Guide, Volume 1*. Refer to Chapter 5 and the topic title "Workflow to enable NAT hosts in NetBackup domain".

- Add the name of the new NAT media server to the NetBackup Servers list on the primary server.
On an appliance primary server, log in to the shell menu and run the following command:
`Main > Settings > NetBackup NATServers Add`
On a traditional (non-appliance) NetBackup primary server, add the NAT server names manually to the `bp.conf` registry file, or use the `bpsetconfig` command. The server names must be entered on one line with each server name separated by a space, as follows:

NAT_SERVER_LIST = media1 media2 media3

See ["Performing the initial configuration on a NetBackup Virtual Appliance media server"](#) on page 64.

Performing the initial configuration on a NetBackup Virtual Appliance media server

This section describes how to perform the initial configuration on a NetBackup Virtual Appliance with the media server role.

You must complete the following tasks on the primary server before you start the initial configuration. The following link provides specific instructions about how to accomplish the necessary tasks:

See [“Configuring a primary server to communicate with an appliance media server”](#) on page 62.

- Make sure that the primary server and this media server have compatible software versions.
- Add the host name of this media server to the `SERVERS` list on the primary server that you plan to use with it.
- If a firewall exists between the primary server and this media server, open the appropriate ports on the primary server.
- Make sure that the date and time of this media server matches the date and time on the primary server.
- If you plan to use this media server in a NAT network, make sure to enable the DNAT feature on the primary server and to also add this media server name to the NAT servers list on the primary server.

To perform the initial configuration of a NetBackup Virtual Appliance

- 1 After you have deployed a new virtual appliance, log on to the NetBackup Virtual Appliance Shell Menu.

The login is `admin`, and the default password is `P@ssw0rd`.

- 2 (Optional) Configure the appliance date and time.

NTP is an optional during the initial configuration wizard. If you do not use an NTP server in your environment, make sure to configure the appliance date and time before the initial configuration.

Caution: If the date and time of this media server matches the date and time of the primary server, the initial configuration wizard fails.

- Navigate to the `Main > Network view`.
- Set the time zone by entering the following command:
`TimeZone Set`
 Select the appropriate time zone from the displayed list.

- Set the date and the time by entering the following command:

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

Where *Month* is the name of the month.

Where *Day* is the day of the month from 1 to 31.

Where *HHMMSS* is the hour, minute, and seconds in a 24-hour format.

The fields are separated by semi-colons, for example, HH:MM:SS.

Where *Year* is the calendar year from 1970 through 2037.

3 (Optional)

If you plan to use this media server in a NAT network, perform the following tasks on the associated primary server before you start the initial configuration:

- Enable the `DNAT` feature on the primary server.
- Add the name of this media server to the NetBackup Servers list on the primary server.
 See [“Configuring a primary server to communicate with an appliance media server”](#) on page 62.

4 Use the following command to start the initial configuration:

```
Main > Appliance > Configure
```

A message about the **Virtual Appliance Initial Configuration Wizard** appears. This wizard will walk you through a two-step process to configure this appliance.

5 The wizard prompts you to change the default passwords.

Change each user account password as prompted.

Review the following password policy before setting a new password:

- Passwords must contain at least eight characters.
- Passwords must contain at least one lowercase letter (a-z) and one number (0-9).
- Dictionary words are considered weak passwords and are not accepted.
- The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.

Note: If you enter five consecutive invalid passwords for any user account, the appliance aborts the initial configuration process automatically. You must start the initial configuration process again.

Note: If you enable the STIG feature after completing the initial configuration, you may be prompted to change the new passwords you entered here to meet the requirements of the STIG password policy.

6 The wizard takes you to the network configuration.

Specify the following:

- **Hostname**

Enter a short host name or a fully qualified domain name (FQDN) for this appliance. As a best practice, Veritas recommends that you use FQDN.

Caution: After the initial deployment has completed successfully, the only way to change the host name is to perform a factory reset.

Note: If you plan to configure Active Directory (AD) authentication on this appliance, the host name must be 15 characters or less. Otherwise, AD configuration can fail.

- **DNS domain name**

Enter a DNS domain name for this appliance.

- **IPv4 address**

Enter the IPv4 address to be used for this appliance.

- **Netmask**

Enter the netmask that corresponds to the IP address.

- **Gateway IP address**

Enter the IPv4 address of the gateway (network point) that acts as an entrance to another network.

- **DNS server 1 IP address**

Enter the IPv4 address of the primary DNS server for this appliance.

- **DNS server 2 IP address(Optional)**

Enter the IPv4 address of the secondary DNS server for this appliance.

7 (Optional) The following prompt appears:

```
The host name must be resolvable with a DNS or a HOSTS file for
the initial configuration to be successful. Do you want to write
the host name resolution information to the HOSTS file? [yes,
no] (no)
```

Note: If the host name is not resolvable with a DNS or a HOSTS file during the initial configuration, the initial configuration wizard will fail.

Type **yes** to use the HOSTS file to resolve the appliance host name. This ensures that the host name is resolvable when DNS is not available.

Type **no** to use the DNS you entered.

8 After the network configuration is completed, the wizard takes you to the next step for storage configuration.

In the second step, specify the following:

- **NTP server (Optional)**

Enter the Network Time Protocol (NTP) server for this appliance.

- **Primary server**

Enter the NetBackup primary server name or IP address for this appliance. The primary server can be a traditional (non-appliance) NetBackup primary server or a NetBackup physical appliance.

Note: If the host name of the primary server is an FQDN, Veritas recommends that you use the FQDN to specify the primary server for the media server.

- After you have entered the primary server name, the appliance pings the primary server for the Certificate Authority (CA) status and shows the result. Each of the following bullet statements describes the possible status results. Follow the instructions that appear below the applicable status result to complete the certificate configuration.

- The primary server `<primary_server_name>` has an enabled External CA-signed certificate. Do you want to import the External CA-signed certificate for this Media server now [yes,no] (yes) :

Press **Enter** to continue. The following message appears:

The following shares have been opened on the appliance for you to upload certificate files:

NFS share <media_server_name>:/inst/share

CIFS share \\<media_server_name>\general_share

Enter the following details for external certificate configuration:

Enter the certificate file path:

Enter the trust store file path:

Enter the private key path:

Enter the password for the passphrase file path or skip security configuration (default: NONE):

Enter the following details for CRL usage:

Should a CRL be honored for the external certificate?

- 1) Use the CRL defined in the certificate.
- 2) Use the specific CRL directory.
- 3) Do not use a CRL.
- q) Skip security configuration.

CRL option: Enter 1, 2, 3, or q.

Verify the External CA details that you entered:

Certificate file name:

Trust store file name:

Private key file name:

CRL check level: (Shows the selected CRL option.)

Do you want to use the above certificate files? [yes, no] (yes):

After verifying that the entered information is correct, press **Enter to continue and answer the following prompt:**

Is this correct? [yes, no] (yes):

If all of the information is correct, press **Enter to continue.**

The appliance performs an ECA health check and shows the result of each validation check. When the health check has completed successfully, the following messages appear:

ECA health check was successful.

The external certificate has been registered successfully.

- The primary server <primary_server_name> currently uses an external CA issued certificate and its own internal certificate. Would you like to proceed with the external CA issued certificate? [yes,no] (yes):

If you select **no, the following message appears:**

This appliance will use a NetBackup issued certificate for secure communication.

If you select **yes**, enter the following details for external certificate configuration:

Enter the certificate file path:

Enter the trust store file path:

Enter the private key path:

Enter the password for the passphrase file path or skip security configuration (default: NONE):

Enter the following details for CRL usage:

Should a CRL be honored for the external certificate?

1) Use the CRL defined in the certificate.

2) Use the specific CRL directory.

3) Do not use a CRL.

q) Skip security configuration.

CRL option: Enter 1, 2, 3, or q.

Verify the External CA details that you entered:

Certificate file name:

Trust store file name:

Private key file name:

CRL check level: (Shows the selected CRL option.)

Do you want to use the above certificate files? [yes, no] (yes):

After verifying that the entered information is correct, press **Enter** to continue and answer the following prompt:

Is this correct? [yes, no] (yes):

If all of the information is correct, press **Enter** to continue.

The appliance performs an ECA health check and shows the result of each validation check. When the health check has completed successfully, the following messages appear:

ECA health check was successful.

The external certificate has been registered successfully.

- This appliance will use a NetBackup issued certificate for secure communication.

No further certificate configuration is required. Click **Next** to continue

For more information about security certificates, refer to the *NetBackup Security and Encryption Guide*.

9 Complete the remaining prompts for the storage configuration as follows:

- **AdvancedDisk disk pool name**
Enter a name for the AdvancedDisk disk pool on the appliance.
- **AdvancedDisk storage unit name**
Enter a name for the AdvancedDisk storage unit on the appliance.
- **AdvancedDisk storage size**
Enter a size for the AdvancedDisk storage.
- **MSDP storage unit name**
Enter a name for the MSDP storage unit on the appliance.
- **MSDP disk pool name**
Enter a name for the MSDP disk pool on the appliance.
- **MSDP storage size**
Enter a size for the MSDP storage.
- **MSDP Catalog size**
Enter a size for the MDSP Catalog storage.

- 10** Use the following command to verify that the automatic configuration completed successfully:

```
Main > Appliance > Status
```

The command output should contain a message similar to the following:

```
Appliance Version is 4.1.
```

```
Appliance is configured as media appliance.
```

If the output does not show that the appliance is configured as a media appliance, you need to redeploy the appliance or perform other troubleshooting steps to fix the issue before you proceed to the next step. See [“Troubleshooting NetBackup Virtual Appliance initial deployment issues”](#) on page 308.

- 11** Use the following command to set the time zone:

```
Main > Network > TimeZone Set
```

Select the appropriate time zone from the displayed list.

- 12** Add a permanent license key before the evaluation key expires with the following command:

```
Main > Manage > License > Add
```

You can locate your permanent license key from the Veritas Entitlement Management System (VEMS). To access VEMS, click **Licensing** on the [Veritas Support website](#).

Warning: If the correct license key is not installed, the appliance services stop functioning after the evaluation key expires. Make sure that the NetBackup license you add includes support for NetBackup Virtual Appliance.

See [“Managing license keys on the NetBackup Virtual Appliance”](#) on page 84.

- 13** (Optional)

If you want to configure an IPv6 address for the appliance, run the following command:

```
Main > Network > IPv6 <IPAddress> <Prefix> InterfaceName
```

Where *<IPAddress>* is the IPv6 address and *<Prefix>* is the prefix length.

See [“About IPv4-IPv6-based network support”](#) on page 120.

- 14** (Optional)

If you want to an IPv6 DNS server on the appliance, run the following command:

```
Main > Network > DNS Add NameServer <IPAddress>
```

Where *<IPAddress>* is the IPv6 address of the additional DNS server. Only global-scope and unique-local IPv6 addresses are allowed.

See [“Configuring DNS and host name mapping for the NetBackup Virtual Appliance”](#) on page 122.

- 15** If you want to configure the appliance for MSDP cloud, log in to the NetBackup web UI as the **nbsecadmin** user and configure the MSDP cloud storage as follows:

- Create a disk pool.
- Create a storage unit.

For details, see the *NetBackup Web UI Administrator's Guide*.

After the appliance is configured and operational, you are ready to install NetBackup client software on the computers that you want to back up.

See the *NetBackup Installation Guide* for how to install NetBackup clients.

How to deploy and configure a NetBackup Virtual Appliance primary server

Use the following procedure to deploy a NetBackup Virtual Appliance primary server.

Table 3-4 Before you deploy a NetBackup Virtual Appliance primary server

Step	Task
Step 1	Review the available product files (OVF templates) for deployment. See “NetBackup Virtual Appliance product files (OVF templates)” on page 29.
Step 2	Download the NetBackup Virtual Appliance product file from the Download Center on the Veritas Support website.
Step 3	Review the deployment guidelines and prepare the checklist. See “NetBackup Virtual Appliance deployment guidelines” on page 34.

Table 3-5 Deployment and initial configuration

Step	Task
Step 4	Deploy the NetBackup Virtual Appliance primary server. See “Using the vSphere Client to deploy a NetBackup Virtual Appliance primary server” on page 72. See “Using the OVF Tool to deploy a primary server” on page 74.
Step 5	Configure the appliance for the first time. See “Performing the initial configuration on a NetBackup Virtual Appliance primary server” on page 75.

Using the vSphere Client to deploy a NetBackup Virtual Appliance primary server

The section describes how to deploy and configure a NetBackup Virtual Appliance primary server by using the vSphere Client.

To ensure a successful deployment, make sure that you meet all of the deployment guidelines before you begin these procedures.

See [“NetBackup Virtual Appliance deployment guidelines” on page 34.](#)

Note: The following procedure is based on the VMware vSphere Client. It also applies to the browser-based VMware vSphere Web Client. Note that the order of the steps are slightly different with the web client.

To deploy a primary server appliance using the VMware vSphere Client

- 1 Using the VMware vSphere Client, log on to the vCenter Server where you want to deploy your appliance.

Note: Your vCenter Server user account must have at least the minimum privileges required to deploy an OVF template. Refer to the VMware documentation for more information.

- 2 Select **File > Deploy OVF Template** to start the deployment wizard.
- 3 On the **Source** page of the deployment wizard, click **Browse** to navigate to the NetBackup Virtual Appliance product file. If you split the file when you downloaded it, make sure that all of the pieces are saved in the same folder and navigate to that folder.

Verify the path and click **Next**.
- 4 Review the **OVF Template Details** page and click **Next**.
- 5 On the **End User License Agreement** page, read through the EULA and click **Accept**, and then **Next**.
- 6 Enter the destination details as follows:
 - **Name:** Enter a unique name for your appliance.
 - **Inventory Location:** Select the folder or the data center where you want the appliance to be located. The options are autopopulated based on what is available to that vCenter Server.
 Click **Next**.
- 7 Select the resource location where you want the deployed template to run.
Click **Next**.
- 8 Select the destination storage where you want to store the appliance files.
Click **Next**.

Caution: If you select a storage cluster, make sure that one of the datastores in the cluster has enough storage space for the entire appliance. If none of the individual datastores in the cluster has enough space, the deployment fails.

- 9 Select **Thick Provision Lazy Zeroed** as the provisioning format for the appliance disks, and make sure that the **Disk Mode** is set to **Independent - Persistent** for all disks other than the OS disk. For more information on provisioning or the disk mode, refer to the VMware documentation.

Click **Next**.

- 10 Select the destination networks to map the networks used in the OVF template.

Click **Next**.

- 11 Read through and verify the deployment options that you entered. If everything is correct, click **Finish** to start the deployment.

The amount of time that it takes for the deployment process to complete varies depending on your network connection. The process can take up to 30 minutes to complete.

After the deployment is complete, proceed to perform the initial configuration steps in the following topic.

See [“Performing the initial configuration on a NetBackup Virtual Appliance primary server”](#) on page 75.

After the appliance is configured and operational, you are ready to install NetBackup client software on the computers that you want to back up.

See the *NetBackup Installation Guide* for how to install NetBackup clients.

See [“Common tasks in NetBackup Virtual Appliance”](#) on page 86.

See [“About modifying the NetBackup Virtual Appliance settings”](#) on page 81.

Using the OVF Tool to deploy a primary server

The section describes how to deploy a NetBackup Virtual Appliance primary server by using the VMware OVF Tool.

To ensure a successful deployment, make sure that you meet all of the deployment guidelines before you begin these procedures.

See [“NetBackup Virtual Appliance deployment guidelines”](#) on page 34.

Note: This procedure requires a vCenter Server. For how to deploy an OVF package directly on an ESXi host, see the following technical article.

https://www.veritas.com/support/en_US/article.100038949

To deploy a primary server appliance using the VMware OVF Tool

- 1 Log on to the vCenter Server where you want to deploy your appliance.

Note: Your vCenter Server user account must have at least the minimum privileges required to deploy an OVF template. Refer to the VMware documentation for more information.

- 2 Use the VMware OVF Tool to deploy the OVF package.

OVF descriptors can contain configuration properties for the deployed OVF package. Replace the variables with the environment information you gathered, and use a blank to separate the options and property mappings.

Run the following OVF tool command to deploy the virtual appliance:

```
ovftool
--name=<nbva_name>
--acceptAllEulas
--net:"VM Network=<vm_network>"
--allowAllExtraConfig
--datastore=<vm_datastore>
--powerOn
<nbva_ova>
vi://<vCenter_username>:<vCenter_password>/?ip=<hostIPAddress>
```

For more information about the OVF Tool, refer to the [VMware OVF Tool documentation](#).

- 3 Once the deployment is complete, proceed to perform the initial configuration steps in the following topic.

See [“Performing the initial configuration on a NetBackup Virtual Appliance primary server”](#) on page 75.

Performing the initial configuration on a NetBackup Virtual Appliance primary server

This section describes how to perform the initial configuration on a NetBackup Virtual Appliance primary server.

To perform the initial configuration on a NetBackup Virtual Appliance with the combined primary and media server role

- 1** After you have deployed a new virtual appliance, log on to the NetBackup Virtual Appliance Shell Menu.

The logon is `admin`, and the default password is `P@ssw0rd`.

- 2** Use the following command to start the initial configuration:

```
Main > Appliance > Configure
```

A message about the **Virtual Appliance Configuration Wizard** appears.

- 3** The wizard prompts you to change the default passwords.

Change each user account password as prompted.

Review the following password policy before setting a new password:

- Passwords must contain at least eight characters.
- Passwords must contain at least one lowercase letter (a-z) and one number (0-9).
- Dictionary words are considered weak passwords and are not accepted.
- The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.

Note: If you enter five consecutive invalid passwords for any user account, the appliance aborts the initial configuration process automatically. You must start the initial configuration process again.

Note: If you enable the STIG feature after completing the initial configuration, you may be prompted to change the new passwords you entered here to meet the requirements of the STIG password policy.

- 4** The wizard takes you to the network configuration.

Specify the following:

- **Hostname**
Enter a short host name or a fully qualified domain name (FQDN) for this appliance. As a best practice, Veritas recommends that you use FQDN.

Caution: After the initial deployment has completed successfully, the only way to change the host name is to redeploy the appliance.

Note: If you plan to configure Active Directory (AD) authentication on this appliance, the host name must be 15 characters or less. Otherwise, AD configuration can fail.

- **DNS domain name**

Enter a DNS domain name for this appliance.

- **IPv4 address**

Enter the IPv4 address to be used for this appliance.

- **Netmask**

Enter the netmask that corresponds to the IP address.

- **Gateway IP address**

Enter the IPv4 address of the gateway (network point) that acts as an entrance to another network.

- **DNS server 1 IP address**

Enter the IPv4 address of the primary DNS server for this appliance.

- **DNS server 2 IP address(Optional)**

Enter the IPv4 address of the secondary DNS server for this appliance.

When you are prompted with the following message, choose whether you want to add the host name and IP address to the HOSTS file.

```
The host name must be resolvable with a DNS or a HOSTS file for
the initial configuration to be successful. Do you want to write
the host name resolution information to the HOSTS file? [yes,
no] (no)
```

Note: The host name must be resolvable with a DNS server or a HOSTS file for the initial configuration to be successful. If DNS is not available, you can add the host name and IP address to the HOSTS file.

- 5 After the network configuration is completed, the wizard takes you to the next step for the Veritas Usage Insights customer registration key. You cannot complete the configuration until you provide the registration key. To obtain a key, follow the onscreen prompts.

- 6 Use the following command to verify that the automatic configuration completed successfully:

```
Main > Appliance > Status
```

The command output should contain a message similar to the following:

```
Appliance Version is 4.1.
```

```
Appliance is configured as primary appliance.
```

If the output does not show that the appliance is configured as a primary appliance, you need to redeploy the appliance or perform other troubleshooting steps to fix the issue before you proceed to the next step. See [“Troubleshooting NetBackup Virtual Appliance initial deployment issues”](#) on page 308.

- 7 Use the following command to change the **nbasecadmin** account password from the known default password (**P@ssw0rd**):

```
Main > Settings > Password nbasecadmin
```

Note: You cannot access the NetBackup web UI until you have changed the **nbasecadmin** user password.

- 8 Use the following command to set the time zone:

```
Main > Network > TimeZone Set
```

Select the appropriate time zone from the displayed list.

- 9 Use the following command to add a Network Time Protocol (NTP) server:

```
Main > Network > NTPServer Add <Server>
```

Where **<Server>** is the name of the NTPServer.

- 10** Add a permanent license key before the evaluation key expires with the following command:

```
Main > Manage > License > Add
```

You can locate your permanent license key from the Veritas Entitlement Management System (VEMS). To access VEMS, click **Licensing** on the [Veritas Support website](#).

Warning: If the correct license key is not installed, the appliance services stop functioning after the evaluation key expires. Make sure that the NetBackup license you add includes support for NetBackup Virtual Appliance.

See [“Managing license keys on the NetBackup Virtual Appliance”](#) on page 84.

- 11** (Optional)

If you want to configure an IPv6 address for the appliance, run the following command:

```
Main > Network > IPv6 <IPAddress> <Prefix> InterfaceName
```

Where *<IPAddress>* is the IPv6 address and *<Prefix>* is the prefix length.

See [“About IPv4-IPv6-based network support”](#) on page 120.

- 12** (Optional)

If you want to an IPv6 DNS server on the appliance, run the following command:

```
Main > Network > DNS Add NameServer <IPAddress>
```

Where *<IPAddress>* is the IPv6 address of the additional DNS server. Only global-scope and unique-local IPv6 addresses are allowed.

See [“Configuring DNS and host name mapping for the NetBackup Virtual Appliance”](#) on page 122.

- 13** (Optional)

If you want to use an external Certificate Authority (CA) for communication between the appliance and your other NetBackup hosts, run the following command:

```
Main > Settings > NetBackup CertificateUsage Enable ECA
```

- 14** (Optional)

If you plan to use this primary server with a media server in a NAT network, perform the following tasks:

- Enable the NetBackup DNAT feature on this primary server as follows:

Main > Settings > NetBackup DNAT Enable

- Add the name of the media server to the NetBackup Servers list on this primary server as follows:

Main > Settings > NetBackup NATServers Add

- 15** Log on to the appliance from the NetBackup Administration Console and create a NetBackup catalog backup policy.

By default, the primary server appliance does not contain a NetBackup catalog backup policy. To protect the NetBackup catalog, configure a catalog backup before using NetBackup for regular client backups.

You can create a backup policy that uses a Storage Lifecycle Policy (SLP) to protect the NetBackup catalog. Use the SLP to back up the data to AdvancedDisk and then duplicate it to MSDP. You are then able to use Auto Image Replication to save your catalog backup off site. Veritas recommends that you use this replication-based strategy for disaster recovery (DR).

Note: You must set a encryption passphrase for the disaster recovery package for the catalog to be successful. Catalog backups continue to fail until the passphrase is set.

For more information about the security requirements for disaster recovery , see the *NetBackup Security and Encryption Guide*.

After the appliance is configured and operational, you are ready to install NetBackup client software on the computers that you want to back up.

See the *NetBackup Installation Guide* for how to install NetBackup clients.

If you plan to use AdvancedDisk to back up your clients, note that the AdvancedDisk does not support Auto Image Replication. If you want to save the data off site, create an SLP to duplicate the backup data on AdvancedDisk to MSDP. You are then able to use Auto Image Replication to transfer the data off site.

Post initial configuration procedures

This chapter includes the following topics:

- [About modifying the NetBackup Virtual Appliance settings](#)
- [Adding a permanent license key if an evaluation license key expires](#)
- [Managing license keys on the NetBackup Virtual Appliance](#)

About modifying the NetBackup Virtual Appliance settings

After you have successfully deployed your appliance, you can use the NetBackup Virtual Appliance Shell Menu to change various settings for your appliance.

[Table 4-1](#) contains information about some of the commonly used appliance settings.

Table 4-1

Appliance function	Task	Command view
Network	Add host information, configure static routes, and manage WAN Optimization on the appliance.	Network See “Network settings for the NetBackup Virtual Appliance” on page 121.

Table 4-1 (continued)

Appliance function	Task	Command view
User management and authentication	Add new users and create user groups for accessing your appliance.	Settings > Security > Authentication Settings > Security > Authorization See “About managing NetBackup Virtual Appliance users” on page 127.
Password management	Change a user, admin, or maintenance password.	Settings > Security > Authentication See “Changing NetBackup Virtual Appliance user passwords” on page 145.
Alert configuration	Configure the SNMP, SMTP, and Call Home settings.	Settings > Alerts See “About NetBackup Virtual Appliance alerts” on page 212.
Date and time configuration	Change the date and time on your appliance.	Network See “Setting the date and time on a NetBackup Virtual Appliance” on page 123.
Login banner	Create a customized text banner that appears when you access the appliance.	Settings > Notifications > Login Banner See “Setting the appliance login banner” on page 250.

See [“Common tasks in NetBackup Virtual Appliance”](#) on page 86.

See [“Configuring static routes on the NetBackup Virtual Appliance”](#) on page 124.

Adding a permanent license key if an evaluation license key expires

If your evaluation license key expires, you may encounter problems with your appliance. You can avoid future issues if you add a permanent license key before the evaluation key expires.

The following list identifies some symptoms that you may encounter if the evaluation key has expired and if you have not added a permanent key:

- A fully configured NetBackup Virtual Appliance stops working.
- You may even observe the following issues with an appliance that does not have permanent keys installed:
 - System self-test fails.
 - Backup and restore jobs fail.
 - The user interface does not load.

You can locate your permanent license key from the Veritas Entitlement Management System (VEMS). To access VEMS, click **Licensing** on the [Veritas Support website](#).

To install a permanent license key on a NetBackup Virtual Appliance with an expired evaluation key

- 1 Log on to the NetBackup Virtual Appliance Shell Menu as an administrator.

Note: If the appliance has not already been configured, use `admin` as the user name and `P@ssw0rd` as the password.

- 2 Enter `Main_Menu > Manage > License > Add`.
- 3 Enter a valid evaluation or production license key when prompted for a NetBackup license key.

Caution: The appliance services do not function if the correct key is not installed. Make sure that the license key you add includes support for NetBackup Virtual Appliance.

- 4 Enter `n` when prompted to add an additional license key.
- 5 Stop the NetBackup processes.

```
Main_Menu > Support > Processes > NetBackup Stop
```

- 6 Start NetBackup processes.

```
Main_Menu > Support > Processes > NetBackup Start
```

See [Manage > License > Add](#) on page 393.

See [“Managing license keys on the NetBackup Virtual Appliance”](#) on page 84.

Managing license keys on the NetBackup Virtual Appliance

The following procedures describe how to view, add, and delete license keys through the NetBackup Virtual Appliance Shell Menu.

Caution: The appliance services do not function if the correct license key is not installed. When managing the license keys, make sure that you always have a license key entered on the appliance and that it includes support for NetBackup Virtual Appliance.

To view, add, and delete license keys through the NetBackup Virtual Appliance Shell Menu

- 1 To view a list of all installed license keys or view the details of each key, enter one of the following commands:

- `Main_Menu > Manage > License > List`

A complete list of installed license keys appears.

- `Main_Menu > Manage > License > ListInfo`

The associated feature IDs and feature names appear.

The NetBackup Virtual Appliance feature ID appears as follows:

```
Feature ID          = 91 Virtual Appliance +
```

- 2 To add license keys, do the following:

- Enter `Main_Menu > Manage > License > Add`.

- Enter the license key for the option that you want to install. Then press **Enter**.

Caution: The NetBackup Virtual Appliance requires a specific license key, and the appliance services do not function if the correct key is not installed. Make sure that the license key that you add is correct for NetBackup Virtual Appliance.

- To add another license key, press `y`.

- Repeat the previous step or press `n` to exit.

- 3 To delete license keys, do the following:

- Enter `Main_Menu > Manage > License > Remove`.

- Enter the license key for the option that you want to remove. Then press **Enter**.

Warning: If you remove the NetBackup Virtual Appliance license key, appliances services shut down until you enter a new key.

- To remove another license key, press `y`.
- Repeat the previous step or press `n` to exit.

See [“Adding a permanent license key if an evaluation license key expires”](#) on page 82.

Appliance common tasks

This chapter includes the following topics:

- [Common tasks in NetBackup Virtual Appliance](#)

Common tasks in NetBackup Virtual Appliance

The following table contains quick links on how to perform the common tasks in NetBackup Virtual Appliance.

Table 5-1 Quick links for common appliance tasks

Appliance functions	Tasks	Go to this topic
Monitoring	Monitor software and Symantec Data Center Security (SDCS)	See “About Call Home” on page 219. See “About Symantec Data Center Security on the NetBackup Virtual Appliance” on page 225.
Managing the appliance	Configure Auto Image Replication from the appliance Manage host and deduplication settings of the appliance Add or remove license keys	See “About Auto Image Replication from a NetBackup Virtual Appliance” on page 208. See “About configuring Host parameters for your appliance on the NetBackup Virtual Appliance” on page 181. See “Managing NetBackup Virtual Appliance deduplication” on page 187. See “Managing license keys on the NetBackup Virtual Appliance” on page 84.

Table 5-1 Quick links for common appliance tasks (*continued*)

Appliance functions	Tasks	Go to this topic
Storage management	Resize or move partitions, if applicable Add or remove disks, if applicable View disk status View the partition distribution on a disk	See “About NetBackup Virtual Appliance storage configuration” on page 89. See “About viewing storage space information using the <code>show</code> command” on page 92. See “Resizing a partition” on page 101. See “Moving a partition” on page 102. See “Monitoring the progress of storage manipulation tasks” on page 104. See “Scanning storage devices using the NetBackup Virtual Appliance Shell Menu” on page 105. See “Adding storage space for the NetBackup Virtual Appliance” on page 105. See “Removing an existing storage disk” on page 107.
Restoring an appliance	Create a checkpoint Rollback to a checkpoint Perform Factory Reset (not available on primary server)	See “About appliance restore” on page 285.
Configuring appliance settings	Alert and Call Home Network Date and Time User authentication and management Password management	See “About modifying the NetBackup Virtual Appliance settings” on page 81.

Table 5-1 Quick links for common appliance tasks (*continued*)

Appliance functions	Tasks	Go to this topic
Deployment and initial configuration	Deploy a NetBackup Virtual Appliance Perform initial configuration	See “How to deploy and configure a NetBackup Virtual Appliance combined primary and media server” on page 40. See “How to deploy and configure a NetBackup Virtual Appliance media server” on page 58. See “How to deploy and configure a NetBackup Virtual Appliance primary server” on page 72.
Troubleshooting	Troubleshoot appliance issues	See “About troubleshooting the NetBackup Virtual Appliance” on page 297. See “Gathering device logs on a NetBackup virtual appliance” on page 326.

Storage management

This chapter includes the following topics:

- [About NetBackup Virtual Appliance storage configuration](#)
- [About Universal Shares](#)
- [About OpenStorage plugin installation](#)

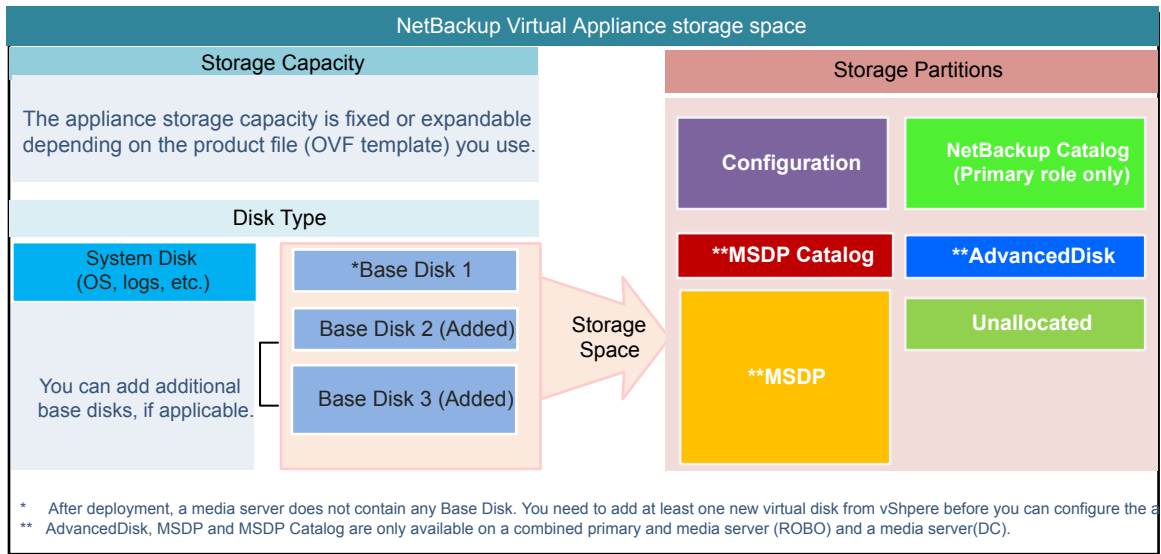
About NetBackup Virtual Appliance storage configuration

The `Manage > Storage` commands enable you to manage the storage configuration. You can use the `Storage > Show ALL` command to quickly view the storage configuration.

You can add additional storage space to the appliance. Use the `Storage > Add` command to add disks with a capacity that is a multiple of 0.5 TB.

[Figure 6-1](#) provides a bird's-eye view of how storage space is configured within your appliance.

Figure 6-1 NetBackup Virtual Appliance storage space



NetBackup Virtual Appliance supports AdvancedDisk and Media Server Deduplication (or MSDP) on the following:

- Combined primary and media server for remote offices and branch offices (ROBO)
- Media server for data centers (DC)

Note: AdvancedDisk, MSDP and MSDP Catalog are not available on primary server appliances.

Depending on your appliance platform, the appliance storage can be divided using the following storage partitions:

Configuration A storage partition that stores configuration information. The configuration partition size is 50 GB.

AdvancedDisk AdvancedDisk enables you to back up and restore data at a faster rate. It does not involve any deduplication.

NetBackup Catalog This partition contains metadata for NetBackup which includes information regarding backups, storage devices, and configuration. The NetBackup Catalog partition is only supported on an appliance primary server.

The NetBackup Catalog is always located on a Base disk.

MSDP	The allocated space for Media Server Deduplication (or MSDP) on your appliance.
MSDP Catalog	This partition contains metadata for MSDP which includes information regarding MSDP backups.
NDMP Log	This partition contains logs that are generated when NDMP is enabled during the backup operation. The NDMP Log partition is only available to a media server, and you must create it first if you want to use it. If you do not create it, the NDMP logs are saved to the system disk and have limited storage space. If you need additional space, you can create the NDMP log partition. See “Creating an NDMP log partition” on page 103.
VxUpdate Repository	This storage space is allocated for supported VxUpdate client and NetBackup EEB packages.
Unallocated	The storage space that has not been allocated to the other partitions (includes all partitions that are displayed except Unallocated). When you expand the storage space for partitions like MSDP, AdvancedDisk, it is used from the Unallocated space. When you add a disk, the size of the Unallocated space increases. The size of the MSDP, AdvancedDisk, and any other partition remains the same.

[Table 6-1](#) lists the supported sizes for each partition.

Table 6-1 Appliance storage partitions supported size

Partition Name	Minimum supported size	Maximum supported size
AdvancedDisk	5 GB	Maximum available capacity
NetBackup Catalog	5 GB	Maximum available capacity
MSDP	5 GB	Maximum available capacity
MSDP Catalog	5 GB	Maximum available capacity
NDMP Log	100 GB	Maximum available capacity
VxUpdate Repository	10 GB	Maximum available capacity

See the NetBackup documentation for more information on partitions.

See [“About viewing storage space information using the `show` command”](#) on page 92.

See [“Resizing a partition”](#) on page 101.

See [“Moving a partition”](#) on page 102.

- See “Monitoring the progress of storage manipulation tasks” on page 104.
- See “Scanning storage devices using the NetBackup Virtual Appliance Shell Menu” on page 105.
- See “Adding storage space for the NetBackup Virtual Appliance” on page 105.
- See “Removing an existing storage disk” on page 107.

About viewing storage space information using the `Show` command

The `Manage > Storage > Show` command enables you to view the appliance storage information:

- [Disk information](#)
- [Partition information](#)
- [Storage unit and disk pool configuration](#)

You can use the `Storage > Show` commands to do the following:

- `Show ALL` - to view disk, partition, and distribution information together.
- `Show Disk` - to view total capacity, unallocated storage capacity, and current status of a disk.
- `Show Partition [All/Configuration/Usage]` - to view total, available, and used storage capacity of a partition.
- `Show Distribution` - to view the distribution of partitions on a disk.

Disk information

This disk information section provides a tabular representation of the storage disks that comprise your appliance and the partition distribution.

For example:

Disk ID	Type	Total	Unallocated	Status
SCSI(0:0)	System	512 GB	-	N/A
SCSI(0:1)	Base	2.10 TB	1.97 GB	In Use

SCSI(0:1) (Base)

AdvancedDisk	:	64 GB
- 0	:	64 GB
Configuration	:	50 GB
- 0	:	50 GB

```
MSDP                :    1.94 TB
- 0                 :    1.94 TB
MSDP Catalog        :     20 GB
- 0                 :     20 GB
NetBackup Catalog    :     30 GB
- 0                 :     30 GB
```

The columns are described in the following table:

Column names	Description
Disk ID	Displays the ID that is associated with the disk. Example: SCSI(0:1)
Type	Displays the type of disk. Example: Base Table 6-2 describes each disk type.
Total	Displays the total storage space within the disk. Example: 4.5429 TB
Unallocated	Displays the available space within the disks. Example: 1.9172 GB
Status	Displays the status of the disk. Example: In Use Table 6-3 describes each status.

[Table 6-2](#) lists the disk types that can appear depending on your appliance model.

Table 6-2 Disk types

Type	Description
System	Contains the appliance operating system, logs, etc.
Base	Contains the appliance storage partitions.
Unknown	This type appears when appliance cannot determine the disk type like when the disk is not accessible.

Table 6-3 Disk status

Status	Description
In Use	Denotes that the disk is currently in use. Note: The appliance can only remove an In Use disk when the disk does not contain any partitions.
N/A	Denotes that no commands or operations can be performed on disks with this status. An example of a disk that has an N/A status is System.
New Available	Denotes that the disk is available to be added to the storage space. Note: The appliance can only add a New Available disk when the disk size is a multiple of 0.5 TB or 512 GB.
Not Accessible	Storage disk that was In Use is not accessible any more.

If you want to expand storage by provisioning new disks to the appliance, make sure the disk size is a multiple of 0.5 TB or 512 GB. Once these storage disks have been created, you must scan for the newly available disks by using the `Storage > Scan` command from the shell menu. The new disks have the **New Available** status. Once the newly available disks are displayed, you can add these disks to increase the storage space.

See [“Adding storage space for the NetBackup Virtual Appliance”](#) on page 105.

Note: You can use the `Datacollect` command from the `Main > Support` shell menu to gather storage disk logs. You can share these disk logs with the Support team to resolve disk-related issues. More information about the `Main > Support > Datacollect` menu is available.

Partition information

The partition information section shows the details about all the storage partitions that are configured on the appliance by type and by name (numeric).

For example:

Partition	Total	Available	Used	%Used	Status
AdvancedDisk	64 GB	63.43 GB	582.67 MB	1	Optimal
Configuration	50 GB	49.25 GB	771.95 MB	2	Optimal

MSDP	1.94 TB	1.92 TB	15.87 GB	1	Optimal
MSDP Catalog	20 GB	19.78 GB	228.21 MB	2	Optimal
NetBackup Catalog	30 GB	29.44 GB	573.84 MB	2	Optimal
Unallocated	1.96 GB	-	-	-	-

AdvancedDisk

Partition	Total	Available	Used	%Used	Status
0	64 GB	63.43 GB	582.67 MB	1	Mounted

Configuration

Partition	Total	Available	Used	%Used	Status
0	50 GB	49.25 GB	771.95 MB	2	Mounted

...

The columns are described in the following table:

Column Name	Description
Partition	Displays the type or name of the partition. Type example: AdvancedDisk Name example: 0
Total	Displays the total space within the partition. Example: 1.63 TB
Available	Displays the free space within a partition. Example: 1.62 TB
Used	Displays the used space within a partition. Example: 13.70 GB
Used Percentage	Displays the percentage of used space in the partition. Example: 2%
Status	Displays the status of the partition. Example: Optimal Table 6-4 describes each partition status.

Table 6-4 describes the various status of a partition type.

Table 6-4 Partition type status

Status	Description
Optimal	The storage partition is accessible and the entire capacity is available for backups.
Degraded	The entire storage capacity of the partition is not available in this state. Only a limited storage capacity of the partition is available.
Not Accessible	The entire storage capacity of the partition is not available so no tasks can be performed.
Not Configured	Storage is not configured or imported for the storage partition.

Table 6-5 describes the various status of a particular partition.

Table 6-5 Partition name status

Status	Description
Mounted	The partition is currently mounted.
Not Mounted	The partition is not currently mounted. If the partition is not mounted, the status can either be Degraded or Not Accessible. See Table 6-4 for more information.
I/O Error	There is an I/O error with the partition. If the partition has an I/O error, the status can either be Degraded or Not Accessible. See Table 6-4 for more information.

Note: The sizes that are displayed for the MSDP partition by using the **Manage > Storage > Show** command may not be the full space that is 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. For more information, see the *NetBackup Deduplication Guide*

Check the MSDP disk pool sizes displayed on the NetBackup Administration Console to know the MSDP statistics.

Storage unit and disk pool configuration

The configuration information section shows the details about all the disk pool and storage unit names that are configured on the appliance.

For example:

```
AdvancedDisk
-----
Disk Pool (DP)   | Storage Unit (STU)
-----
dp_adv_abc123   | stu_adv_abc123

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

The columns are described in the following table:

Column name	Description
Disk Pool (DP)	Displays the disk pool name for the partition type.
Storage Unit (STU)	Displays the storage unit name for the partition type.

See also

- See [“Viewing all storage information”](#) on page 97.
- See [“Viewing disk information”](#) on page 98.
- See [“Viewing partition information”](#) on page 99.
- See [“Viewing the partition distribution on disks”](#) on page 99.
- See [“About NetBackup Virtual Appliance storage configuration”](#) on page 89.

Viewing all storage information

The following procedure describes how to use the `Show All` command, using the NetBackup Virtual Appliance Shell Menu:

To view all storage information

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 Open the `Storage` menu. To open the storage menu, use the following command:

```
Main > Manage > Storage
```

The appliance displays all the sub-tasks in the storage menu.

- 3 Enter the `Show All` command to view device information.

See [“About NetBackup Virtual Appliance storage configuration”](#) on page 89.

See [“About viewing storage space information using the `Show` command ”](#) on page 92.

See [“Viewing disk information”](#) on page 98.

See [“Viewing partition information”](#) on page 99.

See [“Viewing the partition distribution on disks”](#) on page 99.

Viewing disk information

The following procedure describes how to use the `Show Disk` command, using the NetBackup Virtual Appliance Shell Menu.

To view disk information

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 Open the `Storage` menu. To open the storage menu, use the following command:

```
Main > Manage > Storage
```

The appliance displays all the sub-tasks in the storage menu.

- 3 Enter the `Show Disk` command to view disk information.

The appliance displays the disk information as shown in the following example:

Disk ID	Type	Total	Unallocated	Status
SCSI(0:1)	System	512.00 GB	-	n/a
SCSI(0:2)	Base	4.54 TB	4.00 TB	In Use

See [“About NetBackup Virtual Appliance storage configuration”](#) on page 89.

See [“Viewing all storage information”](#) on page 97.

See [“Viewing partition information”](#) on page 99.

See [“Viewing the partition distribution on disks”](#) on page 99.

Viewing partition information

The following procedure describes how to use the `Show Partition` command to view the partition information.

To view partition information

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main > Manage > Storage` view, type the following command:

```
Show Partition [Info] [PartitionType] [Name]
```

- Specify the `[Info]` if you want to view either the usage information or the disk pool and storage unit configuration. The available options are `ALL`, `Configuration`, and `Usage`. The default value is `ALL`.
- Specify the `[PartitionType]` if you want to view the information about a particular partition type. The available options are `ALL`, `AdvancedDisk`, `NetBackupCatalog`, `Configuration`, `MSDP`, `MSDPCatalog`, `NDMPLog`, `NetBackupVxupdateRepository`. If not specified, the default value `ALL` is used.
- Specify the `[Name]` if you want to view the information of a particular partition. `Name` is the numeric 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.

See [“About NetBackup Virtual Appliance storage configuration”](#) on page 89.

See [“Viewing all storage information”](#) on page 97.

See [“Viewing disk information”](#) on page 98.

See [“Viewing the partition distribution on disks”](#) on page 99.

Viewing the partition distribution on disks

The following procedure describes how to use the `Show Distribution` command, using the NetBackup Virtual Appliance Shell Menu:

To view the partition distribution on a disk

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 Open the `Storage` menu. To open the storage menu, use the following command:

```
Main > Manage > Storage
```

The appliance displays all the sub-tasks in the storage menu.

- 3 Enter the `Show Distribution` command to view distribution of partitions on a disk.

The appliance displays the distribution of partitions on a disk as shown in the following example:

```
SCSI(0:1) (Base)
-----
AdvancedDisk      :      64 GB
- 0               :      64 GB
Configuration     :      50 GB
- 0               :      50 GB
MSDP              :     1.94 TB
- 0               :     1.94 TB
MSDP Catalog      :       20 GB
- 0               :       20 GB
NetBackup Catalog :       30 GB
- 0               :       30 GB

SCSI(0:2) (Base)
-----
MSDP              :     62.03 GB
- 1               :     62.03 GB
```

This command also shows the partition number that resides on the disk. This can help with troubleshooting issues when a partition status is degraded or when the disk fails.

See [“About NetBackup Virtual Appliance storage configuration”](#) on page 89.

See [“Viewing all storage information”](#) on page 97.

See [“Viewing disk information”](#) on page 98.

See [“Viewing partition information”](#) on page 99.

Resizing a partition

A partition can be resized to a higher or lower value.

Starting with release 4.0, you can resize the VxUpdate repository upward from its minimum of 10 GB. The maximum size of the partition is dependent on the amount of all unallocated storage.

Review the following points before you resize a storage partition:

- The AdvancedDisk, Configuration, MSDP, MSDP Catalog, NetBackup Catalog, NetBackup VxUpdate Repository, and the NDMP Log partitions can be resized to a higher or a lower value. To resize, enter values in increments of 1 GB.

Note: If you resize the MSDP storage partition to a greater amount, you may also need to resize the MSDP Catalog. If you need to resize the Catalog, the MSDP resize fails with an error message that lists the sizing requirement.

- Each partition has a minimum and maximum supported size. Ensure that you resize a partition within these values.

Note: Resizing a partition may take a significant amount of time depending on the configuration of the system and how much data is present. In some instances, the operation may appear to hang while running. Allow the operation time to fully complete.

The following procedure describes how to resize partitions.

To resize a storage partition from the NetBackup Virtual Appliance Shell Menu

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main > Manage > Storage` view, type the following command:

```
Resize <PartitionType> Size Unit
```

- *PartitionType* refers to the name of the partition like AdvancedDisk, 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).

See [Manage > Storage > Resize](#) on page 375.

See [“Troubleshooting resize-related issues”](#) on page 102.

See [“Monitoring the progress of storage manipulation tasks”](#) on page 104.

See [“About NetBackup Virtual Appliance storage configuration”](#) on page 89.

See [“About viewing storage space information using the `Show` command”](#) on page 92.

Troubleshooting resize-related issues

The following sample error message may appear when you resize a partition:

This message appears if the specific partition is being used or is fragmented. For example, the resize operation may fail when backup and restore operations are reading or writing data to the partition. In this scenario, you can retry resizing the partition after some time.

The message may also appear if the partition is fragmented. Contact Technical Support for further assistance.

See [“Resizing a partition”](#) on page 101.

See [“About NetBackup Virtual Appliance storage configuration”](#) on page 89.

See [“About viewing storage space information using the `Show` command”](#) on page 92.

Moving a partition

This procedure describes the process to move a partition from one storage disk to another.

Starting with release 4.0, you can move the NetBackup VxUpdate repository to any other disk volumes.

To move a partition

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main > Manage > Storage` view, type the following command:

```
Move Partition SourceDiskID TargetDiskID Size Unit
```

- `Partition` refers to the storage partition like AdvancedDisk, Configuration, MSDP, etc.

Note: The NetBackup Catalog partition cannot be moved on a combined primary and media server appliance.

- `SourceDiskID` refers to the disk ID of the source disk. Use `Show Distribution` to view the disk ID and the partitions on it.

- *TargetDiskID* refers to the disk ID of the target disk. Use `Show Distribution` to view the disk ID and the partitions on it.
- *Size* refers to the storage size that you want to move from the current disk to the new disk. 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.
- *Unit* refers to unit size (GB/TB/PB).

For example:

```
abc123.Storage> Move MSDP SCSI (0:3) SCSI (0:4) 5 GB
```

Note: The partition size and the workload on the system determine the time required to move a partition.

See [“Adding storage space for the NetBackup Virtual Appliance”](#) on page 105.

See [Manage > Storage > Move](#) on page 371.

See [“Monitoring the progress of storage manipulation tasks”](#) on page 104.

See [“Resizing a partition”](#) on page 101.

See [“About NetBackup Virtual Appliance storage configuration”](#) on page 89.

See [“About viewing storage space information using the `Show` command ”](#) on page 92.

Creating an NDMP log partition

When NDMP is enabled during your backup operations, the NDMP logs are saved to the system disk by default and have limited storage space. If you need additional space, you can create the NDMP log partition and move the current NDMP log data to that partition. Use the following procedure to create the NDMP log partition.

To create a partition for the NDMP logs

- 1 Make sure that you have at least 100 GB of storage space available on the appliance.
- 2 Stop all active NetBackup jobs.

- 3 Log in to the NetBackup Virtual Appliance Shell Menu and run the following command:

```
Support > Storage Create NDMPLogPartition
```

- 4 Follow the prompts to create the partition. When the operation is complete, run the following command and confirm that the new NDMP Log partition displays in the table.

```
Manage > Storage > Show Partition
```

Monitoring the progress of storage manipulation tasks

The following procedure describes how to use the `Monitor` command when using the NetBackup Virtual Appliance Shell Menu.

To monitor storage tasks

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 Go to the `Main > Manage > Storage` menu
- 3 Enter the `Monitor` command to view the current progress of the storage management tasks being performed.

The appliance displays the task progress as shown in the following example:

```
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)
```

See [“Removing an existing storage disk”](#) on page 107.

See [“Resizing a partition”](#) on page 101.

See [“About viewing storage space information using the `Show` command”](#) on page 92.

See [“About NetBackup Virtual Appliance storage configuration”](#) on page 89.

Scanning storage devices using the NetBackup Virtual Appliance Shell Menu

You can create new virtual disks and provision the disks to the NetBackup Virtual Appliance for storage expansion. Whenever a virtual disk is connected or disconnected to the virtual host, use the `Storage > Scan` command to detect the storage device or refresh its status.

Note: When creating new disks for disk provisioning, make sure the disk size is a multiple of 0.5 TB, or 512 GB. The appliance can only add a disk when the disk size matches that criteria.

The following procedure describes how to scan the connected storage devices to your appliance from the NetBackup Virtual Appliance Shell Menu.

To scan the storage devices

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main > Manage > Storage` menu, type the following command:

```
Scan
```

When the scan operation is complete, the storage disks and devices information is updated.

See [Manage > Storage > Scan](#) on page 377.

See [“Adding storage space for the NetBackup Virtual Appliance”](#) on page 105.

See [“Removing an existing storage disk”](#) on page 107.

See [“About NetBackup Virtual Appliance storage configuration”](#) on page 89.

See [“About viewing storage space information using the `Show` command”](#) on page 92.

Adding storage space for the NetBackup Virtual Appliance

The following procedure describes how to add space from one or more newly available disks into the unallocated space.

This operation is supported on the following types of NetBackup Virtual Appliance:

- Combined primary and media server for remote offices and branch offices (ROBO)
- Media server for data centers (DC)
- Primary server

Note: The appliance can only add a disk when the disk size is a multiple of 0.5 TB, or 512 GB. You must also select **Thick Provision Lazy Zeroed** as the provisioning format in VMware, and make sure that the **Disk Mode** is set to **Independent - Persistent** for all disks other than the OS disk. For more information on provisioning or the disk mode, refer to the VMware documentation.

To add the storage space from one or more newly available disks

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main > Manage > Storage` view, type the following command:

```
Scan
```

When the scan operation is complete, the storage disk and device information is updated.

- 3 You have the following options for adding disks:

- To use the wizard for adding disks, type the following command:

```
Add
```

This command launches a wizard for adding disks. The wizard lists all the newly available disks with a size that is a multiple of 0.5 TB, and prompts you for a selection. To add multiple disks at one time, use a comma-separated list.

- To add a disk by disk ID, type the following command:

```
ADD [DiskID]
```

Where the `DiskID` is the SCSI ID of the disk. The Disk ID appears when you run the `Show Disk` command. For example, `SCSI(0:2)`. Make sure the disk to be added is a `New Available` disk and the disk size is a multiple of 0.5 TB.

After a disk is added, the total capacity of the disk gets added to the `Unallocated space`.

Warning: Do not modify the disk size after a disk has been added to the appliance; otherwise the appliance may hang when performing storage operations on the modified disk.

See [Manage > Storage > Add](#) on page 363.

See [“Removing an existing storage disk”](#) on page 107.

See [“Scanning storage devices using the NetBackup Virtual Appliance Shell Menu”](#) on page 105.

See [Manage > Storage > Scan](#) on page 377.

Removing an existing storage disk

The following procedure describes how to remove an existing storage disk.

This operation is supported on the following types of NetBackup Virtual Appliance:

- Combined primary and media server for remote offices and branch offices (ROBO)
- Media server for data centers (DC)
- Primary server

Note: Before removing a disk with the status **In Use**, ensure that you move all the partitions on the disk to other disks. You can view the partitions on each disk from the `Manage > Storage > Show Distribution` command output.

See [“Viewing the partition distribution on disks”](#) on page 99.

To remove an existing disk

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main > Manage > Storage` view, type the following command:

```
Remove [DiskID]
```

Where the `DiskID` is the SCSI ID of the disk to be removed from the appliance. The SCSI ID appears when you run the `Show Disk` command.

If the `DiskID` is not specified, the command launches a wizard for removing disks. The wizard lists all the disks with the **In Use** status and prompts you for a selection.

When you remove a disk, the appliance updates the status of this disk to `New Available`. The unallocated space is decreased and updated. You can use the `Storage > Show` command to view the updated information.

See [“About NetBackup Virtual Appliance storage configuration”](#) on page 89.

See [“About viewing storage space information using the `Show` command”](#) on page 92.

About Universal Shares

The Universal Share feature provides data ingest into NetBackup Virtual Appliance using an NFS or a CIFS (SMB) share. Space efficiency is achieved by storing this data directly into an existing NetBackup-based deduplication pool.

You can configure and manage the Universal Share from NetBackup. For more information, see the chapter "Configuring and using universal shares" in the NetBackup Deduplication Guide.

Advantages of Universal Shares

The following information provides a brief description of the advantages for using Universal Shares:

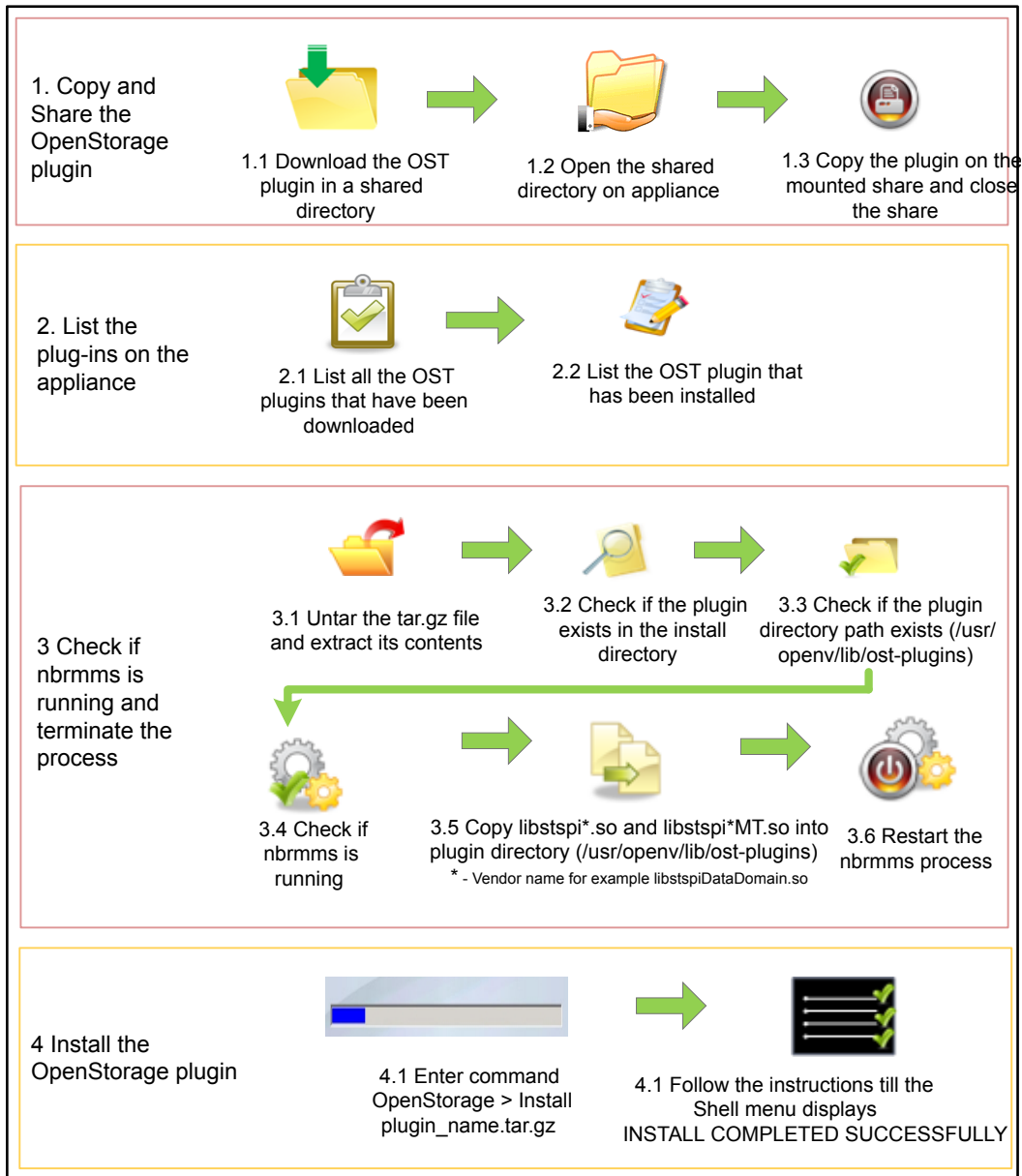
- **As a NAS-based storage target**
Unlike traditional NAS-based storage targets, Universal Shares offer all of the data protection and management capabilities that are provided by NetBackup.
- **As a DB dump location**
Universal Shares offer a space saving (deduplicated) dump location, along with direct integration with NetBackup technologies including data retention, replication, and direct integration with cloud technologies.
- **Financial and time savings**
Universal Shares eliminate the need to purchase and maintain third-party intermediary storage, which typically doubles the required I/O throughput since the data must be moved twice. Universal Shares also cut in half the time it takes to protect valuable application or DB data.
- **Protection Points**
The Universal Share Protection Point offers a fast point in time copy of all data that exists in the share. This copy of the data can be retained like any other data that is protected within NetBackup. All advanced NetBackup data management facilities such as Auto Image Replication, Storage Lifecycle Policies, Optimized Duplication, cloud, and tape are all available with any data in the Universal Share.
- **Copy Data Management (CDM)**
The Universal Share Protection Point also offers powerful CDM tools. A read/write copy of any Protection Point can be "provisioned" or made available through a NAS (CIFS/NFS) based share. A provisioned copy of any Protection Point can be used for common CPD activities, including instant recovery or access of data in the provisioned Protection Point. For example, a DB that has been previously dumped to the Universal Share can be run directly from the provisioned Protection Point.
- **Backup and restore without client software**
Client software is not required for Universal Share backups or for restores to the original source client. However, restoring Universal Share images to an alternate location requires NetBackup client software on the destination client. Universal Shares work with any POSIX-compliant operating system that supports NFS or CIFS.

About OpenStorage plugin installation

You can install and open an OpenStorage (OST) plugin on the NetBackup Virtual Appliance using the NetBackup Virtual Appliance Shell Menu. The OST plugins enable you to install multiple plugins to communicate with their corresponding storage systems.

The following diagram illustrates the process to install the OpenStorage plugin.

Figure 6-2 OpenStorage plugin installation process



See “Installing the OpenStorage plugin” on page 111.

See “Uninstalling the OpenStorage plugin” on page 112.

See [Manage > OpenStorage > Install](#) on page 378.

Installing the OpenStorage plugin

The following procedure describes how to install the OpenStorage (OST) plugin through the NetBackup Virtual Appliance Shell Menu.

To install the OpenStorage plugin

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 Download the latest version of the OST plugin from the required vendor's support Website.
- 3 Open the shared directory. To open the shared directory on the appliance choose from the following commands:

- `Main Menu > Manage > OpenStorage > Share Open`

The appliance displays the following message:

```
The CIFS share \\nbappphostname\general_share
and the NFS share nbappphostname:/inst/share
have been opened on this appliance.
```

- 4 Copy the OST plugin using CIFS or NFS share.
 - 5 Close the shared directory. To close the shared directory use the following command:
- 6 After the plugin is downloaded on the appliance, you can use the list commands to view the plugin details. To view the details of the downloaded plugins choose from the following commands:

- `OpenStorage > List Available`
Displays a list of all the downloaded plugins and not yet applied.

- `OpenStorage > List Installed`
Displays a detailed list of all the installed plugins on the appliance.

- 7 Install the downloaded plugin. To install the downloaded plugin, choose from the following commands based on the appliance you use:

- `OpenStorage > Install plugin_name` to install the OST plugin on media and primary appliances.

The appliance initiates the installation process.

Uninstalling the OpenStorage plugin

The following procedure describes how to uninstall the OpenStorage (OST) plugin through the appliance shell menu.

To uninstall a OpenStorage plugin

- 1 To uninstall the OST plugin use the following command:

```
OpenStorage > Uninstall plugin_name
```

Uninstalls the OST plugin on media and primary appliances.

The appliance initiates the process to uninstall the OST plugin as displayed using the following example:

```
- [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)
```

- 2 Type `yes` to continue and uninstall the plugin.

The appliance displays the following message:

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

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

- 3 Type `yes` to continue and uninstall the plugin.

The appliance continues the uninstall process and displays the following:

```
- Uninstalling the plugin plugin_name.tar.gz      ok  
  
- Successfully uninstalled the plugin plugin_name.tar.gz
```

See [“About OpenStorage plugin installation”](#) on page 109.

See [“Installing the OpenStorage plugin”](#) on page 111.

Deduplication pool catalog backup and recovery

This chapter includes the following topics:

- [About the NetBackup Virtual Appliance deduplication pool catalog backup policy](#)
- [Automatic configuration of the NetBackup Virtual Appliance deduplication pool catalog backup policy](#)
- [Manually configuring the NetBackup Virtual Appliance deduplication pool catalog backup policy](#)
- [Manually updating the NetBackup Virtual Appliance deduplication pool catalog backup policy](#)
- [Recovering the NetBackup Virtual Appliance deduplication pool catalog](#)

About the NetBackup Virtual Appliance deduplication pool catalog backup policy

Creating a backup of the deduplication pool (MSDP) catalog is a very important step in protecting your data in the event of a disaster.

Caution: Veritas recommends that you contact your Veritas Support representative before you recover the deduplication pool catalog. The Support representative can help you determine if you need to recover the catalog or if other solutions are available.

The following topics provide more information about the deduplication pool catalog backup policy and the recovery process:

See [“Automatic configuration of the NetBackup Virtual Appliance deduplication pool catalog backup policy”](#) on page 114.

See [“Manually configuring the NetBackup Virtual Appliance deduplication pool catalog backup policy”](#) on page 115.

See [“Manually updating the NetBackup Virtual Appliance deduplication pool catalog backup policy”](#) on page 116.

See [“Recovering the NetBackup Virtual Appliance deduplication pool catalog”](#) on page 117.

Automatic configuration of the NetBackup Virtual Appliance deduplication pool catalog backup policy

A policy is automatically created to protect the deduplication storage pool. The deduplication pool catalog can then be recovered in the event of a disaster. The deduplication pool catalog backup policy is automatically created during the initial deployment of the appliance.

Veritas recommends that you activate this policy to protect the deduplication pool catalog. Protecting the deduplication pool catalog can prove beneficial in a disaster recovery situation.

When configuring the deduplication storage pool backup policy, take the following into consideration:

- You can adjust properties such as schedules, frequency, and backup window.
- Do not modify the policy type, client name, or backup selection in the policy properties.
- The policy must be activated manually.

The name of this policy is `SYMC_NBA_Dedupe_Catalog_<appliance-short-name>` where `<appliance-short-name>` is the short name you have given to your appliance.

Caution: Veritas recommends that you contact your Veritas Support representative before you recover the deduplication pool catalog. The Support representative can help you determine if you need to recover the catalog or if other solutions are available.

See [“Manually configuring the NetBackup Virtual Appliance deduplication pool catalog backup policy”](#) on page 115.

See [“Manually updating the NetBackup Virtual Appliance deduplication pool catalog backup policy”](#) on page 116.

See [“About the NetBackup Virtual Appliance deduplication pool catalog backup policy”](#) on page 113.

See [“Recovering the NetBackup Virtual Appliance deduplication pool catalog”](#) on page 117.

Manually configuring the NetBackup Virtual Appliance deduplication pool catalog backup policy

The following procedure is provided in case the deduplication pool catalog backup policy is not automatically created. Creating a backup policy to protect the deduplication pool catalog is critical in protecting your data in the event of a disaster.

Manually configuring the deduplication pool catalog backup policy

- 1 Log on to the Appliance with a NetBackupCLI user account.

See [“Creating NetBackup administrator user accounts”](#) on page 176.

- 2 Enter the following command to create the deduplication pool catalog backup policy:

```
# drcontrol --new_policy --policy <policy-name> --OS
'NetBackup-Appliance' --log_file ~/<log file name>
```

- Replace *<policy-name>* with:
SYMC_NBA_Dedupe_Catalog_<appliance-short-name> where
<appliance-short-name> is the short name you have given to your appliance.
- Replace *<log file name>* with the name of the log file the `drcontrol` tool creates.

Note: If the `drcontrol` tool is run without the log file option the tool creates a file that is not accessible to the NetBackupCLI user. Make sure to choose a directory accessible by the NetBackupCLI user, such as the home directory of the NetBackupCLI user.

See [“Automatic configuration of the NetBackup Virtual Appliance deduplication pool catalog backup policy”](#) on page 114.

See [“Manually updating the NetBackup Virtual Appliance deduplication pool catalog backup policy”](#) on page 116.

See [“About the NetBackup Virtual Appliance deduplication pool catalog backup policy”](#) on page 113.

See [“Recovering the NetBackup Virtual Appliance deduplication pool catalog”](#) on page 117.

Manually updating the NetBackup Virtual Appliance deduplication pool catalog backup policy

The following procedure is provided in case the deduplication pool catalog backup policy is not automatically updated. Creating a backup policy to protect the deduplication pool catalog is critical in protecting your data in the event of a disaster.

Manually updating the deduplication pool catalog backup policy

- 1 Log on to the Appliance with a NetBackupCLI user account.

See [“Creating NetBackup administrator user accounts”](#) on page 176.

- 2 Update the policy type. Enter the following command to update the policy type to Standard:

```
# bpplinfo <policy-name> -modify -pt Standard
```

Replace *<policy-name>* with

SYMC_NBA_Dedupe_Catalog_<appliance-short-name> where
 <appliance-short-name> is the short name you have given to your appliance.

- 3 Identify the client name:

- Determine if the appliance is added as a client by entering the following command:

```
# bpplclients <policy-name> -l
```

- If the client has not been added, run the following command to identify the client name:

```
# bpgetconfig CLIENT_NAME | cut -f3 -d' '
```

- 4 Update the client and the backup selection by entering the following command:

```
# drcontrol --update_policy --policy <policy name> --client  

  <client name> --OS 'NetBackup-Appliance' --log_file ~/<log file  

  name>
```

- Replace `<client name>` with the name of the client that is identified in the previous step.
- Replace `<log file name>` with the name of the log file the `drcontrol` tool creates.

Note: If the `drcontrol` tool is run without the log file option the tool creates a file that is not accessible to the NetBackupCLI user. Make sure to choose a directory accessible by the NetBackupCLI user, such as the home directory of the NetBackupCLI user.

See [“Automatic configuration of the NetBackup Virtual Appliance deduplication pool catalog backup policy”](#) on page 114.

See [“Manually configuring the NetBackup Virtual Appliance deduplication pool catalog backup policy”](#) on page 115.

See [“About the NetBackup Virtual Appliance deduplication pool catalog backup policy”](#) on page 113.

See [“Recovering the NetBackup Virtual Appliance deduplication pool catalog”](#) on page 117.

Recovering the NetBackup Virtual Appliance deduplication pool catalog

This section outlines how to recover the deduplication pool catalog in the event of a disaster.

Caution: Veritas recommends that you contact your Veritas Support representative before you recover the deduplication pool catalog. The Support representative can help you determine if you need to recover the catalog or if other solutions are available.

Recovering the deduplication pool catalog

- 1 Log on to the Appliance with a NetBackupCLI user account
See [“Creating NetBackup administrator user accounts”](#) on page 176.

- 2 Enter the following command to identify the space requirements:

```
# drcontrol --print_space_required --policy <policy-name>  
--log_file ~/<log file name>
```

Replace *<log file name>* with the name of the log file the `drcontrol` tool creates.

Note: If the `drcontrol` tool is run without the log file option the tool creates a file that is not accessible to the NetBackupCLI user. Make sure to choose a directory accessible by the NetBackupCLI user, such as the home directory of the NetBackupCLI user.

- 3 Log on to the Appliance as an Appliance Administrator.
- 4 Run a self-test to make sure that everything is functioning correctly.
- 5 Run `Manage > Storage > Show` to make sure that all the storage components are in place and functional. Also verify that the deduplication pool catalog partition size meets the space requirements.
- 6 Log on to the Appliance with a NetBackupCLI user account.
- 7 Perform the catalog recovery using `drcontrol` and other tools as documented in the MSDP catalog recovery section of the *NetBackup Deduplication Guide*.

Note: If the `drcontrol` tool is run without the log file option the tool creates a file that is not accessible to the NetBackupCLI user. Make sure to choose a directory accessible by the NetBackupCLI user, such as the home directory of the NetBackupCLI user.

See [“About disaster recovery”](#) on page 302.

See [“About the NetBackup Virtual Appliance deduplication pool catalog backup policy”](#) on page 113.

See [“Automatic configuration of the NetBackup Virtual Appliance deduplication pool catalog backup policy”](#) on page 114.

See [“Manually configuring the NetBackup Virtual Appliance deduplication pool catalog backup policy”](#) on page 115.

See [“Manually updating the NetBackup Virtual Appliance deduplication pool catalog backup policy”](#) on page 116.

Network connection management

This chapter includes the following topics:

- [About IPv4-IPv6-based network support](#)
- [Network settings for the NetBackup Virtual Appliance](#)
- [Configuring DNS and host name mapping for the NetBackup Virtual Appliance](#)
- [Setting the date and time on a NetBackup Virtual Appliance](#)
- [Configuring static routes on the NetBackup Virtual Appliance](#)
- [Expanding the bandwidth on the NetBackup Virtual Appliance](#)

About IPv4-IPv6-based network support

The NetBackup Virtual Appliance is supported on a dual stack IPv4-IPv6 network and can communicate with IPv6 clients for backups and restores. You can assign an IPv6 address to an appliance, configure DNS, and configure routing to include IPv6 based systems.

Review the following considerations for IPv6 addresses:

- Only global addresses can be used, not addresses with link-local or node-local scope. Global-scope and unique-local addresses are both treated as global addresses by the host.
Global-scope IP addresses refer to the addresses that are globally routable. Unique-local addresses are treated as global.

- You cannot 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`.
- Embedding the IPv4 address within an IPv6 address is not supported. For example, you cannot use an address like `9ffe::10.23.1.5`.
- You can add an appliance media server to the primary server if the IPv6 address and the host name of the appliance media server are available.
 For example, to add an appliance media server to the primary server, enter the IPv6 address of the appliance media server as follows:
 Example:

```
Main > Network > Hosts add 9ffe::45 v45 v45
```

```
Main > Settings > NetBackup AdditionalServers Add v45
```

 You do not need to provide the IPv4 address of the appliance media server.
- A pure IPv6 client is supported in the same way as in NetBackup.
- You can add an IPv6 address of a network interface without specifying a gateway address.

See [Network > IPv6](#) on page 427.

See [Network > IPv4](#) on page 426.

Network settings for the NetBackup Virtual Appliance

You can change the NetBackup Virtual Appliance host, routing, and data transfer optimization settings with the NetBackup Virtual Appliance Shell Menu. Use the following commands to manage these settings:

- Use the `Network > Configure|Unconfigure|IPv4|IPv6` commands to configure or unconfigure an Ethernet port.

Note: Eth0 is reserved for internal use on virtual appliances.

- Use the `Network > Hosts` menu to add, delete, and show the IP address host name mapping.
 See [Network > Hosts](#) on page 425.
- Use the `Network > DNS` menu to add, delete, show, and set the DNS information.
 See [“Configuring DNS and host name mapping for the NetBackup Virtual Appliance”](#) on page 122.

- Use the `Network > Gateway` menu to add, delete, and show the static route information.
See [“Configuring static routes on the NetBackup Virtual Appliance”](#) on page 124.
 - Use the `Network > WANOptimization` menu to enable and disable the WAN Optimization feature.
See [Network > WANOptimization](#) on page 440.
 - Use the `Network > LinkAggregation` commands to manage NIC bonds, and to view the link aggregation information.
See [Network > LinkAggregation](#) on page 428.
- See [“About modifying the NetBackup Virtual Appliance settings”](#) on page 81.

Configuring DNS and host name mapping for the NetBackup Virtual Appliance

The appliance can use both DNS and manual host name mapping for host name resolution. If you configure DNS and then manually add host name entries, the appliance checks the host name entries before searching the DNS.

To configure DNS settings

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main_Menu > Network` view, type the following command to add a DNS name server:

```
DNS Add NameServer <IPAddress>
```

Where *<IPAddress>* is the IP address of the name server. You can add multiple name servers.

- 3 Type the following command to add a DNS search domain:

```
DNS Add SearchDomain <DomainName>
```

Where *<DomainName>* is the target domain for searching. For example:

```
DNS Add SearchDomain mn.us.company.com
```

You can add multiple search domains.

- 4 Type the following command to configure the DNS domain name suffix:

```
DNS Domain <Name>
```

Where *<Name>* is the domain name of the DNS server. For example:

```
DNS Domain mn.us.company.com
```

To manually add a host name

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main_Menu > Network` view, type the following command to manually add a host name:

```
Hosts Add <IPAddress> <FQHN> <ShortName>
```

Where *<IPAddress>*, *<FQHN>*, and *<ShortName>* are the IP address, fully qualified host name, and the short host name of the host.

See [Network > DNS](#) on page 420.

See [Network > Hosts](#) on page 425.

Setting the date and time on a NetBackup Virtual Appliance

You can manually set the time or configure the appliance to use a Network Time Protocol (NTP) server.

Note: Some appliance functionality is dependent on keeping accurate time with the rest of your network environment. Veritas recommends that you use an NTP server for the appliance and any hosts that it interacts with.

To set the date and time

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main_Menu > Network` view, type the following command to set the date and time:

```
Date Set <Month> <Day> <HH:MM:SS> <Year>
```

Where *<Month>* is the first three letters of the month, *<Day>* is the day of the month (1-31), *<HH:MM:SS>* is the hour, minute, and second in a 24-hour format, and *<Year>* is the year in `YYYY` format. For example:

```
Date Set Jun 2 15:12:00 2016
```

- 3 Type the following command to set the time zone:

```
TimeZone Set
```

In the menus that follow, type the numbers that correspond to the continent (or ocean), country, and time zone region where the appliance is located. When you complete your selections, type **yes** to set the time zone.

- 4 (Optional) Type the following command to configure the appliance to use an NTP server:

```
NTPServer Add <Server>
```

Where <Server> is the host name or IP address of the NTP server.

See [“About modifying the NetBackup Virtual Appliance settings”](#) on page 81.

Configuring static routes on the NetBackup Virtual Appliance

You can configure static routes on the appliance to communicate with remote networks or hosts if the default route is not suitable. You can also use static routes to filter traffic to specific network interfaces, or to create a backup routing configuration in case the default gateway fails.

For more information about static routes, refer to the following documentation:

To add a static route

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main_Menu > Network` view, type the following command:

```
Gateway Add <GatewayIPAddress> <TargetNetworkIPAddress> <Netmask>  
<InterfaceName>
```

- **<GatewayIPAddress>** - The IP address leading to the remote network (generally a gateway or router).
- **<TargetNetworkIPAddress>** - The IP address of the destination network or host.
- **<Netmask>** - The subnet mask that corresponds to the address that you specified for **<TargetNetworkIPAddress>**.
- **<InterfaceName>** - The name of the network interface that you want the traffic to exit from.

For example:

```
Gateway Add 192.168.1.1 10.10.0.0 255.255.248.0 eth2
```

See [Network > Gateway](#) on page 422.

See “[Network settings for the NetBackup Virtual Appliance](#)” on page 121.

See “[About modifying the NetBackup Virtual Appliance settings](#)” on page 81.

Expanding the bandwidth on the NetBackup Virtual Appliance

The appliance has the capability to provide link aggregation. Link aggregation increases the bandwidth and availability of the communications channel between the appliance and other devices.

You can use the NetBackup Virtual Appliance Shell Menu to enable or disable link aggregation, as well as view the status of the link aggregation.

Use the following commands to enable, disable, and view the status of link aggregation:

- To enable the network link aggregation:
Main_Menu > Network > LinkAggregation Enable
- To disable the network link aggregation:
Main_Menu > Network > LinkAggregation Disable
- To show the status of the network link aggregation:
Main_Menu > Network > LinkAggregation Status

Managing users

This chapter includes the following topics:

- [About managing NetBackup Virtual Appliance users](#)
- [About NetBackup Virtual Appliance account types](#)
- [Adding NetBackup Virtual Appliance users](#)
- [Deleting NetBackup Virtual Appliance users](#)
- [Adding NetBackup Virtual Appliance user groups](#)
- [Deleting NetBackup Virtual Appliance user groups](#)
- [Granting roles to NetBackup Virtual Appliance users and user groups](#)
- [Revoking roles from NetBackup Virtual Appliance users and user groups](#)
- [About user name and password specifications](#)
- [Changing NetBackup Virtual Appliance user passwords](#)
- [About password management and recovery](#)
- [About authenticating LDAP users](#)
- [About authenticating Active Directory users](#)
- [About authentication using smart cards and digital certificates](#)
- [About authenticating Kerberos-NIS users](#)
- [Generic user authentication guidelines](#)
- [About user authorization on the NetBackup Virtual Appliance](#)
- [Creating NetBackup administrator user accounts](#)

- [Deleting NetBackup administrator user accounts](#)

About managing NetBackup Virtual Appliance users

The NetBackup Virtual Appliance enables you to add new users and create user groups for accessing your appliance. You can directly add local users on the appliance, or register users from an LDAP server, Active Directory (AD) server, or NIS server. Registering remote users offers the benefit of letting you leverage your existing directory service for user management and authentication.

[Table 9-1](#) contains quick links with additional information on managing the appliance users.

Table 9-1

Task	Links
Add and delete local, LDAP, AD, and Kerberos-NIS users	See “Adding NetBackup Virtual Appliance users” on page 131. See “Deleting NetBackup Virtual Appliance users” on page 133.
Add and delete LDAP, AD, and Kerberos-NIS user groups	See “Adding NetBackup Virtual Appliance user groups” on page 134. See “Deleting NetBackup Virtual Appliance user groups” on page 137.
Configure and manage LDAP user authentication	See “About authenticating LDAP users” on page 147.
Configure and manage AD user authentication	See “About authenticating Active Directory users” on page 159.
Configure and manage Kerberos-NIS user authentication	See “About authenticating Kerberos-NIS users” on page 165.
Grant Administrator user permissions to local, LDAP, AD, and Kerberos-NIS users and user groups	See “About the Administrator user role” on page 173. See “Granting roles to NetBackup Virtual Appliance users and user groups” on page 138.

Table 9-1 (continued)

Task	Links
Grant NetBackupCLI user permissions to LDAP, AD, and Kerberos-NIS users and user groups	See “About the NetBackupCLI user role” on page 174. See “Granting roles to NetBackup Virtual Appliance users and user groups” on page 138.
Add and delete local NetBackupCLI users	See “Creating NetBackup administrator user accounts” on page 176. See “Deleting NetBackup administrator user accounts” on page 180.
Revoke user permissions from users and user groups	See “Revoking roles from NetBackup Virtual Appliance users and user groups” on page 139.
Change user passwords	See “Changing NetBackup Virtual Appliance user passwords” on page 145.
Synchronize members of registered user groups.	Use the <code>Settings > Security > Authorization > SyncGroupMembers</code> command. See Settings > Security > Authorization on page 504.

See [“About NetBackup Virtual Appliance account types”](#) on page 128.

About NetBackup Virtual Appliance account types

The NetBackup Virtual Appliance is administered and managed through user accounts. You can create local user accounts, or register users and user groups that belong to a remote directory service. Each user account must authenticate itself with a user name and password to access the appliance. For a local user, the user name and password are managed on the appliance. For a registered remote user, the user name and password are managed by the remote directory service.

In order for a new user account to log on and access the appliance, you must first authorize it with a role. By default, a new user account does not have an assigned role, and therefore it cannot log on until you grant it a role.

[Table 9-2](#) describes the user accounts that are available on the appliance.

Table 9-2 NetBackup Virtual Appliance account types

Account name	Description
admin	The admin account is the default Administrator user on the NetBackup Virtual Appliance. This account provides full appliance access and control for the default Administrator user. New appliances are shipped with the following default logon credentials: ■ User name: admin ■ Password: P@ssw0rd When mounting or mapping shares from an appliance, make note of the following: ■ Linux: Only users with a root access account can issue the mount command directly to mount NFS shares.
AMSadmin	The AMSadmin account provides full access to the following appliance interfaces: ■ Appliance Management Console ■ NetBackup Virtual Appliance Shell Menu ■ NetBackup Administration console For complete details about this account, see the <i>Veritas Appliance Management Guide</i>.
maintenance	The maintenance account is used by Veritas Support through the NetBackup Virtual Appliance Shell Menu (after an administrative log-on). This account is used specifically to perform maintenance activity or to troubleshoot the appliance. Note: This account is also used to make GRUB changes, and for single user mode boot when the STIG option is enabled.

Table 9-2 NetBackup Virtual Appliance account types (*continued*)

Account name	Description
nbasecadmin	The nbasecadmin account is used by the Security Administrator user for role-based access control (RBAC) and managing backup and restore operations in NetBackup. Starting with appliance release 3.1.2, this user is created automatically when you perform the initial configuration on an appliance primary server or when you upgrade an appliance primary server. Once created, this account is assigned the default appliance password. When this user first logs in to the NetBackup Virtual Appliance Shell Menu, they are prompted to change the default password for the account. Note: This user cannot log in to the NetBackup Web UI until the default password is changed. After the default password has been changed, by default, the nbasecadmin user is allowed the following access and privileges: ■ NetBackup Web UI Access to the NetBackup Web UI lets this user set user roles for other NetBackup users, manage all NetBackup security settings, and perform backup and restore operations. The nbasecadmin user can also assign NetBackup roles to local users on the appliance, or to users registered on an LDAP server or Active Directory (AD) server. Note: Starting with software version 3.2, you can assign backup and restore privileges to the nbasecadmin user. If you are upgrading from an earlier version, you must manually add the backup and restore privileges to the nbasecadmin user account. For details, see the <i>NetBackup Web UI Security Administrator's Guide</i>. ■ NetBackup Virtual Appliance Shell Menu Log in to the NetBackup Virtual Appliance Shell Menu to change the password for the account. Access is limited to the <code>Main > Settings > Password</code> view. This view is visible to the nbasecadmin user and all appliance local users that have No Role assigned on the appliance. When the nbasecadmin user is logged in to the shell menu, only the following menu items are available: Exit Password The access rules for the nbasecadmin user can also be changed to allow more privileges. To access the NetBackup Web UI, this user can open a browser window and enter the URL <code>https:<appliance primary server host name>/webui</code>. For more information about RBAC and NetBackup user role management, see the <i>NetBackup Web UI Security Administrator's Guide</i>.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

See [“Adding NetBackup Virtual Appliance users”](#) on page 131.

See [“Adding NetBackup Virtual Appliance user groups”](#) on page 134.

Adding NetBackup Virtual Appliance users

You can use the NetBackup Virtual Appliance Shell Menu to add new users to the appliance. You can add the following types of users:

- Local (native user)
See [“To add a new local user”](#) on page 131.
- LDAP
See [“To add a new LDAP user”](#) on page 131.
- Active Directory (AD)
See [“To add a new AD user”](#) on page 132.
- Kerberos-NIS
See [“To add a new NIS user”](#) on page 133.

Note: If you do not register (add) a remote LDAP, AD, or NIS user with the appliance, that user cannot access the appliance.

The following procedures describe how to add new users to the appliance.

To add a new local user

- 1 Log on to the NetBackup Virtual Appliance Shell Menu as `admin`.
- 2 From the `Main_Menu > Settings > Security > Authentication > LocalUser` view, type the following command:


```
Users Add <username>
```

Where `<username>` is the name for the new user account. You can add multiple users at once with a comma-separated list.
- 3 Enter a password for the new user or users.
- 4 Use the `LocalUser List` command to verify the new user or users.
- 5 Authorize the new user or users with a role. By default, a new user account does not have an assigned role, and therefore it cannot log on until you grant it a role. See [“Granting roles to NetBackup Virtual Appliance users and user groups”](#) on page 138.

To add a new LDAP user

- 1 Make sure that LDAP user authentication is configured on the appliance.
See [“About authenticating LDAP users”](#) on page 147.
- 2 Log on to the NetBackup Virtual Appliance Shell Menu as `admin`.

- 3 From the `Main_Menu > Settings > Security > Authentication > LDAP` view, type the following command:

```
Users Add <username>
```

Where *<username>* is the name of the LDAP user. You can add multiple users at once with a comma-separated list.

Note: Only the users that already exist on the LDAP server can be added to the appliance.

- 4 Use the `LDAP List` command to verify the new user or users.
- 5 Authorize the new user or users with a role. By default, a new user account does not have an assigned role, and therefore it cannot log on until you grant it a role. See [“Granting roles to NetBackup Virtual Appliance users and user groups”](#) on page 138.

To add a new AD user

- 1 Make sure that AD user authentication is configured on the appliance.
See [“About authenticating Active Directory users”](#) on page 159.
- 2 Log on to the NetBackup Virtual Appliance Shell Menu as `admin`.
- 3 From the `Main_Menu > Settings > Security > Authentication > ActiveDirectory` view, type the following command:

```
Users Add <username>
```

Where *<username>* is the name of the AD user. You can add multiple users at once with a comma-separated list.

Note: Only the users that already exist on the AD server can be added to the appliance.

- 4 Use the `ActiveDirectory List` command to verify the new user or users.
- 5 Authorize the new user or users with a role. By default, a new user account does not have an assigned role, and therefore it cannot log on until you grant it a role. See [“Granting roles to NetBackup Virtual Appliance users and user groups”](#) on page 138.

To add a new NIS user

- 1 Make sure that Kerberos-NIS user authentication is configured on the appliance. See [“About authenticating Kerberos-NIS users”](#) on page 165.
- 2 Log on to the NetBackup Virtual Appliance Shell Menu as `admin`.
- 3 From the `Main_Menu > Settings > Security > Authentication > Kerberos` view, type the following command:

```
Users Add <username>
```

Where `<username>` is the name of the NIS user. You can add multiple users at once with a comma-separated list.

Note: Only the users that already exist on the NIS server can be added to the appliance.

- 4 Use the `Kerberos List` command to verify the new user or users.
- 5 Authorize the new user or users with a role. By default, a new user account does not have an assigned role, and therefore it cannot log on until you grant it a role. See [“Granting roles to NetBackup Virtual Appliance users and user groups”](#) on page 138.

See [“Adding NetBackup Virtual Appliance user groups”](#) on page 134.

See [“Creating NetBackup administrator user accounts”](#) on page 176.

See [“Deleting NetBackup Virtual Appliance users”](#) on page 133.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Deleting NetBackup Virtual Appliance users

You can use the NetBackup Virtual Appliance Shell Menu to delete users from the appliance.

Note: As a matter of best practice, you should delete a registered user from the NetBackup Virtual Appliance before deleting it from the LDAP server, Active Directory (AD) server, or NIS server. If a user is removed from the remote directory first (and not removed from appliance), the user is listed as an authorized user but can't log on.

The following procedure describes how to delete users from the appliance.

To delete a user account

- 1 Log on to the NetBackup Virtual Appliance Shell Menu as `admin`.
- 2 Navigate to one of the following views, depending on the type of user that you want to delete:
 - To delete a local (native) user, navigate to the `Main_Menu > Settings > Security > Authentication > LocalUser` view.
 - To delete an LDAP user, navigate to the `Main_Menu > Settings > Security > Authentication > LDAP` view.
 - To delete an AD user, navigate to the `Main_Menu > Settings > Security > Authentication > ActiveDirectory` view.
 - To delete a NIS user, navigate to the `Main_Menu > Settings > Security > Authentication > Kerberos` view.
- 3 Type the following command:


```
Users Remove <username>
```

Where `<username>` is the name of the user account that you want to delete. You can delete multiple users at once with a comma-separated list.

Type **yes** to confirm.
- 4 Use the `List` command from the `LocalUser`, `LDAP`, `ActiveDirectory`, or `Kerberos` view to verify that the user has been removed.

Note: You can also delete all local (native) users at once with the `LocalUser > Clean` command. See [Settings > Security > Authentication > LocalUser](#) on page 498.

See [“Deleting NetBackup Virtual Appliance user groups”](#) on page 137.

See [“Deleting NetBackup administrator user accounts”](#) on page 180.

See [“Adding NetBackup Virtual Appliance users”](#) on page 131.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Adding NetBackup Virtual Appliance user groups

You can use the NetBackup Virtual Appliance Shell Menu to add new user groups to the appliance from a registered directory service. You can add the following types of user groups:

- LDAP
 - See [“To add a new LDAP user group”](#) on page 135.

- Active Directory (AD)
 See [“To add a new AD user group”](#) on page 135.
- Kerberos-NIS
 See [“To add a new NIS user group”](#) on page 136.

Note: If you do not register (add) a remote LDAP, AD, or NIS user group with the appliance, the users belonging to that user group cannot access the appliance.

The following procedures describe how to add new user groups to the appliance.

To add a new LDAP user group

- 1 Make sure that LDAP user authentication is configured on the appliance.
 See [“About authenticating LDAP users”](#) on page 147.
- 2 Log on to the NetBackup Virtual Appliance Shell Menu as `admin`.
- 3 From the `Main_Menu > Settings > Security > Authentication > LDAP` view, type the following command:

```
Groups Add <groupname>
```

Where *<groupname>* is the name of the group. You can add multiple user groups at once with a comma-separated list.

Note: Only the user groups that already exist on the LDAP server can be added to the appliance.

- 4 Use the `LDAP List` command to verify the new user group or groups.
- 5 Authorize the new user group or groups with a role. By default, a new user group does not have an assigned role. Therefore, users belonging to the group cannot log on until you grant it a role. See [“Granting roles to NetBackup Virtual Appliance users and user groups”](#) on page 138.

To add a new AD user group

- 1 Make sure that AD user authentication is configured on the appliance.
 See [“About authenticating Active Directory users”](#) on page 159.
- 2 Log on to the NetBackup Virtual Appliance Shell Menu as `admin`.

- 3 From the `Main_Menu > Settings > Security > Authentication > ActiveDirectory` view, type the following command:

```
Groups Add <groupname>
```

Where *<groupname>* is the name of the group. You can add multiple user groups at once with a comma-separated list.

Note: Only the user groups that already exist on the AD server can be added to the appliance.

- 4 Use the `ActiveDirectory List` command to verify the new user group or groups.
- 5 Authorize the new user group or groups with a role. By default, a new user group does not have an assigned role. Therefore, users belonging to the group cannot log on until you grant it a role. See [“Granting roles to NetBackup Virtual Appliance users and user groups”](#) on page 138.

To add a new NIS user group

- 1 Make sure that Kerberos-NIS user authentication is configured on the appliance. See [“About authenticating Kerberos-NIS users”](#) on page 165.
- 2 Log on to the NetBackup Virtual Appliance Shell Menu as `admin`.
- 3 From the `Main_Menu > Settings > Security > Authentication > Kerberos` view, type the following command:

```
Groups Add <groupname>
```

Where *<groupname>* is the name of the group. You can add multiple user groups at once with a comma-separated list.

Note: Only the user groups that already exist on the NIS server can be added to the appliance.

- 4 Use the `LDAP List` command to verify the new user group or groups.
- 5 Authorize the new user group or groups with a role. By default, a new user group does not have an assigned role. Therefore, users belonging to the group cannot log on until you grant it a role. See [“Granting roles to NetBackup Virtual Appliance users and user groups”](#) on page 138.

See [“Adding NetBackup Virtual Appliance users”](#) on page 131.

See [“Deleting NetBackup Virtual Appliance user groups”](#) on page 137.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

See [Settings > Security > Authentication > LDAP](#) on page 486.

See [Settings > Security > Authentication > ActiveDirectory](#) on page 493.

See [Settings > Security > Authentication > Kerberos](#) on page 495.

Deleting NetBackup Virtual Appliance user groups

You can use the NetBackup Virtual Appliance Shell Menu to delete user groups from the appliance.

Note: As a matter of best practice, you should delete a registered user group from the NetBackup Virtual Appliance before deleting it from the LDAP server, Active Directory (AD) server, or NIS server. If a user is removed from the remote directory first (and not removed from appliance), the user is listed as an authorized user but can't log on.

The following procedure describes how to delete existing user groups from the appliance.

To delete a user group

- 1 Log on to the NetBackup Virtual Appliance Shell Menu as `admin`.
- 2 Navigate to one of the following views, depending on the type of user group that you want to delete:
 - To delete an LDAP user group, navigate to the `Main_Menu > Settings > Security > Authentication > LDAP` view.
 - To delete an AD user group, navigate to the `Main_Menu > Settings > Security > Authentication > ActiveDirectory` view.
 - To delete a NIS user group, navigate to the `Main_Menu > Settings > Security > Authentication > Kerberos` view.

- 3 Type the following command:

```
Groups Remove <groupname>
```

Where `<groupname>` is the name of the group that you want to delete. You can delete multiple user groups at once with a comma-separated list.

Type **yes** to confirm.

- 4 Use the `List` command from the `LDAP`, `ActiveDirectory`, or `Kerberos` view to verify that the user group has been removed.

- See [“Deleting NetBackup Virtual Appliance users”](#) on page 133.
- See [“Adding NetBackup Virtual Appliance user groups”](#) on page 134.
- See [“About managing NetBackup Virtual Appliance users”](#) on page 127.
- See [Settings > Security > Authentication > LDAP](#) on page 486.
- See [Settings > Security > Authentication > ActiveDirectory](#) on page 493.
- See [Settings > Security > Authentication > Kerberos](#) on page 495.

Granting roles to NetBackup Virtual Appliance users and user groups

You can use the NetBackup Virtual Appliance Shell Menu to grant roles to appliance users and user groups and grant them different types of permissions to access the appliance. You can grant the following user roles:

- Administrator
See [“About the Administrator user role”](#) on page 173.
- NetBackupCLI
See [“About the NetBackupCLI user role”](#) on page 174.

The following procedures describe how to grant roles to existing users and user groups.

To grant the Administrator role to a user or a user group

- 1 Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the `Settings > Security > Authorization` view.
- 2 Run one of the following commands, depending on whether you want to grant the Administrator role to a user or a user group:
 - `Grant Administrator Users <username>`, where *<username>* is a local user or a registered user that has been added to the appliance from a configured remote directory service (LDAP, AD, or NIS).
 - `Grant Administrator Groups <groupname>`, where *<groupname>* is a registered user group that has been added to the appliance from a configured remote directory service (LDAP, AD, or NIS).

You can grant roles to multiple users or user groups at once with a comma-separated list.

- 3 Use the `Authorization > List` command to verify the changes.

To grant the NetBackupCLI role to a user or a user group

- 1 Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the `Settings > Security > Authorization` view.
- 2 Run one of the following commands, depending on whether you want to grant the NetBackupCLI role to a user or a user group:
 - `Grant NetBackupCLI Users <username>`, where `<username>` is a registered user that has been added to the appliance from a configured remote directory service (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 `Manage > NetBackupCLI > Create` command. See [“Creating NetBackup administrator user accounts”](#) on page 176.

- `Grant NetBackupCLI Groups <groupname>`, where `<groupname>` is a registered user group that has been added to the appliance from a configured remote directory service (LDAP, AD, or NIS).

You can grant roles to multiple users or user groups at once with a comma-separated list.

- 3 Use the `Authorization > List` command to verify the changes.

See [“Revoking roles from NetBackup Virtual Appliance users and user groups”](#) on page 139.

See [“About user authorization on the NetBackup Virtual Appliance”](#) on page 170.

See [“NetBackup Virtual Appliance user role privileges”](#) on page 171.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Revoking roles from NetBackup Virtual Appliance users and user groups

You can use the NetBackup Virtual Appliance Shell Menu to revoke the Administrator or NetBackupCLI roles from appliance users and user groups to limit their permissions to access the appliance.

The following procedures describe how to revoke roles from existing users and user groups.

To revoke the Administrator role from a user or a user group

- 1 Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the `Settings > Security > Authorization` view.
- 2 Run one of the following commands, depending on whether you want to revoke the Administrator role from a user or a user group:
 - `Revoke Administrator Users <username>`, where *<username>* is the user that you want to revoke permissions from.
 - `Grant Administrator Groups <groupname>`, where *<groupname>* is the user group that you want to revoke permissions from.

You can revoke roles from multiple users or user groups at once with a comma-separated list.
- 3 Use the `Authorization > List` command to verify the changes.

To revoke the NetBackupCLI role from a user or a user group

- 1 Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the `Settings > Security > Authorization` view.
- 2 Run one of the following commands, depending on whether you want to revoke the NetBackupCLI role from a user or a user group:
 - `Revoke NetBackupCLI Users <username>`, where *<username>* is the user that you want to revoke permissions from.
 - `Revoke NetBackupCLI Groups <groupname>`, where *<groupname>* is the user group that you want to revoke permissions from.

You can revoke roles from multiple users or user groups at once with a comma-separated list.
- 3 Use the `Authorization > List` command to verify the changes.

See [“Granting roles to NetBackup Virtual Appliance users and user groups”](#) on page 138.

See [“About user authorization on the NetBackup Virtual Appliance”](#) on page 170.

See [“NetBackup Virtual Appliance user role privileges”](#) on page 171.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

About user name and password specifications

The user name for the NetBackup Virtual Appliance user account must be in the format that the selected authentication system accepts. [Table 9-3](#) lists the user name specifications for each user type.

Note: The `Manage > NetBackupCLI > Create` command is used to create local users with the NetBackupCLI role. All the local user and password specifications apply to these users.

Table 9-3 User name specifications

Description	Administrator (local user)	NetBackupCLI (local user)	Registered remote user
Maximum length	No restrictions applied	No restrictions applied	Determined by the LDAP, AD, or NIS policy
Minimum length	2 characters	2 characters	Determined by the LDAP, AD, or NIS policy
Restrictions	User names must not start with: ■ Number ■ Special character	User names must not start with: ■ Number ■ Special character	Determined by the LDAP, AD, or NIS policy
Space inclusion	User names must not include spaces.	User names must not include spaces.	Determined by the LDAP, AD, or NIS policy

Password specifications

The password for the appliance user account must be in the format that the selected authentication system accepts. [Table 9-4](#) lists the password specifications for each user type.

Table 9-4 Password specifications

Description	Administrator (local user)	NetBackupCLI (local user)	Registered remote user
Maximum length	No restrictions applied	No restrictions applied	Determined by the LDAP, AD, or NIS policy
Minimum length	Passwords must contain at least eight characters.	Passwords must contain at least eight characters.	Determined by the LDAP, AD, or NIS policy

Table 9-4 Password specifications (*continued*)

Description	Administrator (local user)	NetBackupCLI (local user)	Registered remote user
Requirements	- One uppercase letter - One lowercase letter (a-z) - One number (0-9) - Dictionary words are considered as weak passwords and are not accepted. - The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.	- One uppercase letter - One lowercase letter (a-z) - One number (0-9) - Dictionary words are considered as weak passwords and are not accepted. - The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.	Determined by the LDAP, AD, or NIS policy
Space inclusion	Passwords must not include spaces.	Passwords must not include spaces.	Determined by the LDAP, AD, or NIS policy
Minimum password age	0 day	0 day Note: You can manage the user password age using the <code>Settings > Security > Authentication > LocalUser</code> command from the NetBackup Virtual Appliance Shell Menu. See “Managing NetBackup administrator user account passwords” on page 177.	Determined by the LDAP, AD, or NIS policy
Maximum password age	99999 days (doesn't expire)	99999 days (doesn't expire)	Determined by the LDAP, AD, or NIS policy

Table 9-4 Password specifications (*continued*)

Description	Administrator (local user)	NetBackupCLI (local user)	Registered remote user
Password history	The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.	The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.	Determined by the LDAP, AD, or NIS policy
Password expiry	Not applicable as the password does not expire	Use the <code>Settings > Security > Authentication > LocalUser</code> command to manage NetBackupCLI user passwords. See “Managing NetBackup administrator user account passwords” on page 177.	Determined by the LDAP, AD, or NIS policy
Password lockout	None	None	Determined by the LDAP, AD, or NIS policy
Lockout duration	None	None	Determined by the LDAP, AD, or NIS policy

Warning: Appliances do not support Maintenance account passwords such as `passwd`. These types of passwords are overwritten once the system is upgraded. Use the NetBackup Virtual Appliance Shell Menu to change the Maintenance account password.

Password protection

The NetBackup Virtual Appliance uses the following password protection measures:

- The SHA-512 hashing algorithm is used for protecting the passwords of all customer-accessible local appliance users (local users, NetBackupCLI users, the Administrator user, and the Maintenance user). Whenever you create a new local appliance user, or change an existing local appliance user password, the password is hashed using SHA-512.

- The password history is set to 7, meaning that the old passwords are protected and logged up to seven times. If you try to use the old password as the new password, the appliance displays a token manipulation error.
 - Passwords in transit include the following:
 - An SSH login where the password is protected by the SSH protocol.
- See [“Changing NetBackup Virtual Appliance user passwords”](#) on page 145.
- See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

About STIG-compliant password policy rules

To comply with the Security Technical Implementation Guides (STIGs), NetBackup Virtual Appliance automatically enforces a higher security password policy when the STIG option is enabled.

After the STIG option is enabled, all current user passwords that were created under the default policy remain valid. Once you are ready to change any user passwords, the STIG-compliant policy rules must be followed.

The following describes the STIG-compliant password policy rules:

- Minimum characters: 15
- Minimum numbers: 1
- Minimum lowercase characters: 1
- Minimum uppercase characters: 1
- Minimum special characters: 1
- Maximum consecutive repeating characters: 2
- Maximum consecutive repeating characters of the same class: 4
- Minimum number of different characters: 8
- Minimum days for password change: 1
- Maximum days for password change: 60
- Dictionary words are not valid or accepted.
- The last seven passwords cannot be reused

Login lockout enforcement

When the STIG option is enabled, it enforces a login lockout for any user that enters three consecutive incorrect passwords within 15 minutes. The lockout condition is in effect for seven days. To clear a lockout condition, use the `Settings > Security > Authentication > AccountStatus > UnlockAccounts` command.

Maintenance account password changes on STIG-enabled appliances

The STIG password age policy delays maintenance account password changes in the following scenarios:

- For 24 hours, after you enable the STIG option.
- For 24 hours, after you upgrade a STIG-enabled appliance

Any attempt to change the maintenance account password within 24 hours of either of these events results in failure. Make sure that you wait at least 24 hours after these events before you change the maintenance account password.

See [“OS STIG hardening for NetBackup Virtual Appliance”](#) on page 245.

Changing NetBackup Virtual Appliance user passwords

Use the NetBackup Virtual Appliance Shell Menu to change an appliance user's password.

To change a local user password

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main_Menu > Settings > Security > Authentication > LocalUser` view, type the following command:

```
Password <username>
```

Where *<username>* is the name of the user account whose password you want to change.

Note: Only the system Admin user can change other users' passwords. You can use the `Users List` command to show all of the appliance user accounts.

- 3 Enter the existing password and then enter the new password.

To change an admin or a maintenance password

- 1
- Log on to the NetBackup Virtual Appliance Shell Menu as `admin`.
- 2
- From the `Main_Menu > Settings` view, type the following command:

`Password <username>`

Where `<username>` is either `admin` or `maintenance`, depending on the user account whose password you want to change.

- 3
- Enter the existing password and then enter the new password.

See [“About user name and password specifications”](#) on page 140.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

About password management and recovery

You may need to recover the admin password or a user password so that those users can regain appliance access. Password recovery can be done based on the following methods:

Table 9-5 Password recovery for local and LDAP users

User Type	Steps to change password	Password recovery situations and action
Local Users	Use the following command in the NetBackup Virtual Appliance Shell Menu: <code>Settings > Security > Authentication > LocalUser > Password <username>.</code> See “Changing NetBackup Virtual Appliance user passwords” on page 145.	Situations: An employee that maintains the password may leave the company, or you may lose or forget the password. Action: If any of these situations occur, contact Veritas Technical Support for assistance and ask the representative to reference tech note 000115910.

Table 9-5 Password recovery for local and LDAP users (*continued*)

User Type	Steps to change password	Password recovery situations and action
LDAP, Active Directory, or Kerberos-NIS users	Use the following steps to reset or change the password: ■ Update the user password in the Active Directory server, LDAP server, or Kerberos-NIS server. ■ If you need to make changes to the server configuration after you update the password, use the <code>Settings > Security > Authentication</code> commands in the NetBackup Virtual Appliance Shell Menu. See “About managing NetBackup Virtual Appliance users” on page 127.	Situation: An LDAP user leaves the company, or may lose or forget the password. Use the following steps to reset or change the password for an LDAP user: ■ Recover the password using the LDAP server. ■ Contact Veritas Technical Support for changing the password.

See [“Adding NetBackup Virtual Appliance users”](#) on page 131.

See [“Deleting NetBackup Virtual Appliance users”](#) on page 133.

About authenticating LDAP users

The NetBackup Virtual Appliance uses the built-in Pluggable Authentication Module (PAM) plug-in to support the authentication of Lightweight Directory Access Protocol (LDAP) users. This functionality allows users belonging to an LDAP directory service to be added and authorized to log on to a NetBackup Virtual Appliance. LDAP is considered as another type of user directory with a schema installed on it by UNIX services.

Pre-requisites for using LDAP user authentication

The following describes the pre-requisites and requirements for using LDAP user authentication on the appliance:

- The LDAP schema must be RFC 2307 or RFC 2307bis compliant.
- UNIX mode must be enabled on the Active Directory server.
- The following firewall ports must be open:
 - LDAP 389
 - LDAP OVER SSL/TLS 636

- HTTPS 443
- Ensure that the LDAP server is available and is set up with the users and user groups that you want to register with the appliance.

Note: As a best practice, do not use group names or 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.

- The appliance does not handle ID mapping for LDAP configuration. Veritas recommends that you reserve a user ID and group ID range of 1000 to 1999 for appliance users only.

Configuration methods for LDAP user authentication

Before registering new LDAP users and user groups on the appliance, you must configure the appliance to communicate with the LDAP server. Once the configuration is complete, the appliance can access the LDAP server user information for authentication.

2FA

Starting with appliance release 3.2, NetBackup appliances support two-factor authentication (2FA) for Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain users with the NetBackup Web UI. The following describes the 2FA support for the 3.2 release:

- The **nbasesadmin** user or any user with the NetBackup Administrator role can configure 2FA for the NetBackup Web UI.
- 2FA is only supported for AD or LDAP domain users with the NetBackup™ Web UI. The 2FA feature is not currently supported through the NetBackup Virtual Appliance Shell Menu or NetBackup Virtual Appliance Web Console.
- 2FA configuration requires separate AD or LDAP configuration for NetBackup, even if AD or LDAP is already configured on the appliance.
 For details about how to enable 2FA, see the following topic:
 See [“About authentication using smart cards and digital certificates”](#) on page 163.

For detailed instructions on how to configure and manage LDAP user authentication on the appliance, refer to the following topics:

See [“Adding or modifying an LDAP server configuration on the NetBackup Virtual Appliance”](#) on page 149.

See [“Importing an LDAP server configuration for the NetBackup Virtual Appliance”](#) on page 152.

See [“Exporting an LDAP server configuration from the NetBackup Virtual Appliance”](#) on page 154.

See [“Setting the SSL certification for LDAP on the NetBackup Virtual Appliance”](#) on page 153.

See [“Adding an LDAP attribute mapping on the NetBackup Virtual Appliance”](#) on page 158.

See [“Deleting an LDAP attribute mapping on the NetBackup Virtual Appliance”](#) on page 159.

See [“Unconfiguring LDAP user authentication on the NetBackup Virtual Appliance”](#) on page 156.

See [“Disabling LDAP user authentication on the NetBackup Virtual Appliance”](#) on page 157.

See [“Enabling LDAP user authentication on the NetBackup Virtual Appliance”](#) on page 157.

Once LDAP authentication is configured, you can add LDAP users and user groups on the appliance with the `Settings > Security > Authentication > LDAP` commands.

See [“Adding NetBackup Virtual Appliance users”](#) on page 131.

See [“Adding NetBackup Virtual Appliance user groups”](#) on page 134.

See [“Generic user authentication guidelines”](#) on page 168.

See [“About authenticating Active Directory users”](#) on page 159.

See [“About authenticating Kerberos-NIS users”](#) on page 165.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Adding or modifying an LDAP server configuration on the NetBackup Virtual Appliance

Before you can register new LDAP users and user groups on the appliance, you need to configure the appliance to communicate with the LDAP server. The following procedure describes the steps to configure LDAP user authentication or change the parameters if LDAP is already configured.

To add or modify an LDAP server configuration

- 1 Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the `Settings > Security > Authentication > LDAP` view.
- 2 Set the LDAP configuration parameters with the `ConfigParam` command. Enter the configuration information based on the following command options:

* Required parameters

Option	Description
*ConfigParam Set host <server_name or IP>	Enter the FQDN or the IP address of your LDAP server. Note: The specified LDAP server should comply with RFC2307bis. 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 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 userList <user_name(s)>	Enter the name of an existing LDAP user on your LDAP server. To enter multiple users, separate each user name with a comma (.).
ConfigParam Set groupList <group_name(s)>	Enter the name of an existing LDAP user group on your LDAP server. To enter multiple groups, separate each group name with a comma (.).

Option

```
*ConfigParam Set ssl
<No|Yes|StartTLS>
```

Description

Decide between the following SSL certificate options for your LDAP server.

- **No** - Select to continue configuring the LDAP server without the SSL certificate
- **Yes** - Select to enable adding an SSL certificate
- **StartTLS**

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. See [“Setting the SSL certification for LDAP on the NetBackup Virtual Appliance”](#) on page 153.

```
ConfigParam Set
directoryType
<directoryType>
```

Select the LDAP directory type from the drop-down list. The available options are:

- **OpenLDAP**
- **ActiveDirectory**
- **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.

Note: The `userList` and `groupList` options are not required to complete LDAP configuration. However, if you do not configure those options, no LDAP users or LDAP groups appear under the `LDAP > List` command until you manually add them.

If you need to delete a parameter that you have already set, use the `ConfigParam Unset <parameter>` command, where `<parameter>` is the option that you want to delete.

- 3 Verify the information that you entered with the `ConfigParam Show` command.
- 4 If you are adding a new LDAP server configuration, use the `Configure` command to complete the configuration and enable LDAP authentication on the appliance.

See [“Importing an LDAP server configuration for the NetBackup Virtual Appliance”](#) on page 152.

See [“About authenticating LDAP users”](#) on page 147.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

See [“About authenticating Active Directory users”](#) on page 159.

See [“About authenticating Kerberos-NIS users”](#) on page 165.

Importing an LDAP server configuration for the NetBackup Virtual Appliance

You can use the NetBackup Virtual Appliance Shell Menu to import the details of an LDAP server and configure it with the appliance. The following procedure describes the steps to import an `.xml` file that includes the LDAP server configuration details. The appliance configures and connects to the LDAP server using these details.

To import an LDAP server configuration

- 1 Log on to the NetBackup Virtual Appliance Shell Menu as an administrator and enter the following command to open the NFS and the CIFS shares:

```
Main_Menu > Manage > Software > Share Open
```

- 2 Map or mount the appliance share directory as follows:

Windows systems	Map the following appliance CIFS share: <code>\\<appliance-name>\general_share</code>
UNIX systems	Mount the following appliance NFS share: <code><appliance-name>:/inst/share</code>

Note that on Windows systems, you are prompted to provide the user name, `admin`, and its corresponding password.

- 3 Save the LDAP server configuration details as an `.xml` file and copy it to this mapped directory.
- 4 From the NetBackup Virtual Appliance Shell Menu, navigate to the `Settings > Security > Authentication > LDAP` view.
- 5 Import the `.xml` file with the `Import <path>` command, where `<path>` is the absolute path to the `.xml` file.
- 6 Unmap or unmount the directory after you have successfully imported the file.
- 7 Enter the following command to close the NFS and the CIFS shares:

```
Main_Menu > Manage > Software > Share Close
```

See [“Adding or modifying an LDAP server configuration on the NetBackup Virtual Appliance”](#) on page 149.

See [“Exporting an LDAP server configuration from the NetBackup Virtual Appliance”](#) on page 154.

See [“About authenticating LDAP users”](#) on page 147.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Setting the SSL certification for LDAP on the NetBackup Virtual Appliance

You can use the NetBackup Virtual Appliance Shell Menu to import and set the SSL certificate for your LDAP server. The following procedure describes the steps to set the SSL certification for your LDAP server.

Note: The `Certificate Set` option is enabled only after the LDAP server is configured.

See [“Adding or modifying an LDAP server configuration on the NetBackup Virtual Appliance”](#) on page 149.

To set the SSL certificate

- 1 Log on to the NetBackup Virtual Appliance Shell Menu as an administrator and enter the following command to open the NFS and the CIFS shares:

```
Main_Menu > Manage > Software > Share Open
```

- 2 Map or mount the appliance share directory as follows:

Windows systems	Map the following appliance CIFS share: <code>\\<appliance-name>\general_share</code>
UNIX systems	Mount the following appliance NFS share: <code><appliance-name>:/inst/share</code>

Note that on Windows systems, you are prompted to provide the user name, `admin`, and its corresponding password.

- 3 Copy the SSL certificate file from your local computer to this mapped directory.
- 4 From the NetBackup Virtual Appliance Shell Menu, navigate to the `Settings > Security > Authentication > LDAP` view.
- 5 Enter `Certificate Set <filename>`, where `<filename>` is the file name of the SSL certificate in the mapped directory.

The appliance imports the SSL certificate and authenticates the LDAP Server.

Note: The LDAP validation starts only after the server's root certificate is explicitly set with this procedure.

- 6 Unmap or unmount the directory after you have successfully imported the file.
- 7 Enter the following command to close the NFS and the CIFS shares:

```
Main_Menu > Manage > Software > Share Close
```

See [“About authenticating LDAP users”](#) on page 147.

See [Settings > Security > Authentication > LDAP](#) on page 486.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Exporting an LDAP server configuration from the NetBackup Virtual Appliance

You can use the NetBackup Virtual Appliance Shell Menu to export the current LDAP configuration to an `.xml` file. This file can be used to save the LDAP server

configuration details and export them to other appliances. The following procedure describes the steps to export the configuration details of your LDAP server into an .xml file.

Note: The `Export` option is enabled only after the LDAP server is configured.

See [“Adding or modifying an LDAP server configuration on the NetBackup Virtual Appliance”](#) on page 149.

To export the configuration file

- 1 Log on to the NetBackup Virtual Appliance Shell Menu as an administrator and navigate to the `Settings > Security > Authentication > LDAP view`.
- 2 Run the `Export` command to export the existing LDAP configuration as an .xml file.

The file is saved to the appliance share directory.

- 3 Return to the main menu of the NetBackup Virtual Appliance Shell Menu and enter the following command to open the NFS and the CIFS shares:

```
Main_Menu > Manage > Software > Share Open
```

- 4 Map or mount the appliance share directory as follows:

Windows systems	Map the following appliance CIFS share: <code>\\<appliance-name>\general_share</code>
UNIX systems	Mount the following appliance NFS share: <code><appliance-name>:/inst/share</code>

Note that on Windows systems, you are prompted to provide the user name, `admin`, and its corresponding password.

- 5 Copy the configuration file from this mapped directory to your local computer.
- 6 Unmap or unmount the directory after you have successfully copied the file.
- 7 Enter the following command to close the NFS and the CIFS shares:

```
Main_Menu > Manage > Software > Share Close
```

See [“Importing an LDAP server configuration for the NetBackup Virtual Appliance”](#) on page 152.

See [“About authenticating LDAP users”](#) on page 147.

See [Settings > Security > Authentication > LDAP](#) on page 486.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Unconfiguring LDAP user authentication on the NetBackup Virtual Appliance

You can stop authenticating the LDAP users from the appliance. The following procedure describes the steps to unconfigure the LDAP server configuration.

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.

If you want to disable LDAP user authentication without deleting the configuration, use the `Settings > Security > Authentication > LDAP > Disable` command. See [“Disabling LDAP user authentication on the NetBackup Virtual Appliance”](#) on page 157.

To unconfigure an LDAP server

- 1 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.

See [“Revoking roles from NetBackup Virtual Appliance users and user groups”](#) on page 139.

- 2 Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the `Settings > Security > Authentication > LDAP` view.

- 3 Enter the following command to unconfigure LDAP user authentication:

```
Unconfigure
```

The appliance deletes the LDAP settings.

See [“About authenticating LDAP users”](#) on page 147.

See [“Deleting NetBackup Virtual Appliance users”](#) on page 133.

See [“Deleting NetBackup Virtual Appliance user groups”](#) on page 137.

See [“Unconfiguring Active Directory user authentication on the NetBackup Virtual Appliance”](#) on page 162.

See [“Unconfiguring Kerberos-NIS user authentication on the NetBackup Virtual Appliance”](#) on page 168.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Disabling LDAP user authentication on the NetBackup Virtual Appliance

You can use the NetBackup Virtual Appliance Shell Menu to disable LDAP authentication without unconfiguring it. The following procedure describes the options to disable LDAP user authentication.

Note: If you want to unconfigure LDAP user authentication and delete the configuration from the appliance, use the `Settings > Security > Authentication > LDAP Unconfigure` command. See [“Unconfiguring LDAP user authentication on the NetBackup Virtual Appliance”](#) on page 156.

To disable the configured server

- 1 Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the `Settings > Security > Authentication > LDAP view`.
- 2 Enter the following command to disable LDAP user authentication:

```
Disable
```

The appliance disables the LDAP server.

See [“Enabling LDAP user authentication on the NetBackup Virtual Appliance”](#) on page 157.

See [“About authenticating LDAP users”](#) on page 147.

See [Settings > Security > Authentication > LDAP](#) on page 486.

See [“Unconfiguring Active Directory user authentication on the NetBackup Virtual Appliance”](#) on page 162.

See [“Unconfiguring Kerberos-NIS user authentication on the NetBackup Virtual Appliance”](#) on page 168.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Enabling LDAP user authentication on the NetBackup Virtual Appliance

You can use the NetBackup Virtual Appliance Shell Menu to enable a disabled LDAP configuration. The following procedure describes the options to enable the LDAP configuration for user authentication.

Note: When you first configure the LDAP server, it is enabled by default. See [“Adding or modifying an LDAP server configuration on the NetBackup Virtual Appliance”](#) on page 149.

To enable the configured server

- 1 Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the `Settings > Security > Authentication > LDAP` view.
- 2 Enter the following command to enable LDAP user authentication:

```
Enable
```

The appliance enables the LDAP server.

See [“Adding NetBackup Virtual Appliance users”](#) on page 131.

See [“Adding NetBackup Virtual Appliance user groups”](#) on page 134.

See [“Disabling LDAP user authentication on the NetBackup Virtual Appliance”](#) on page 157.

See [“About authenticating LDAP users”](#) on page 147.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Adding an LDAP attribute mapping on the NetBackup Virtual Appliance

When you add a new LDAP configuration, its attribute mappings are added or imported and can be seen with the `LDAP > Map Show` command. The following procedure describes the steps to add a new attribute mapping to the LDAP server configuration.

To add an attribute mapping

- 1 Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the `Settings > Security > Authentication > LDAP` view.

- 2 Enter the following command:

```
Map Add Attribute <attribute type> <attribute value>, where <attribute type> is the mapping type, and <attribute value> is the value for the attribute.
```

For example, `Map Add Attribute uid sAMAccountName`.

- 3 Use the `LDAP > Map Show` command to verify your changes.

See [“Deleting an LDAP attribute mapping on the NetBackup Virtual Appliance”](#) on page 159.

See [“About authenticating LDAP users”](#) on page 147.

See [Settings > Security > Authentication > LDAP](#) on page 486.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Deleting an LDAP attribute mapping on the NetBackup Virtual Appliance

When you add a new LDAP configuration, its attribute mappings are added or imported and can be seen with the `LDAP > Map Show` command. The following procedure describes the steps to delete an attribute mapping from the LDAP server configuration.

To delete an attribute mapping

1 Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the `Settings > Security > Authentication > LDAP view`.

2 Enter the following command:

`Map Delete Attribute <attribute type>`, where *<attribute type>* is the mapping type that you want to delete.

For example, `Map Delete Attribute uid`

3 Use the `LDAP > Map Show` command to verify your changes.

See [“Adding an LDAP attribute mapping on the NetBackup Virtual Appliance”](#) on page 158.

See [“About authenticating LDAP users”](#) on page 147.

See [Settings > Security > Authentication > LDAP](#) on page 486.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

About authenticating Active Directory users

The NetBackup Virtual Appliance uses the built-in Pluggable Authentication Module (PAM) plug-in to support the authentication of Active Directory (AD) users. This functionality allows users belonging to an AD service to be added and authorized to log on to a NetBackup Virtual Appliance. AD is considered as another type of user directory with a schema installed on it by UNIX services.

Pre-requisites for using Active Directory user authentication

The following describes the pre-requisites and requirements for using AD user authentication on the appliance:

- Ensure that the AD service is available and is set up with the users and user groups that you want to register with the appliance.

Note: As a best practice, do not use group names or 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 AD users.

- Ensure that the authorized domain user credentials are used to configure the AD server with the appliance.
- Configure the appliance with a DNS server that can forward DNS requests to an AD DNS server. Alternatively, configure the appliance to use the AD DNS server as the name service data source.

Configuration methods for Active Directory user authentication

Before registering new AD users and user groups on the appliance, you must configure the appliance to communicate with the AD service. Once the configuration is complete, the appliance can access the AD server user information for authentication.

2FA

Starting with appliance release 3.2, NetBackup appliances support two-factor authentication (2FA) for Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain users with the NetBackup Web UI. The following describes the 2FA support for the 3.2 release:

- The **nbasecadmin** user or any user with the NetBackup Administrator role can configure 2FA for the NetBackup Web UI.
- 2FA is only supported for AD or LDAP domain users with the NetBackup™ Web UI. The 2FA feature is not currently supported through the NetBackup Virtual Appliance Shell Menu or NetBackup Virtual Appliance Web Console.
- 2FA configuration requires separate AD or LDAP configuration for NetBackup, even if AD or LDAP is already configured on the appliance.
For details about how to enable 2FA, see the following topic:

See [“About authentication using smart cards and digital certificates”](#) on page 163.
or detailed instructions on how to configure and manage AD user authentication on the appliance, refer to the following topics:

See [“Adding an Active Directory server configuration”](#) on page 161.

See [“Unconfiguring Active Directory user authentication on the NetBackup Virtual Appliance”](#) on page 162.

Once AD authentication is configured, you can add AD users and user groups on the appliance with the `Settings > Security > Authentication > ActiveDirectory` commands.

See [“Adding NetBackup Virtual Appliance users”](#) on page 131.

See [“Adding NetBackup Virtual Appliance user groups”](#) on page 134.

See [“Generic user authentication guidelines”](#) on page 168.

See [“About authenticating LDAP users”](#) on page 147.

See [“About authenticating Kerberos-NIS users”](#) on page 165.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Adding an Active Directory server configuration

This topic describes how to add the details of an Active Directory (AD) server and configure it with your appliance. The Active Directory server enables you to access the directory information services for your appliance. The following procedures describe the steps to configure Active Directory user authentication.

Note: Before you configure new Active Directory authentication, first verify that the DNS of the appliance directs to the Active Directory server or Active Directory DNS server.

To configure an Active Directory server from the NetBackup Virtual Appliance Shell Menu

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 Navigate to the Active Directory view as follows:
`Main_Menu > Settings > Security > Authentication > ActiveDirectory`
- 3 Use the following command to enter the Active Directory fully qualified host name or IP address, then press **Enter**:
`Configure <hostname or IP Address>`
- 4 When the `Username` prompt appears, enter the user name of the AD server Administrator, then press **Enter**.
- 5 When the `Password` prompt appears, enter a password for the AD server Administrator, then press **Enter**.

The message **Command was successful** should appear.

See [“Unconfiguring Active Directory user authentication on the NetBackup Virtual Appliance”](#) on page 162.

See [“About authenticating Active Directory users”](#) on page 159.

See [“About authenticating LDAP users”](#) on page 147.

See [“About authenticating Kerberos-NIS users”](#) on page 165.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Unconfiguring Active Directory user authentication on the NetBackup Virtual Appliance

You can stop authenticating the Active Directory (AD) users from the appliance. The following procedure describes the steps to unconfigure the AD server configuration.

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.

Note: To unconfigure the Active Directory authentication from the appliance, you must have the Administrator authority on the AD server.

To unconfigure an AD server

- 1 Before you unconfigure the AD server, you must revoke the roles from all of the AD users that have been added to the appliance.

See [“Revoking roles from NetBackup Virtual Appliance users and user groups”](#) on page 139.

- 2 Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the `Settings > Security > Authentication > ActiveDirectory` view.

- 3 Enter the following command to unconfigure AD user authentication:

```
Unconfigure
```

The appliance deletes the AD settings.

See [“Adding an Active Directory server configuration”](#) on page 161.

See [“About authenticating Active Directory users”](#) on page 159.

See [“About authenticating LDAP users”](#) on page 147.

See [“About authenticating Kerberos-NIS users”](#) on page 165.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

About authentication using smart cards and digital certificates

The NetBackup Web UI supports authentication of Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain users with a digital certificate or smart card, including CAC and PIV. This authentication method only supports one AD or LDAP domain for each appliance primary server domain and is not available for local domain users. You must configure LDAP for NetBackup, even if LDAP is already configured on the appliance.

Note: Perform this configuration separately for each appliance primary server domain where you want to use this authentication method.

Ensure that you add the AD or the LDAP domain before you add access rules for domain users or configure the domain for smart card authentication. Use the `vssat` command to add AD or LDAP domains.

To add the AD or the LDAP domain for NetBackup

- 1 Log on to the appliance primary server as a NetBackupCLI user.
- 2 Run the `vssat` command.

```
vssat addldapdomain -d DomainName -s server_URL -u user_base_DN
-g group_base_DN -t schema_type -m admin_user_DN
```

Replace the variables in the above command as per the following descriptions:

- *DomainName* is a symbolic name that uniquely identifies an LDAP domain.
- *server_URL* is the URL of the LDAP directory server for the given domain. The LDAP server URL must start with either `ldap://` or `ldaps://`. Starting with `ldaps://` indicates that the given LDAP server requires SSL connection. For example `ldaps://my-server.myorg.com:636`.
- *user_base_DN* is the LDAP-distinguished name for the user container. For example, `ou=user,dc=mydomain,dc=myenterprise,dc=com`.
- *group_base_DN* is the LDAP-distinguished name for the group container. For example, `ou=group,dc=mydomain,dc=myenterprise,dc=com`.
- *schema_type* specifies which type of LDAP schema to use. The two default schema types that are supported are `rfc2307` or `msad`.

- `admin_user_DN` is a string that contains the DN of the administrative user or any user that has search permission to the user container, or user subtree as specified by `UserBaseDN`. If the user container is searchable by anyone including an anonymous user, you can configure this option as an empty string. For example, `--admin_user=`. This configuration allows anyone to search the user container.
- 3** Verify that the specified AD or LDAP domain was successfully added using `vssat validateprpl`. Note that you can also use the `vssat` command with the following options:
- `vssat removeldapdomain` removes an LDAP domain from the authentication broker.
 - `vssat validategroup` checks the existence of a user group in domain provided.
 - `vssat validateprpl` checks the existence of a user in domain provided.

For more details on the `vssat` command, see the *Veritas NetBackup Commands Reference Guide*

Configure role-based access control

After adding the AD and LDAP domains for NetBackup, you can use the `nbasecadmin` user to log on to the NetBackup Web UI and configure role-based access control for the NetBackup web UI. For more information about configuring RBAC for NetBackup Virtual Appliance users, see the *NetBackup Web UI Security Administrator's Guide*.

Configure authentication for a smart card or digital certificate

You can use the `nbasecadmin` user to log on to the NetBackup Web UI and configure authentication for a smart card or digital certificate. Refer to the *NetBackup Web UI Security Administrator's Guide* for steps on performing the following procedures required for the configuration:

- Configure NetBackup Web UI to authenticate users with a smart card or digital certificate.
- Edit the configuration for smart card authentication.
- Add a CA certificate that is used for smart card authentication.
- Delete a CA certificate that is used for smart card authentication.

About authenticating Kerberos-NIS users

The NetBackup Virtual Appliance uses the built-in Pluggable Authentication Module (PAM) plug-in to support the authentication of Network Information Service (NIS) users. This functionality allows users belonging to a NIS directory service to be added and authorized to log on to a NetBackup Virtual Appliance. NIS is considered as another type of user directory with a schema installed on it by UNIX services.

Configuring the appliance to authenticate NIS users requires Kerberos authentication. You must have an existing Kerberos service associated with your NIS domain before you can configure the appliance to register the NIS users.

Pre-requisites for using NIS user authentication with Kerberos

The following describes the pre-requisites and requirements for using NIS user authentication on the appliance:

- Ensure that the NIS domain is available and is set up with the users and user groups that you want to register with the appliance.
- The appliance does not handle ID mapping for NIS configuration. Veritas recommends that you reserve a user ID and group ID range of 1000 to 1999 for appliance users only.

Note: As a best practice, do not use group names or 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 NIS users.

- Ensure that the Kerberos server is available and properly configured to communicate with the NIS domain.
- Due to the strict time requirements in Kerberos, always use an NTP server to synchronize time between the appliance, the NIS server, and the Kerberos server.

Configuration methods for NIS user authentication with Kerberos

Before registering new NIS users and user groups on the appliance, you must configure the appliance to communicate with the NIS server and the Kerberos server. Once the configuration is complete, the appliance can access the NIS domain user information for authentication.

For detailed instructions on how to configure and manage Kerberos-NIS user authentication on the appliance, refer to the following topics:

See [“Adding a Kerberos-NIS authentication configuration on the NetBackup Virtual Appliance”](#) on page 166.

See [“Unconfiguring Kerberos-NIS user authentication on the NetBackup Virtual Appliance”](#) on page 168.

Once Kerberos-NIS authentication is configured, you can add NIS users and user groups on the appliance with the `Settings > Security > Authentication > Kerberos` commands.

See [“Adding NetBackup Virtual Appliance users”](#) on page 131.

See [“Adding NetBackup Virtual Appliance user groups”](#) on page 134.

See [“Generic user authentication guidelines”](#) on page 168.

See [“About authenticating LDAP users”](#) on page 147.

See [“About authenticating Active Directory users”](#) on page 159.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Adding a Kerberos-NIS authentication configuration on the NetBackup Virtual Appliance

Before you can register new NIS users and user groups on the appliance, you need to configure the appliance to communicate with the NIS server and the Kerberos server. The following procedure describes the steps to configure Kerberos-NIS user authentication.

To configure a Kerberos-NIS authentication

- 1
- Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the Settings > Security > Authentication > Kerberos view.
- 2
- Set the Kerberos-NIS configuration parameters with the following command:

Configure NIS *<NIS Server FQDN or IP> <NIS Domain> <Kerberos Server FQDN or IP> <Kerberos Default Realm> [<Kerberos Default Domain>]*.

Refer to the following table for a description of the `Configure NIS` command options:

* Required parameters

Option	Description
<i>*<NIS Server FQDN or IP></i>	Enter the NIS server name or IP address. Veritas recommends that you use the Fully Qualified Domain Name (FQDN) for the NIS server.
<i>*<NIS Domain></i>	Enter the domain for the NIS server.
<i>*<Kerberos Server FQDN or IP></i>	Enter the Kerberos server name or IP address. Veritas recommends that you use the Fully Qualified Domain Name (FQDN) for the Kerberos server.
<i>*<Kerberos Default Realm></i>	Enter the realm for the Kerberos server.
<i>[<Kerberos Default Domain>]</i>	Enter the domain for the Kerberos server.

See [“Unconfiguring Kerberos-NIS user authentication on the NetBackup Virtual Appliance”](#) on page 168.

See [“About authenticating Kerberos-NIS users”](#) on page 165.

See [“About authenticating LDAP users”](#) on page 147.

See [“About authenticating Active Directory users”](#) on page 159.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Unconfiguring Kerberos-NIS user authentication on the NetBackup Virtual Appliance

You can stop authenticating the Kerberos-NIS users from the appliance. The following procedure describes the steps to unconfigure the Kerberos-NIS authentication configuration.

Warning: Unconfiguring Kerberos-NIS user authentication disables and deletes the current Kerberos-NIS configuration. The NIS users are deleted from the appliance, but not from the NIS server.

To unconfigure a Kerberos-NIS authentication

- 1 Before you unconfigure the Kerberos-NIS authentication, you must revoke the roles from all of the NIS users that have been added to the appliance. Otherwise the operation fails.

See [“Revoking roles from NetBackup Virtual Appliance users and user groups”](#) on page 139.

- 2 Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the `Settings > Security > Authentication > Kerberos` view.

- 3 Enter the following command to unconfigure LDAP user authentication:

The appliance deletes the Kerberos-NIS settings.

See [“Adding a Kerberos-NIS authentication configuration on the NetBackup Virtual Appliance”](#) on page 166.

See [“About authenticating Kerberos-NIS users”](#) on page 165.

See [“About authenticating LDAP users”](#) on page 147.

See [“About authenticating Active Directory users”](#) on page 159.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Generic user authentication guidelines

Use the following guidelines for authenticating users on the appliance:

- Only one remote user type (LDAP, Active Directory (AD), or NIS) can be configured for authentication on an appliance. For example, if you currently authenticate LDAP users on an appliance, you must remove the LDAP configuration on it before changing to AD user authentication.
- The NetBackupCLI role can be assigned to a maximum of nine (9) user groups at any given time.

- You cannot grant the NetBackupCLI role to an existing local user. However, you can create a local NetBackupCLI user by using the `Manage > NetBackupCLI > Create` command from the NetBackup Virtual Appliance Shell Menu. See [“Creating NetBackup administrator user accounts”](#) on page 176.
- You cannot add a new user or a user group to an appliance with the same user name, user ID, or group ID as an existing appliance user.
- Do not use group names or 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, AD, or NIS users.
- The appliance does not handle ID mapping for LDAP or NIS configuration. Veritas recommends that you reserve a user ID and group ID range of 1000 to 1999 for appliance users only.
- Starting with appliance software version 4.0, Guest users and existing local users cannot access a Universal Share CIFS. After an upgrade to versions 4.0 and later, you can grant access to a Universal Share CIFS for these users as follows:
 - Guest users: Replace a Guest user by creating a new local user.
 - Existing local users: Change the passwords for these users.
- NetBackup Virtual Appliance uses general CIFS shares for some of its internal operations such as storing patches and installation files, uploading logs to support, forwarding logs to an external server, and uploading OST plug-ins. Starting with appliance software version 4.0, you must manage access to the general CIFS shares for all local users and Active Directory users and user groups (except the **admin** user). Use the `Settings > Security > Authentication > CIFSShare` command to manage access to the general CIFS shares.
 - Guest users: Replace a Guest user by creating a new local user.
 - Existing local users: Change the passwords for these users.

See [“About authenticating LDAP users”](#) on page 147.

See [“About authenticating Active Directory users”](#) on page 159.

See [“About authenticating Kerberos-NIS users”](#) on page 165.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

About user authorization on the NetBackup Virtual Appliance

The NetBackup Virtual Appliance is administered and managed through user accounts. You can create local user accounts, or register users and user groups that belong to a remote directory service. In order for a new user account to log on and access the appliance, you must first authorize it with a role. By default, a new user account does not have an assigned role, and therefore it cannot log on until you grant it a role.

Table 9-6 NetBackup Virtual Appliance user roles

Role	Description
Administrator	A user account that is assigned the Administrator role is provided administrative privileges to manage the NetBackup Virtual Appliance. An Administrator user is allowed to log on, view, and perform all functions on the NetBackup Virtual Appliance Shell Menu. These user accounts have permissions to log on to the appliance and run NetBackup commands with superuser privileges. See “About the Administrator user role” on page 173.
NetBackupCLI	A user account that is assigned the NetBackupCLI role is solely restricted to run a limited set of NetBackup CLI commands and does not have access outside the scope of NetBackup software directories. Once these users log on to the appliance, they are taken to a restricted shell menu from where they can manage NetBackup. The NetBackupCLI users do not have access to the NetBackup Virtual Appliance Shell Menu. See “About the NetBackupCLI user role” on page 174.
AMSadmin	A user account that is assigned the AMSadmin role is provided administrative privileges to access the Appliance Manager that is hosted on the AMS. An AMSadmin user is allowed to perform all the functions on the Appliance Manager and centrally manage multiple appliances. The AMSadmin user cannot log on the NetBackup Virtual Appliance Shell Menu for AMS. An Administrator can create AMSadmin users.

The following list describes some of the characteristics of NetBackup Virtual Appliance authorization:

- Ability to prevent unintended access to the appliance by password protecting logins.
- Access to shared data is provided only to authorized appliance users and NetBackup processes.
- Data that is stored within an appliance cannot inherently protect itself from unintended modification or deletion by a malicious user that knows the admin credentials to the appliance.
- Network access to the NetBackup Virtual Appliance Shell Menu is only allowed through SSH.
- Access to `FTP`, `Telnet`, and `rlogin` are disabled on all appliances.

Note: The NetBackup Virtual Appliance limits login attempts and enforces lockout policies only when the STIG feature is enabled. See [“About STIG-compliant password policy rules”](#) on page 144.

Note: The `Telnet` packaged has been removed from VxOS to comply with the STIG feature when it is enabled on NetBackup Virtual Appliance. The `Telnet` protocol is not secure or encrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The `ssh` package provides an encrypted session and stronger security, and is included in VxOS.

See [“NetBackup Virtual Appliance user role privileges”](#) on page 171.

See [“Granting roles to NetBackup Virtual Appliance users and user groups”](#) on page 138.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

NetBackup Virtual Appliance user role privileges

User roles determine the access privileges that a user is granted to operate the system or to change the system configuration. The user roles that are described in this topic are specific to LDAP, Active Directory (AD), and NIS users.

The following describes the appliance user roles and their associated privileges:

Table 9-7 User roles and privileges

User role	Privileges
NetBackupCLI	Users can only access the NetBackup CLI. See “About the NetBackupCLI user role” on page 174.

Table 9-7 User roles and privileges (continued)

User role	Privileges
Administrator	Users can access the following: - NetBackup Virtual Appliance Shell Menu - NetBackup Administration Console See “About the Administrator user role” on page 173.
AMSadmin	A user account that is assigned the AMSadmin role is provided administrative privileges to access the Appliance Management Console that is hosted on the AMS. An AMS user is allowed to perform all the functions on the Appliance Management Console and centrally manage multiple appliances. The AMS user cannot log on the NetBackup Virtual Appliance Shell Menu for AMS. An Administrator can create AMS users.

A role can be applied to an individual user, or it can be applied to a group that includes multiple users.

A user cannot be granted privileges to both user roles. However, a NetBackupCLI user can also be granted access to the NetBackup Virtual Appliance Shell Menu in the following scenarios:

- The user with the NetBackupCLI role is also in a group that is assigned the Administrator role.
- The user with the Administrator role is also in a group that is assigned the NetBackupCLI role.

Note: When granting a user to have privileges to the NetBackupCLI and the NetBackup Virtual Appliance Shell Menu, an extra step is required. The user must enter the `switch2admin` command from the NetBackup CLI to access the NetBackup Virtual Appliance Shell Menu.

Granting privileges to users and user groups can be done as follows:

- From the NetBackup Virtual Appliance Shell Menu, use the following commands in the `Settings > Security > Authorization` view:


```
Grant Administrator Group
Grant Administrator Users
Grant NetBackupCLI Group
Grant NetBackupCLI Users
```

See [“Granting roles to NetBackup Virtual Appliance users and user groups”](#) on page 138.

See [“About user authorization on the NetBackup Virtual Appliance”](#) on page 170.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

About the Administrator user role

The NetBackup Virtual Appliance provides access control mechanisms to prevent unauthorized access to the backup data on the appliances. These mechanisms include administrative user accounts that provide elevated privileges to modify appliance configurations, monitoring the appliance, and so on. Only the users that are assigned the Administrator role are authorized to configure and manage the NetBackup Virtual Appliance.

The Administrator role should be provided only to authorized system administrators to prevent unauthorized and inappropriate modification of the appliance configuration or the backup data that is contained in the expansion disk storage.

An Administrator user can access the appliance using the NetBackup Virtual Appliance Shell Menu through SSH.

An Administrator user as a superuser can perform all the following tasks:

- Perform appliance initial configuration.
- Monitor SDCS logs.
- Manage licenses.
- Update configuration settings like **Date and Time**, **Network**, **Notification**, etc.
- Apply patches to the appliance.
- Mount or map shares. The following limitations apply:
 - Linux: Only users with a root access account can issue the mount command directly to mount NFS shares.

A local, LDAP, Active Directory (AD), or NIS user needs to have the permissions of the Administrator user role to access and administer the appliance. After you have added a new user or a user group, use the `Settings > Security > Authorization` commands in the NetBackup Virtual Appliance Shell Menu to grant the Administrator user permissions. See [“Granting roles to NetBackup Virtual Appliance users and user groups”](#) on page 138.

- Local users and LDAP or Active Directory (AD) users and user groups assigned with an Administrator role can access the NetBackup Java console.

See [“About the NetBackupCLI user role”](#) on page 174.

See [“NetBackup Virtual Appliance user role privileges”](#) on page 171.

See [“About user authorization on the NetBackup Virtual Appliance”](#) on page 170.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

About the NetBackupCLI user role

A NetBackupCLI user can execute all NetBackup commands, view logs, edit NetBackup touch files, and edit NetBackup notify scripts. NetBackupCLI users are solely restricted to run NetBackup commands with superuser privileges and do not have access outside the scope of NetBackup software directories. Once these users log on, they are taken to a restricted shell from where they can run the NetBackup commands. The NetBackupCLI users share a home directory and do not have access to the NetBackup Virtual Appliance Shell Menu.

The NetBackupCLI role can be assigned to a maximum of nine user groups at any given time. To create a local NetBackupCLI user, use the `Manage > NetBackupCLI > Create` command from the NetBackup Virtual Appliance Shell Menu. For more information, see the *NetBackup Appliance Commands Reference Guide*.

Note: You cannot grant the NetBackupCLI role to an existing local user.

[Table 9-8](#) lists the rights and restrictions of NetBackupCLI users.

Table 9-8 Privileges and restrictions of the appliance NetBackupCLI user

Privileges	Restrictions
The NetBackupCLI user can use the NetBackup Virtual Appliance Shell Menu to do the following: - Run the NetBackup CLI and access the NetBackup directories and files. - Modify or create NetBackup notify scripts using the <code>cp-nbu-notify</code> command. - Run the following NetBackup commands and for the following directories that contain the NetBackup CLI: <code>/usr/opensv/netbackup/bin/*</code> <code>/usr/opensv/netbackup/bin/admincmd/*</code> <code>/usr/opensv/netbackup/bin/goodies/*</code> <code>/usr/opensv/volmgr/bin/*</code> <code>/usr/opensv/volmgr/bin/goodies/*</code> <code>/usr/opensv/pdde/pdag/bin/mtstrmd</code> <code>/usr/opensv/pdde/pdag/bin/pdcfg</code> <code>/usr/opensv/pdde/pdag/bin/pdusercfg</code> <code>/usr/opensv/pdde/pdconfigure/pdde</code> <code>/usr/opensv/pdde/pdcr/bin/*</code>	The following restrictions are placed on NetBackupCLI users: - NetBackupCLI users do not have access outside of the NetBackup software directories. - They cannot edit the <code>bp.conf</code> file directly using an editor. Use the <code>bpsetconfig</code> command to set an attribute. - The <code>cp-nbu-config</code> command supports creating and editing NetBackup touch configuration files only in the <code>/usr/opensv/netbackup/db/config</code> directory. - They cannot use the <code>man</code> or <code>-h</code> command to see the help of any other command.

How to run NetBackup commands as a NetBackupCLI user

Use one of the following methods to run commands as a NetBackupCLI user:

- Restricted shell.
- Absolute path [`sudo`]. For example: `bppllist` or `/usr/opensv/netbackup/bin/admincmd/bppllist`

See [“About running NetBackup commands from the appliance”](#) on page 199.

How to run special directive operations

Special directive operations can fail if the special directive files and commands are not in the correct NetBackup list or path. One example of a special directive operation is when you specify an alternate restore path.

Appliance users that need to run NetBackup commands to access special directive files as a NetBackupCLI user, must do the following to ensure successful operation:

- Add the `/home/nbusers` path to the NetBackup `bpcd` allowed list.
- Add the special directive commands to the `/home/nbusers` directory.

For details about adding entries to the NetBackup `bpcd` allowed list, refer to the `BPCD_WHITELIST_PATH` configuration option in the following documents:

NetBackup Administrator's Guide, Volume 1

NetBackup Commands Reference Guide

See [“Granting roles to NetBackup Virtual Appliance users and user groups”](#) on page 138.

See [“Creating NetBackup administrator user accounts”](#) on page 176.

See [“About the Administrator user role”](#) on page 173.

See [“NetBackup Virtual Appliance user role privileges”](#) on page 171.

See [“About user authorization on the NetBackup Virtual Appliance”](#) on page 170.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Creating NetBackup administrator user accounts

NetBackup Virtual Appliance administrators can use the following procedure to create new NetBackup administrator user accounts. These user accounts have permissions to log on to the appliance and run NetBackup commands with superuser privileges.

To create a NetBackup administrator user account

- 1 Open an SSH session on the appliance.
- 2 Log on as **admin**.
- 3 Enter the following command to create a NetBackup administrator user account:

```
Main > Manage > NetBackupCLI > Create UserName
```

Where *UserName* is the name that you designate for the new user. In addition, you can only create one user account at a time.

- 4 You must then enter a new password for the new user account.

Veritas recommends that the new password is a mix of upper and lowercase letters, digits, and other characters to increase the strength of the password. In addition, you are asked to enter the password a second time for validation purposes.

After the new user account is created, a confirmation message appears stating the new user account was created successfully.

See [“Logging on as a NetBackup administrator”](#) on page 177.

See [“About running NetBackup commands from the appliance”](#) on page 199.

- See [“About the NetBackupCLI user role”](#) on page 174.
- See [“Viewing NetBackup administrator user accounts”](#) on page 179.
- See [“Managing NetBackup administrator user account passwords”](#) on page 177.
- See [“Auditing NetBackup administrator accounts”](#) on page 179.
- See [“Deleting NetBackup administrator user accounts”](#) on page 180.
- See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Logging on as a NetBackup administrator

After a NetBackup administrator account has been created for you, you can log onto the appliance using the new account credentials.

Logging onto an appliance as a NetBackup administrator

- 1 Open an SSH session on the appliance.
- 2 Enter the user name and password that was created for your NetBackup administrator account to log on to the appliance.

The following welcome message appears after you have successfully logged into the appliance as a NetBackup administrator.

```
Welcome NetBackup CLI Administrator to the NetBackup Appliance
```

- 3 To leave the session, type `exit` and press **Return**.
- See [“About running NetBackup commands from the appliance”](#) on page 199.
 - See [“About the NetBackupCLI user role”](#) on page 174.
 - See [“Creating NetBackup administrator user accounts”](#) on page 176.
 - See [“Auditing NetBackup administrator accounts”](#) on page 179.
 - See [“Viewing NetBackup administrator user accounts”](#) on page 179.
 - See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Managing NetBackup administrator user account passwords

After the NetBackup Virtual Appliance administrator has created a NetBackup administrator account, the appliance administrator can manage the password of that account through the NetBackup Virtual Appliance Shell Menu.

[Table 9-9](#) describes the functions that you can perform as you manage your account passwords.

Table 9-9 Managing NetBackup administrator user account passwords

Function	Command
The NetBackup Virtual Appliance administrator can specify a maximum number of days that a password is valid for a user or users.	Main > Manage > NetBackupCLI > PasswordExpiry Age <i>UserName Days</i> You use the <i>Days</i> variable to set the number of days the password is valid. In addition, you use the <i>UserName</i> variable to specify the user or users. Enter <i>All</i> to apply this setting to all users. You can also enter <i>Default</i> to apply this setting to all new users accounts that were created later.
The NetBackup Virtual Appliance administrator can force a password to expire immediately for one or more users.	Main > Manage > NetBackupCLI > PasswordExpiry Now <i>UserName</i> You use the <i>UserName</i> variable to specify the user or users. Enter <i>All</i> to expire the password for all users.
The NetBackup Virtual Appliance administrator can view the password expiry information.	Main > Manage > NetBackupCLI > PasswordExpiry Show <i>UserName</i> You use the <i>UserName</i> variable to specify the user or users. Enter <i>All</i> to expire the password for all users. You can also enter <i>Default</i> to view the default settings.
The NetBackup Virtual Appliance administrator can 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.	Main > Manage > NetBackupCLI > PasswordExpiry Warn <i>UserName Days</i> You use the <i>Days</i> variable to set the number of days or warning before the password expires. In addition, you use the <i>UserName</i> variable to specify the user or users who receive the warning. Enter <i>All</i> to apply the setting to all users. You can also enter <i>Default</i> to specify the default settings.

- See [“About user name and password specifications”](#) on page 140.
- See [“About the NetBackupCLI user role”](#) on page 174.
- See [“Logging on as a NetBackup administrator”](#) on page 177.
- See [“Auditing NetBackup administrator accounts”](#) on page 179.
- See [“Viewing NetBackup administrator user accounts”](#) on page 179.
- See [“Creating NetBackup administrator user accounts”](#) on page 176.
- See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Viewing NetBackup administrator user accounts

NetBackup Virtual Appliance administrators can use the following procedure to view a list of NetBackup administrator user accounts.

To view the current list of NetBackup administrator user accounts

- 1 Open an SSH session on the appliance.
- 2 Log on as **admin**.
- 3 Enter the following command to view the existing user accounts:

```
Main > Manage > NetBackupCLI > List
```

All of the existing user account names appear.

See [Manage > NetBackupCLI > List](#) on page 401.

See [“Logging on as a NetBackup administrator”](#) on page 177.

See [“About the NetBackupCLI user role”](#) on page 174.

See [“Creating NetBackup administrator user accounts”](#) on page 176.

See [“Deleting NetBackup administrator user accounts”](#) on page 180.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Auditing NetBackup administrator accounts

NetBackup Virtual Appliance administrators can monitor the activity of each NetBackup administrator account. That means a NetBackup Virtual Appliance administrator can monitor the NetBackup commands that a NetBackup administrator executes. To audit that activity from the NetBackup Virtual Appliance Shell Menu, the NetBackup Virtual Appliance administrator can run the following command.

```
Main > Support > Logs > Browse > cd OS > less messages.
```

If you run that command, an output similar to the following is shown. The following example shows the NetBackup administrator, `nbadmin`, executed a `bpps` command on an appliance named, `nbappliance`.

```
Aug 24 23:10:28 nbappliance sudo: nbadmin : TTY=pts/1 ;  
PWD=/home/nbusers ; USER=root ; COMMAND=/usr/opensv/netbackup/bin/bpps
```

See [“Creating NetBackup administrator user accounts”](#) on page 176.

See [“Managing NetBackup administrator user account passwords”](#) on page 177.

See [“Deleting NetBackup administrator user accounts”](#) on page 180.

See [“Viewing NetBackup administrator user accounts”](#) on page 179.

See [“About the NetBackupCLI user role”](#) on page 174.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Deleting NetBackup administrator user accounts

NetBackup Virtual Appliance administrators can use the following procedure to delete NetBackup administrator user accounts.

To delete a NetBackup administrator user account

- 1 Open an SSH session on the appliance.
- 2 Log on as **admin**.
- 3 Enter the following command to delete a user account:

```
Main > Manage > NetBackupCLI > Delete UserName
```

Where *UserName* is the name of an existing user account. In addition, you can only delete one user account at a time.

After the user account is deleted, a confirmation message appears that states the user account was deleted successfully.

See [Manage > NetBackupCLI > Delete](#) on page 400.

See [“Viewing NetBackup administrator user accounts”](#) on page 179.

See [“Creating NetBackup administrator user accounts”](#) on page 176.

See [“Deleting NetBackup Virtual Appliance users”](#) on page 133.

See [“About managing NetBackup Virtual Appliance users”](#) on page 127.

Using the appliance

This chapter includes the following topics:

- [About configuring Host parameters for your appliance on the NetBackup Virtual Appliance](#)
- [About Copilot functionality and Share management](#)
- [About NetBackup Virtual Appliance as a VMware backup host](#)
- [About running NetBackup commands from the appliance](#)
- [About mounting a remote NFS](#)
- [About Auto Image Replication from a NetBackup Virtual Appliance](#)
- [Generating certificates](#)

About configuring Host parameters for your appliance on the NetBackup Virtual Appliance

The `Settings > NetBackup Databuffers` commands enables you to view and edit the following NetBackup settings for your appliance:

- Specify Data Buffer parameters
See [“Configuring data buffer options on the NetBackup Virtual Appliance”](#) on page 182.
- Specify Lifecycle parameters
See [“Configuring lifecycle parameters on the NetBackup Virtual Appliance”](#) on page 184.
- Specify Deduplication parameters
- Enable or disable BMR as a server recovery option

See [“About BMR integration”](#) on page 189.

Configuring data buffer options on the NetBackup Virtual Appliance

Note: The `Tape` and `FT` options remain in the NetBackup Virtual Appliance Shell Menu, but they do not apply to the virtual appliance. Modifying those parameters does not affect appliance operation.

You can configure the parameters for the data buffer shared with NetBackup using the `Settings > NetBackup DataBuffers` commands from the NetBackup Virtual Appliance Shell Menu. You can specify the number and size of the following data buffer storage:

- Data buffer tapes
- Data buffer on disks
- Data buffer using Fibre Transport
- Data buffer restore
- Data buffer for NDMP (Network Data Management Protocol)
- Data buffer for multiple copies

The following data buffer parameters can be updated using the appliance shell menu:

Table 10-1 Data Buffer parameters

Data buffer parameters	Description
Data buffer tapes - Number	Specifies the total number of shared data buffer tapes used by NetBackup. The default value is 30.
Data buffer tapes - Size	Specifies the size of each shared data buffer tape in Bytes. The default value is 262144 Bytes.
Data buffer on disks - Number	Specifies the number of shared data buffer disks used by NetBackup. The default value is 30.
Data buffer on disks - Size	Specifies the size of each shared data buffer disks in Bytes. The default value is 262144 Bytes.
Data buffer FT - Number	Specifies the number of shared data buffer FT storage used by NetBackup. The default value is 16.

Table 10-1 Data Buffer parameters (continued)

Data buffer parameters	Description
Data buffer FT - Size	Specifies the size of each shared data buffer FT storage in Bytes. The default value is 262144 Bytes.
Data buffer restore - Number	Specifies the number of shared data buffer restore storage used by NetBackup. The default value is 30.
Data buffer NDMP - Size	Specifies the size of each shared data buffer NDMP (Network Data Management Protocol) storage in Bytes. The default value is 262144 Bytes.
Data buffer multiple copies - Size	Specifies the size of each shared data buffer storage restored in Bytes. The default value is 262144 Bytes.

The following procedure describes how to view and update the data buffer parameters using the `Settings > NetBackup DataBuffers` commands.

To configure data buffer parameters

- Log on to the shell menu.
- Navigate to the `Main > Settings` view. Type the command to specify whether you want to configure the data buffer number or size and which data buffer you want to configure.

For example, to configure data buffers for disks, type the following command, depending on whether you want to configure the data buffer number or size.

```
NetBackup DataBuffers Number Disk <Count>

NetBackup DataBuffers Size Disk <Size>
```

- At any point of time, you can run the following command to show the default and current data buffer numbers and sizes.

```
NetBackup DataBuffers Numbers Defaults

NetBackup DataBuffers Numbers Show

NetBackup DataBuffers Size Defaults

NetBackup DataBuffers Sie Show
```

See [“About configuring Host parameters for your appliance on the NetBackup Virtual Appliance”](#) on page 181.

Configuring lifecycle parameters on the NetBackup Virtual Appliance

You can set the lifecycle parameters using the `Settings > LifeCycle` commands from the NetBackup Virtual Appliance Shell Menu.

[Table 10-2](#) describes the lifecycle parameters that are displayed.

Table 10-2 Lifecycle parameters

Field	Description
CLEANUP_SESSION_INTERVAL	Specifies the time interval after which the deleted life cycle policies should be cleaned up. The default value is 24 hours. You have the following options for the unit to measure the time: - Hour(s) - Second(s) - Minute(s) - Day(s) - Week(s) - Month(s) - Year(s)
DUPLICATION_GROUP_CRITERIA	Specifies the duplication group criteria that is used to define how batches are created. The default value is 1.
IMAGE_EXTENDED_RETRY_PERIOD	Specifies the interval period till NetBackup waits before an image copy is added to the next duplication job. The default value is 2 hours. You have the following options for the unit to measure the time: - Hour(s) - Second(s) - Minute(s) - Day(s) - Week(s) - Month(s) - Year(s)

Table 10-2 Lifecycle parameters (continued)

Field	Description
JOB_SUBMISSION_INTERVAL	Specifies the frequency of job submission for all operations. The default value is 5 minutes. By default, all jobs are processed before more jobs are submitted. Increase this interval to allow NetBackup to submit more jobs before all jobs are processed. You have the following options for the unit to measure the time: - Hour(s) - Second(s) - Minute(s) - Day(s) - Week(s) - Month(s) - Year(s)
MAX_SIZE_PER_DUPLICATION_JOB	Specifies the maximum size up to which the batch of images is allowed to grow. The default value is 100 GB. You have the following options for the unit to measure the size: - Byte(s) - KB - MB - GB - TB - PB
MAX_TIME_TIL_FORCE_SMALL_DUPLICATION_JOB	Specifies the time to determine how old any image in a group can become before the batch is submitted as a duplication job. The default value is 30 minutes. You have the following options for the unit to measure the time: - Hour(s) - Second(s) - Minute(s) - Day(s) - Week(s) - Month(s) - Year(s)

Table 10-2 Lifecycle parameters (continued)

Field	Description
MIN_SIZE_PER_ DUPLICATION_JOB	Specifies the minimum size up to which the batch of images should reach before a duplication job is run for the entire batch. The default value is 8 GB. You have the following options for the unit to measure the size: - Byte(s) - KB - MB - GB - TB - PB
REPLICA_METADATA_ CLEANUP_TIMER	Specifies the number of days after which the Import Manager stops trying to import the image. The default value is 0 hours. You have the following options for the unit to measure the time: - Hour(s) - Second(s) - Minute(s) - Day(s) - Week(s) - Month(s) - Year(s)
TAPE_RESOURCE_ MULTIPLIER	Specifies the multiplier for the number of concurrently active duplication jobs that can access a single storage unit. The default value is 2.
VERSION_CLEANUP_ DELAY	Specifies the number of hours to determine how much time must pass since an inactive version was the active version. The default value is 14 days. You have the following options for the unit to measure the time: - Hour(s) - Second(s) - Minute(s) - Day(s) - Week(s) - Month(s) - Year(s)

To configure lifecycle parameters

- 1 Log on to the shell menu.
- 2 Navigate to the `Settings > Lifecycle` view. Type the command to specify which lifecycle parameter you want to tune, the parameter value, and the unit, if applicable.

For example, to configure the lifecycle parameter `CLEANUP_SESSION_INTERVAL`, type the following command:

```
Tune CLEANUP_SESSION_INTERVAL <Interval> <Unit>
```

- 3 At any point of time, you can run the following command to show the default and current lifecycle parameter configurations.

```
Defaults
```

```
Show
```

Managing NetBackup Virtual Appliance deduplication

You can set the deduplication parameters using the `Settings> Deduplication` menu in the NetBackup Virtual Appliance Shell Menu. Use this menu to show current values, display default values, tune the deduplication parameters, as well as other menu choices.

Use the `Deduplication > Default` command and the `Deduplication > Show` command to display the default values for each of the deduplication parameters and the current parameter values, respectively.

You can change the media server deduplication parameters using the `Deduplication> Tune` menu. [Table 10-3](#) shows the fields and their descriptions.

Table 10-3 Deduplication > Tune fields

Field	Description
BACKUPRESTORERANGE	Enter the IP address or range of addresses of the local network interface card (NIC) for maintaining backups and restores.
BANDWIDTH_LIMIT	Enter the maximum bandwidth that is allowed when backing up or restoring data to the deduplication pool.
COMPRESSION	Select to compress the data. By default, the files are not compressed.

Table 10-3 Deduplication > Tune fields (continued)

Field	Description
DONT_SEGMENT_TYPES	The file types within which NetBackup do not analyze and manage segments.
ENCRYPTION	Enable this option to encrypt data that is written directly to this media server, or from an MSDP pool which also has the ENCRYPTION or the MSDP ENCRYPTION option enabled. By default, this option is disabled.
LOCAL_SETTINGS	Determines if the settings of the deduplication server override the local settings.
LOGLEVEL	Select the amount of information to be written to the log file. You can select from the values 0 to 10, with 10 being the maximum information that can be logged. Note: Change this value only when directed to do so by a Veritas representative.
MAX_IMG_MBSIZE	Enter the maximum backup image fragment size in megabytes. Note: Change this value only when directed to do so by a Veritas representative.
MAX_LOG_MBSIZE	Enter the maximum size of the log file in megabytes.
MSDP_ENCRYPTION	Enable this option to encrypt all data that is written to the MSDP pool, regardless of the source. When enabled, this option overrides the Encryption option. By default, this option is disabled.
OPTDUP_BANDWIDTH	Enter the maximum bandwidth that is allowed when backing up or restoring optimized deduplication data.
OPTDUP_COMPRESSION	Select to compress optimized duplication data. By default, the files are not compressed.

Table 10-3 Deduplication > Tune fields (continued)

Field	Description
OPTDUP_ENCRYPTION	Use this option to encrypt the optimized deduplication data. By default, files are not encrypted. When you enable this option the data is encrypted during transfer and on the storage.
OPTDUP_TIMEOUT	The number of minutes before the optimized duplication times out.
SEGKSIZE	The file segment size
WS_RETRYCOUNT	Enter the number of retries that can be attempted in case the Web service fails out or times out. Note: This parameter applies to the PureDisk Deduplication Option only. It does not affect NetBackup deduplication.
WS_TIMEOUT	Enter the parameter to increase or decrease the time-out value for Web service calls made from NetBackup media servers to PureDisk storage units. Note: This parameter applies to the PureDisk Deduplication Option only. It does not affect NetBackup deduplication.

See [“About configuring Host parameters for your appliance on the NetBackup Virtual Appliance”](#) on page 181.

See [“About modifying the NetBackup Virtual Appliance settings”](#) on page 81.

About BMR integration

Bare Metal Restore (BMR) is the Server Recovery option of NetBackup. BMR automates and streamlines the server recovery process, making it unnecessary to manually reinstall Operating Systems or configure hardware. With simple commands, complete server restores can be accomplished in a fraction of the time without extensive training or tedious administration.

Note: Please be aware that for the NetBackup Virtual Appliance BMR is disabled by default.

BMR allows the recovery of:

- Windows systems to completely different hardware (Dissimilar System Recovery or DSR)
- UNIX/Linux systems to disks of varying geometry (Dissimilar Disk Recovery or DDR)

See the *BMR Administrator's Guide* for more information.

Note: A NetBackup Virtual Appliance cannot be used as a BMR boot server. This convention is unlike NetBackup, where you can use any primary server, media server, or client as a BMR boot server. Your boot server can be any non-appliance NetBackup platform with the same operating system as the hosts that are to be recovered.

See [“Enabling BMR from the NetBackup Virtual Appliance Shell Menu”](#) on page 190.

See [“About configuring Host parameters for your appliance on the NetBackup Virtual Appliance”](#) on page 181.

See [“About modifying the NetBackup Virtual Appliance settings”](#) on page 81.

Enabling BMR from the NetBackup Virtual Appliance Shell Menu

If you want to enable BMR on the appliance, you must run the appropriate commands. Note that BMR is disabled by default.

To enable BMR from the NetBackup Virtual Appliance Shell Menu

- 1 Create a NetBackup administrator user account.
See [“Creating NetBackup administrator user accounts”](#) on page 176.
- 2 Log out of the NetBackup Virtual Appliance Shell Menu.
- 3 Log back into the NetBackup Virtual Appliance Shell Menu using the new NetBackup Virtual Appliance Shell Menu user credentials you created.
- 4 Enable BMR with the command shown:

```
/usr/opensv/netbackup/bin/bmrsetupprimary
```

See [“About BMR integration”](#) on page 189.

See [“About configuring Host parameters for your appliance on the NetBackup Virtual Appliance”](#) on page 181.

See [“About modifying the NetBackup Virtual Appliance settings”](#) on page 81.

About Copilot functionality and Share management

Note: The Copilot feature is only supported on a NetBackup Virtual Appliance with the media server role.

Copilot integrates with native Oracle tools and processes to give database backup administrators more control, visibility, and the ability to recover their database backups. Backup administrators can then manage policies, move the data to different storage types, and create off-site backup copies of the database backups.

Additionally, Copilot features NetBackup Accelerator technology to boost Oracle backup and restore performance. NetBackup Accelerator integrates with Oracle's incremental merge capabilities to eliminate the need for full backups and allow new full database images to be synthesized on backup storage post-process.

Copilot lets you create shares on the appliance for Oracle backup and recovery and create further protection policies in NetBackup for advanced data protection features like long-term retention, replication, and NetBackup Oracle Accelerator technology. Copilot is exclusive to the appliance but requires additional configuration steps within NetBackup software.

Note: The Copilot feature is not supported for use in high availability (HA) configurations.

Copilot configuration overview

To configure Copilot functionality, the following steps must be completed:

- Create a Share on the appliance using the NetBackup Virtual Appliance Shell Menu.
- Mount the appliance share on the Oracle server.
- Configure a Storage Lifecycle Policy (SLP) and Oracle Intelligent Policy (OIP) using NetBackup Administration Console.

Refer to the *NetBackup Copilot for Oracle Configuration Guide* for the entire configuration process.

Share management

Shares can be created, modified, viewed, and deleted through the use of the shell menu. Use the following topics as a guide to managing your Shares.

- See [“Viewing Share information from the NetBackup Virtual Appliance Shell Menu”](#) on page 196.

Refer to the NetBackup Virtual Appliance commands chapter for more specific details about the command.

Refer to the *NetBackup™ for Oracle Administrator's Guide* for more information on Copilot in NetBackup software.

Creating a Share

Note: The Copilot feature is only supported on a NetBackup Virtual Appliance with the media server role.

The following procedure explains how to create a Standard Share from the shell menu.

Creating a Standard Share from the NetBackup Virtual Appliance Shell Menu

To create a new Share from the shell menu

- 1 Open an SSH session to log on to the appliance as an administrator.
- 2 From the `Main_Menu > Manage > Storage` view, enter the following command to create a Standard Share:

```
Create Share Standard
```

The command guides you through the process of configuring a new Share.

- 3 Enter the Share name, for example `share_1`.
- 4 Enter a short description for the Share, for example `Test for share_1`.
- 5 Enter the allocated capacity for the Share, for example `5GB`.
- 6 Enter a comma-separated list of Oracle server clients that can access the Share, for example `10.100.0.2, 10.100.0.3`.

Note: Client names can be entered using the short name, the FQDN, or the IP format.

- 7 Enter the NFS export options for each of the Oracle clients. You are prompted to enter options for each client you added in the previous step.

See [“NFS export options”](#) on page 196.

- 8 Once you have entered the NFS export options, a summary is displayed.
- 9 Enter `yes` to create the Share. A series of messages are displayed as the Share is created.

See [“About Copilot functionality and Share management”](#) on page 191.

Refer to the *NetBackup™ Copilot™ for Oracle Configuration Guide* for more information on configuring Oracle database backups.

Refer to the *NetBackup™ for Oracle Administrator's Guide* for more information on Copilot in NetBackup software.

Editing a Share

Note: The Copilot feature is only supported on a NetBackup Virtual Appliance with the media server role.

The following procedures explain how to edit a Share from the shell menu. You can edit the description, size, clients, and NFS options of the clients.

- [Editing a Share from the NetBackup Virtual Appliance Shell Menu](#)
- [Resizing a Share from the NetBackup Virtual Appliance Shell Menu](#)

Editing a Share from the NetBackup Virtual Appliance Shell Menu

The following procedures explain how to edit a Share from the NetBackup Virtual Appliance Shell Menu.

To edit a Share description from the shell menu

- 1 Open an SSH session to log on to the appliance as an administrator.
- 2 Enter `Main_Menu > Manage > Storage > Edit Share Description <ShareName>`.
- 3 Enter a new Share description, then press Enter to view a summary of the edit.
- 4 Enter `yes` to complete the edit process.

The following procedure explains how to add a client to a Share from the shell menu.

To add a client to a Share from the shell menu

- 1 Open an SSH session to log on to the appliance as an administrator.
- 2 Enter `Main_Menu > Manage > Storage > Edit Share Clients Add <ShareName>`.

- 3 Enter the clients you want to add, then press Enter.
- 4 Enter the NFS export options for each client. Press Enter to move to the next client. When you are finished, the summary is displayed.
- 5 Enter `yes` to complete the edit process.

The following procedure explains how to update the clients of a Share from the shell menu.

To update the clients of a Share from the shell menu

- 1 Open an SSH session to log on to the appliance as an administrator.
- 2 Enter `Main_Menu > Manage > Storage > Edit Share <ShareName> Clients Update.`
- 3 Enter the clients you want to update, then press Enter.
- 4 Enter the NFS export options for each updated client. Press Enter to move to the next client. When you are finished the summary is displayed.
- 5 Enter `yes` to complete the edit process.

The following procedure explains how to delete clients from a Share from the shell menu.

To delete clients from a Share from the shell menu

- 1 Open an SSH session to log on to the appliance as an administrator.
- 2 Enter `Main_Menu > Manage > Storage > Edit Share <ShareName> Clients Delete.`
- 3 Enter the clients you want to delete, then press Enter to delete the clients.
- 4 Enter `yes` to complete the edit process.

Resizing a Share from the NetBackup Virtual Appliance Shell Menu

The following procedure explains how to resize a Share from the NetBackup Virtual Appliance Shell Menu.

To resize a Share from the shell menu

- 1 Open an SSH session to log on to the appliance as an administrator.
- 2 Enter `Main_Menu > Manage > Storage > Resize Share <Size> <Unit> <ShareName>` then press Enter.

Note: The Share is resized to the new size that you enter. It is not added or subtracted from the current size.

- 3 Type `yes`, then press Enter to complete the resize operation.

See [“About Copilot functionality and Share management”](#) on page 191.

Deleting a Share

Note: The Copilot feature is only supported on a NetBackup Virtual Appliance with the media server role.

The following procedure explains how to delete a Share from the shell menu.

Deleting a Share from the NetBackup Virtual Appliance Shell Menu

The following procedure explains how to delete a Share from the NetBackup Virtual Appliance Shell Menu.

To delete a Share using the shell menu

- 1 Open an SSH session to log on to the appliance as an administrator.
- 2 Enter `Main_Menu > Manage > Storage > Delete Share <ShareName>`.
- 3 Enter `yes` to delete the Share.

See [“About Copilot functionality and Share management”](#) on page 191.

See [“About Universal Shares”](#) on page 107.

Moving a Share

Note: The Copilot feature is only supported on a NetBackup Virtual Appliance with the media server role.

The following procedures explain how to move a Share from the shell menu.

Moving a Share from the NetBackup Virtual Appliance Shell Menu

The following procedure explains how to move a Share from the NetBackup Virtual Appliance Shell Menu.

To move a Share using the shell menu:

- 1 Open an SSH session to log on to the appliance as an administrator.
- 2 Enter `Main_Menu > Manage > Storage > Move Share <Share_Name> <SourceDiskID> <TargetDiskID> <Size> <Unit>`
- 3 Enter `yes` to move the Share.

Refer to the NetBackup Virtual Appliance commands chapter for more specific details about the command.

Viewing Share information from the NetBackup Virtual Appliance Shell Menu

Note: The Copilot feature is only supported on a NetBackup Virtual Appliance with the media server role.

The following procedure explains how to view Share information using the shell menu.

To view Share partition information using the shell menu:

- 1 Open an SSH session to log on to the appliance as an administrator.
- 2 Enter `Main_Menu > Manage > Storage > Show Partition All Share`.

Refer to the NetBackup Virtual Appliance commands chapter for more specific details about the command.

See [“About viewing storage space information using the `Show` command”](#) on page 92.

NFS export options

Note: The CoPilot feature is only supported on a NetBackup Virtual Appliance with the media server role.

The following table describes the export options available for Share creation or modification.

Option	Description
<code>ro</code>	Allows only read requests on the Share.
<code>rw</code>	Allows both read requests and write requests on the Share.
<code>no_root_squash</code>	Disables all root squashing. Allows root account on client to access export share on server as the root account.
<code>root_squash</code>	Maps requests from UID and GID 0 to the anonymous UID and GID.
<code>all_squash</code>	Maps all UIDs and GIDs to the anonymous user account. By default, the NFS server chooses a UID and GID of 65534 for squashed access. These values can be overridden by using the <code>anonuid</code> and <code>anongid</code> options.
<code>anonuid</code>	Sets the <code>uid</code> of the anonymous user account. This option forces all anonymous connections to a predefined UID on a server.
<code>anongid</code>	Sets the <code>gid</code> of the anonymous account. This option forces all anonymous connections to a predefined GID on a server.
<code>secure</code>	Requires that requests originate from an Internet port less than <code>IPPORT_RESERVED</code> (1024).
<code>insecure</code>	Disables the requirement that requests originate from an Internet port less than <code>IPPORT_RESERVED</code> (1024).

About NetBackup Virtual Appliance as a VMware backup host

NetBackup Virtual Appliance uses the VMware policy type to back up VMware virtual machines.

The following topics contain notes on the appliance as the backup host:

- For an overview of the appliance as backup host in a virtual environment:
See [“NetBackup Virtual Appliance as backup host: component overview”](#) on page 198.
- For a list of requirements and limitations:
See [“Notes on NetBackup Virtual Appliance as a VMware backup host”](#) on page 198.

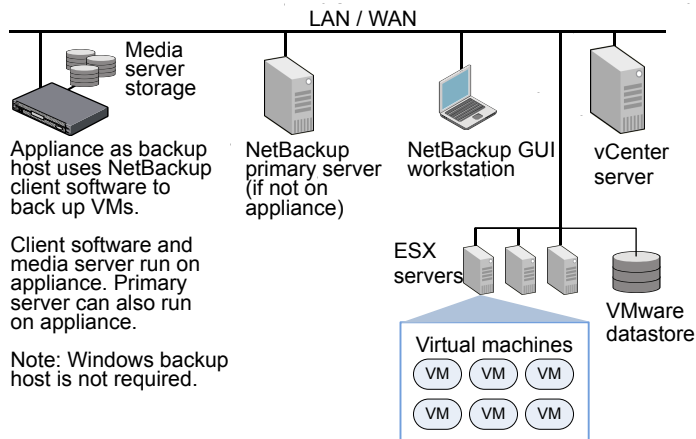
- For further information, see the latest *NetBackup for VMware Administrator's Guide*:
<http://www.veritas.com/docs/DOC5332>

NetBackup Virtual Appliance as backup host: component overview

As [Figure 10-1](#) shows, the appliance can operate as the VMware backup host. A separate Windows backup host is not required.

The appliance as backup host can also run the NetBackup media server and primary server.

Figure 10-1 NetBackup for VMware with appliance as backup host



Further information is available on the appliance as backup host:

See ["Notes on NetBackup Virtual Appliance as a VMware backup host"](#) on page 198.

Notes on NetBackup Virtual Appliance as a VMware backup host

Note the following requirements and limitations for the appliance as the backup host:

- The appliance supports vSphere versions 6.5, 6.7, 7.0, and 7U1.
- You must use the VMware policy type.
- NetBackup Virtual Appliance does not support SAN transport for VMware policies. The appliance supports the following transport modes:
 - HotAdd

- NBD
- NBDSSL

See [“NetBackup Virtual Appliance as backup host: component overview”](#) on page 198.

About running NetBackup commands from the appliance

The NetBackup command-line shell feature enables NetBackup administrators to execute NetBackup commands with superuser privileges. These privileges enable NetBackup administrators to execute the commands that support full NetBackup logging as well as develop and use scripts and automation.

NetBackup Virtual Appliance administrators can provide access for multiple NetBackup administrators and audit the activity of these administrators. In addition, NetBackup Virtual Appliance administrators can manage the NetBackup administrator accounts from the `Main > Manage > NetBackupCLI` view within the NetBackup Virtual Appliance Shell Menu. From the `NetBackupCLI` view, a NetBackup Virtual Appliance administrator can create, delete, and list NetBackup administrator accounts as well as manage their user account passwords.

See [“About the NetBackupCLI user role”](#) on page 174.

See [“Creating NetBackup administrator user accounts”](#) on page 176.

See [“Running NetBackup commands from the NetBackup Virtual Appliance”](#) on page 199.

See [“Creating a NetBackup touch file from the NetBackup Virtual Appliance”](#) on page 200.

See [“Best practices for running NetBackup commands from the NetBackup Virtual Appliance”](#) on page 201.

See [“Known limitations of running NetBackup commands from the NetBackup Virtual Appliance”](#) on page 202.

Running NetBackup commands from the NetBackup Virtual Appliance

NetBackup administrators can use multiple methods to execute NetBackup commands from the restricted NetBackup Virtual Appliance shell. NetBackup administrators can use a base command name, an absolute or a relative path, or execute commands from shell scripts.

The following are examples of how a NetBackup administrator can run NetBackup commands from the restricted NetBackup Virtual Appliance shell:

- Using a base command name. For example,
 - # `bpps`
 - # `nbsmmcmd -listhosts`
 - Using an absolute or a relative path. You must specify `sudo` before the command in this case. For example,
 - # `sudo /usr/opensv/netbackup/bin/bpps`
 - # `sudo /usr/opensv/netbackup/bin/admincmd/nbsmmcmd -listhosts`
 - Execute from shell scripts. You must specify `sudo` before you use a command. That applies to a base command name, an absolute path, or a relative path.
- See [“Creating a NetBackup touch file from the NetBackup Virtual Appliance”](#) on page 200.
- See [“About NetBackup operating system commands”](#) on page 202.
- See [“Best practices for running NetBackup commands from the NetBackup Virtual Appliance”](#) on page 201.
- See [“Known limitations of running NetBackup commands from the NetBackup Virtual Appliance”](#) on page 202.
- See [“About the NetBackupCLI user role”](#) on page 174.

Creating a NetBackup touch file from the NetBackup Virtual Appliance

A NetBackup administrator can use the `cp-nbu-config` command to create and edit a NetBackup touch configuration file in any of the following directories:

- `/usr/opensv/netbackup`
- `/usr/opensv/netbackup/bin`
- `/usr/opensv/netbackup/bin/snapcfg`
- `/usr/opensv/netbackup/db/config`
- `/usr/opensv/netbackup/db/event`
- `/usr/opensv/netbackup/db/images`
- `/usr/opensv/netbackup/db/media`
- `/usr/opensv/netbackup/ext/db_ext`
- `/usr/opensv/netbackup/ext/db_ext/db2`
- `/usr/opensv/volmgr`
- `/usr/opensv/volmgr/database`

- `/usr/opensv/var`

For example, to create a touch file called `DEFERRED_IMAGE_LIMIT` in the `/usr/opensv/netbackup/db/config` directory, use the following steps:

- Create a file with that name in the NetBackup administrator home directory or a subdirectory.
- Use the `cp-nbu-config configuration-file target-directory` command to add the desired content to the touch file. For example:

```
cp-nbu-config DEFERRED_IMAGE_LIMIT /usr/opensv/netbackup/db/config
```

See [“Running NetBackup commands from the NetBackup Virtual Appliance”](#) on page 199.

See [“About NetBackup operating system commands”](#) on page 202.

See [“Best practices for running NetBackup commands from the NetBackup Virtual Appliance”](#) on page 201.

See [“Known limitations of running NetBackup commands from the NetBackup Virtual Appliance”](#) on page 202.

Best practices for running NetBackup commands from the NetBackup Virtual Appliance

The following list provides examples of how you, a NetBackup administrator, can configure an appliance so you can run NetBackup commands from the restricted shell.

- You can only create files and directories in user home directory and the subdirectories.
- An auto-generated alias file is created in the user home directory that contains a `sudo` alias for all the NetBackup commands. Thus, when you use a base command name you do not need to specify `sudo` when you run the command.
- The alias file is not honored when you run a command in a script. You must specify `sudo` before you can use the command.
- You can create a file that contains variables for all NetBackup commands with `sudo` prefix. The variable can be used in the automation scripts to avoid use of `sudo` for every NetBackup command invocation. The variable file can be sourced in the scripts. For example:
 - The following command enables you to use the variable `${bpps}`.
`bpps="sudo /usr/opensv/netbackup/bin/bpps"`
 - The following command enables you to use the variable `${nbemmcnd}`.

```
nbemmcmd="sudo /usr/opensv/netbackup/bin/admincmd/nbemcmd"
```

- A `cdnbu` alias is available for you to use to change directory to a NetBackup install path. That alias takes you to the `/usr/opensv/` directory.

See [“Running NetBackup commands from the NetBackup Virtual Appliance”](#) on page 199.

See [“About NetBackup operating system commands”](#) on page 202.

See [“Known limitations of running NetBackup commands from the NetBackup Virtual Appliance”](#) on page 202.

See [“About the NetBackupCLI user role”](#) on page 174.

About NetBackup operating system commands

The following rules apply to the operating system commands:

- The following commands are available:
`awk, bash, cat, clear, cut, grep, head, ls, rm, sudo, uname, vi`
- The commands that are useful for scripting :
`date, mkdir, rmdir, touch, whoami, hostname, and so forth`
- A NetBackup administrator can use the `passwd` command to change their password.
- To perform a host name lookup you must use the `host` command. The `nslookup` command is not supported.

See [“Running NetBackup commands from the NetBackup Virtual Appliance”](#) on page 199.

See [“Creating a NetBackup touch file from the NetBackup Virtual Appliance”](#) on page 200.

See [“Best practices for running NetBackup commands from the NetBackup Virtual Appliance”](#) on page 201.

See [“Known limitations of running NetBackup commands from the NetBackup Virtual Appliance”](#) on page 202.

Known limitations of running NetBackup commands from the NetBackup Virtual Appliance

The following list identifies the known limitations that a NetBackup administrator should understand before they use this feature:

- You cannot edit the `bp.conf` file directly using an editor. To edit the `bp.conf` file you must use the `bpsetconfig` command to set an attribute within the file.
- You cannot modify or create NetBackup notify scripts.
- The `nslookup` command is not supported.
- You cannot use the `man` command. To see the usage of a command, use the `help` option that is provided with the command.
- The operating system commands that are used to perform appliance management are not supported.

See [“Running NetBackup commands from the NetBackup Virtual Appliance”](#) on page 199.

See [“Creating a NetBackup touch file from the NetBackup Virtual Appliance”](#) on page 200.

See [“About NetBackup operating system commands”](#) on page 202.

See [“Best practices for running NetBackup commands from the NetBackup Virtual Appliance”](#) on page 201.

About mounting a remote NFS

You can use the NetBackup Virtual Appliance Shell Menu to mount a remote Network File System (NFS) onto the appliance server through the `Manage > MountPoints` menu. To work with the NFS drive, you can use the following commands in the NetBackup Virtual Appliance Shell Menu.

Table 10-4 Commands to work with NFS drive

Command	Descriptions
<code>Mount</code>	Use the <code>Mount</code> command to mount an NFS drive.
<code>List</code>	Use the <code>List</code> command to list all the existing mount points on your appliance.
<code>Unmount</code>	Use the <code>Unmount</code> command to un-mount a previously mounted NFS drive.

See [“Mounting a remote NFS drive”](#) on page 204.

See [“Unmounting an NFS drive”](#) on page 206.

In certain circumstances, you may find that a NetBackup Virtual Appliance NFS share is not accessible. If this issue occurs, use the NetBackup Virtual Appliance Shell Menu to restart the NFS server. Use the following command:

`Support > Service Restart nfsserver`

Once you have restarted the server, try again to access the NFS share.

See [Manage > MountPoints > Mount](#) on page 389.

See [Manage > MountPoints > List](#) on page 388.

See [Manage > MountPoints > Unmount](#) on page 391.

Mounting a remote NFS drive

This procedure describes how to mount your remote NFS drive.

To mount a remote NFS drive

- 1 Log on to the NetBackup Virtual Appliance Shell Menu using your administrator's credentials.
- 2 Type the `Main > Manage> MountPoints` command.

The appliance lists all the commands under in the `MountPoints` menu.

3 To mount your remote NFS drive, type the following command:

```
Mount RemotePath MountPoint [FileSystemType] [options]
```

This command includes the following parameters:

	RemotePath	MountPoint	[FileSystemType]	[Options]
Description	Provide the address of a device or a directory to be mounted on to your appliance.	Provide the name of the local mount point. This appears as a subdirectory where the NFS drive is mounted. After the command runs 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).	Specify the type of the device to be mounted.	Specify any additional options to be passed to the appliance along with the Mount command.
Format	HOST:DIRECTORY Note: A short hostname is also supported. Ensure that the short hostname can be resolved.	A subdirectory name under /mnt/remote. The subdirectory may or may not exist and is created under /mnt/remote by default.		You can only use options specific for mounting the NFS drive.
Parameter type	Mandatory	Mandatory	Optional	Optional
Example	appesx5.ros.veritas.com:/build1	garry	NFSv3 or any other supported type by the underlying Mount command.	ro is used to mount the device as read only.

- 4 The appliance mounts your remote NFS drive.

Note: If you mount a remote share and then restart the appliance, the mount is re-established when the appliance starts. The mount points are persistent across all the restart operations and there is no exception to this rule.

To list and view the mounted devices

- 1 Log in to the NetBackup Virtual Appliance Shell Menu using your administrator credentials.
- 2 Type the `Main > Manage > MountPoints` command.

The appliance lists all the commands under the `MountPoints` menu.

- 3 To view the list of mounted devices use the following command:

```
List [Type]
```

When you specify the value for the `[Type]` parameter as `[All]`, the appliance displays all the available mount points along with the NFS drives. If this parameter is not provided, this command lists all the NFS mount points.

Note: In certain circumstances, you may find that a NetBackup Virtual Appliance NFS share is not accessible. If this issue occurs, use the NetBackup Virtual Appliance Shell Menu to restart the NFS server.

Use the following command: `Support > Service Restart nfsserver`

Once you have restarted the server, try to access the NFS share again.

See [Manage > MountPoints > Mount](#) on page 389.

See [Manage > MountPoints > List](#) on page 388.

See [“About mounting a remote NFS”](#) on page 203.

See [“Unmounting an NFS drive”](#) on page 206.

Unmounting an NFS drive

This procedure describes how to unmount an NFS drive.

To unmount an NFS drive

- 1
- Log on to the NetBackup Virtual Appliance Shell Menu using your administrator credentials.
- 2
- Type the `Main > Manage > MountPoints` command.
The appliance lists all the commands under the `MountPoints` menu.
- 3
- To unmount a drive, use the following command:

`Unmount MountPoint [force].`

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

	<i>MountPoint</i>	[force]
Description	Provide the name of the directory that is to be un-mounted. Note: An error is displayed in case of the following situations: ■ If the directory name is incorrect. ■ If the directory with the given name does not exist.	Specify this parameter to unmount the NFS forcibly.
Format	The directory name must start with / and must have the correct directory name. Note: If the specified directory is a valid mount directory, it is unmounted.	
Parameter type	Mandatory	Optional
Example	/mymounts/mount1	

- 4
- 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.

See [Manage > MountPoints > Unmount](#) on page 391.

See [“Mounting a remote NFS drive”](#) on page 204.

See [“Mounting a remote NFS drive”](#) on page 204.

About Auto Image Replication from a NetBackup Virtual Appliance

The backups that are generated in one NetBackup domain can be replicated to storage in one or more NetBackup domains. This process is referred to as Auto Image Replication. You can configure Auto Image Replication between two NetBackup Virtual Appliances or between a NetBackup Virtual Appliance and a NetBackup 52xx (physical) Appliance or other NetBackup primary server.

To configure Auto Image Replication, you need to perform the following tasks:

Step No.	Task	Reference
1.	Establish trust between the two primary servers	See the section titled 'Adding a trusted primary server' in the <i>NetBackup Administrator's Guide, Volume I</i>
2.	Review the prerequisites for Auto Image Replication	See “Prerequisites for Auto Image Replication” on page 208.
3.	Configure the replication target	See “Configuring a replication target” on page 208.
4.	Configure storage lifecycle policy on source and target domains	See the section titled 'Creating a storage lifecycle policy' in the <i>NetBackup Administrator's Guide, Volume I</i> .

Prerequisites for Auto Image Replication

The following prerequisites must be followed before you set up replication configuration from a NetBackup Virtual Appliance:

- The target storage server type must be the same that is configured in the target primary server domain.
- The target storage server name must be the same that is configured in the target primary server domain.

See [“Configuring a replication target”](#) on page 208.

See [“About Auto Image Replication from a NetBackup Virtual Appliance”](#) on page 208.

Configuring a replication target

Use the following procedure to configure a replication target in the source domain.

To configure a replication target

- 1 In the NetBackup Administration Console in the source NetBackup domain, expand **Media and Device Management > Credentials > Storage Server**.

- 2 Select the source storage server.

- 3 On the **Edit** menu, select **Change**.

- 4 In the **Change Storage Server** dialog box, select the **Replication** tab.

- 5 Select a trusted primary server and a replication target.

In the **Target Primary Server** drop-down list, select the primary server of the domain to which you want to replicate data. All trusted primary servers are in the drop-down list.

- 6 In the **Storage Server Type** drop-down list, select the type of target storage server. All available target types are in the drop-down list.

The target storage server type must be the same that is configured in the target primary server domain.

- 7 In the **Storage Server Name** field, enter the shortname of the target storage server.

You must enter the target storage server name that is configured in the target primary server domain.

- 8 In the **Deduplication Server Name** field, enter the name of the deduplication server.

Note: The **Deduplication Server Name** and **User Name** fields may be pre-populated in some scenarios.

- 9 Enter the User name and Password for the target primary server's deduplication storage server.

If the target primary server is a NetBackup Virtual Appliance or a NetBackup 52xx (physical) Appliance, use the following procedure to determine the appliance deduplication password:

See [“Determining the appliance deduplication password”](#) on page 210.

- 10 Click **Add**. You can now see the new replication target in the **Replication Targets** section at the top.

Click **OK**.

- 11 You must refresh the disk pool after setting up a replication target. In the **NetBackup Administration Console**, in the left pane, expand **Media and Device Management Devices > Disk Pools**. In the right pane, select the disk pool you want to update. In the **Change Disk Pool** dialog box, click **Refresh** to configure the replication settings for the disk pool.

Once you have configured a replication target, you can configure storage lifecycle policies on source and target domains. For more information about configuring storage lifecycle policies, refer to the section named 'Creating a storage lifecycle policy' in *NetBackup Administrator's Guide, Volume I for UNIX, Windows, and Linux*.

See [“About Auto Image Replication from a NetBackup Virtual Appliance”](#) on page 208.

Determining the appliance deduplication password

The following credentials are required to configure Auto Image Replication between two NetBackup Virtual Appliances or between a NetBackup Virtual Appliance and a NetBackup 52xx Appliance.

- **username:** `user_name`
- **password:** `appliance dedupe password`

To determine the appliance deduplication password

- 1 Log on to the target appliance and enter into the appliance shell menu.
- 2 From the Main_Menu prompt, enter the following:

```
Appliance > ShowDedupPassword
```

This command shows the password for the deduplication solution that is configured on the appliance. The deduplication password appears on the screen.

Note: If you changed the deduplication password, the appliance shell menu does not display the new password. The `ShowDedupPassword` option only displays the original password that was created during the installation process.

Note: If your configuration has an appliance primary server and one or more appliance media servers, the deduplication password is the same for all servers. In this case, use the appliance primary server's shell menu to retrieve the deduplication password.

For more information about Auto Image Replication, refer to the *NetBackup™ Administrator's Guide, Volume I*.

See [“Configuring a replication target”](#) on page 208.

See [“About Auto Image Replication from a NetBackup Virtual Appliance”](#) on page 208.

Generating certificates

Use the `Manage > Certificates > Generate` command to generate a new certificate from the NetBackup Virtual Appliance Shell Menu. The certificate is an authentication token which used by the NetBackup plug-in. It is downloaded automatically to your local directory as a `.pem` file.

NetBackup Virtual Appliance supports the generation of the following certificate types:

- vCenter
- SCVMM

For more information about vCenter and SCVMM clients, refer to the following documents:

NetBackup™ Plug-in for Microsoft SCVMM Console Guide

NetBackup™ Plug-in for VMware vSphere Web Client Guide

See [“About SSL usage”](#) on page 239.

See [“About NetBackup Virtual Appliance as a VMware backup host”](#) on page 197.

Monitoring the appliance

This chapter includes the following topics:

- [About NetBackup Virtual Appliance alerts](#)
- [Setting up email notifications for a NetBackup Virtual Appliance](#)
- [Setting up SNMP notifications for a NetBackup Virtual Appliance](#)
- [Enabling and disabling Call Home from the appliance shell menu](#)
- [Configuring a Call Home proxy server from the NetBackup Virtual Appliance Shell Menu](#)
- [About SNMP](#)
- [About Call Home](#)
- [About AutoSupport](#)
- [About storage email alerts](#)

About NetBackup Virtual Appliance alerts

The NetBackup Virtual Appliance can send alerts when software components fail or encounter errors.

[Table 11-1](#) lists the available alerting mechanisms with links to additional information and configuration steps.

Table 11-1 NetBackup Virtual Appliance alert types

Alert mechanism	How to configure
Call Home (AutoSupport)	See “About Call Home” on page 219. See “About AutoSupport ” on page 222. See “Enabling and disabling Call Home from the appliance shell menu” on page 216. See “Configuring a Call Home proxy server from the NetBackup Virtual Appliance Shell Menu” on page 217.
Email (SMTP)	See “Setting up email notifications for a NetBackup Virtual Appliance” on page 213.
SNMP	See “About SNMP” on page 218. See “Setting up SNMP notifications for a NetBackup Virtual Appliance” on page 214.

Note: If you use NetBackup OpsCenter, the information that displays for the NetBackup Virtual Appliance on the **Appliance Hardware** page does not apply. The collected hardware information displays as question marks or as error messages similar to the following:

No <part(s)> detected

All of this information can be disregarded.

Setting up email notifications for a NetBackup Virtual Appliance

The NetBackup Virtual Appliance can send email alerts when software components fail or encounter errors.

To configure email notifications

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main_Menu > Settings > Alerts` view, enter the following command to set the SMTP mail server:

```
Email SMTP Add <server> [[account]] [[password]]
```

Where <server> is the IP address or FQDN of your SMTP mail server.

- 3 Enter the following command to set the email address that you want the appliance to send emails to:

```
Email Software Add <admin>
```

Where *<admin>* is the email address of the appliance administrator.

Note: You can add multiple email addresses at once by separating them with a semi-colon (;).

- 4 (Optional) Enter the following command to set the email account that you want the emails to originate from (sender email):

```
Email SenderID Set <sender_email>
```

Where *<sender_email>* is the email address that you want the appliance emails to originate from.

- 5 (Optional) Enter the following command to set the time interval between email notifications:

```
Email NotificationInterval <minutes>
```

Where *<minutes>* is the time interval in minutes.

- 6 (Optional) Enter the following command to verify the appliance email notification settings:

```
Email Show
```

See [Settings > Alerts > Email](#) on page 520.

See [“About NetBackup Virtual Appliance alerts”](#) on page 212.

Setting up SNMP notifications for a NetBackup Virtual Appliance

You can configure the appliance to generate and send Simple Network Management Protocol (SNMP) traps to your SNMP server for monitoring purposes.

To configure SNMP notifications

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main_Menu > Settings > Alerts` view, enter the following command to set the SNMP server:

```
SNMP Set Community Server [Port] Security
```

Where:

- *Community* is the SNMP Community string. The default setting is *public*. This setting is required for SNMP V2, and is optional for SNMP V3.
- *Server [Port]* sets the SNMP server name and the port assignment. The default port assignment is *162*.

Note: NetBackup Virtual Appliance supports all of the SNMP servers in the market. However, the ManageEngine™ SNMP server and the HP OpenView SNMP server are tested and certified.

- *Security* is one of the following:
 - `Security noAuthNoPriv [Username]`
Sets the security level to no authentication and no privileges for a specific SNMP user.
 - `Security AuthNoPriv [Username] [Authentication Protocol] [Authentication Password]`
Sets the security level to authentication with no privileges for a specific SNMP user. Authentication Protocol can be set to SHA256 or SHA512. An Authentication Password is required.
 - `Security AuthPriv [Username] [Authentication Protocol] [Encryption Policy] [Authentication Password] [Encryption Passphrase]`
Sets the security level to authentication with privileges for a specific SNMP user. Authentication Protocol can be set to SHA256 or SHA512. Encryption Policy can be set to AES128, AES192, or AES256. An Authentication Password and an Encryption Passphrase are required.
Rules for Username, Authentication Password, and Encryption Passphrase:
 - Username can have 1-32 characters.
Authentication Password and Encryption Passphrase must have 8 or more characters.
 - Username, passwords, and passphrases may include uppercase letters, lowercase letters, numbers, and the following punctuation marks: period, hyphen/dash, underscore.
 - Spaces, commas, and special characters are not allowed.

- 3 Enter the following command to show the appliance MIB:

```
SNMP ShowMIB
```

Copy the Management Information Base (MIB) text and import it into your SNMP management software so that it can interpret the appliance traps.

- 4 Enter the following command to enable the SNMP configuration:

```
SNMP Enable version, where version is v2 or v3.
```

See [Settings > Alerts > SNMP](#) on page 517.

See [“About SNMP”](#) on page 218.

See [“About the Management Information Base \(MIB\)”](#) on page 219.

See [“About NetBackup Virtual Appliance alerts”](#) on page 212.

Enabling and disabling Call Home from the appliance shell menu

You can enable or disable Call Home from the NetBackup Virtual Appliance Shell Menu. Call Home is enabled by default.

To enable or disable Call Home from the shell menu

- 1 Log on to the shell menu.
- 2 To enable Call Home, run the `Main > Settings > Alerts > CallHome Enable` command.
- 3 Use the `Settings > Alerts > CallHome > Test` command to test that Call Home is working correctly.
- 4 To disable Call Home, run the `Main > Settings > Alerts > CallHome Disable` command.

See [Settings > Alerts > CallHome](#) on page 513.

See [“Configuring a Call Home proxy server from the NetBackup Virtual Appliance Shell Menu”](#) on page 217.

See [“About Call Home”](#) on page 219.

See [“About NetBackup Virtual Appliance alerts”](#) on page 212.

Configuring a Call Home proxy server from the NetBackup Virtual Appliance Shell Menu

You can configure a proxy server for Call Home, if required. If the 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 AutoSupport server. This option is disabled by default.

To add a Call Home proxy server from the NetBackup Virtual Appliance Shell Menu

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 To enable proxy settings, run the `Main > Settings > Alerts > CallHome Proxy Enable` command.
- 3 To add a proxy server, run the `Main > Settings > Alerts > CallHome Proxy Add` command.
 - You are prompted to enter the name of the proxy server. The proxy server name is the TCP/IP address or the fully qualified domain name of the proxy server. By default, the HTTP protocol is used to communicate with the proxy server.

Note: If you want to use the HTTPS protocol, enter `https://` before the proxy server name. To ensure successful communication with the proxy server, add the latest CA certificate used by the proxy server by running the `Settings > Security > Certificate > AddCACertificate` command.

- After you have entered a name for the proxy server, you are prompted to enter the port number for the proxy server.
- Further, you are required to answer the following:

```
Do you want to set credentials for proxy server? (yes/no)
```
- On answering yes, you are prompted to enter a user name for the proxy server.
- After you have entered the user name, you are prompted to enter a password for the user. On entering the required information, the following message is displayed:

Successfully set proxy server

- 4 To disable proxy settings, run the `Main > Settings > Alerts > CallHome Proxy Disable` command.

Further, you can also use the NetBackup Virtual Appliance Shell Menu to enable or disable proxy server tunneling for your appliance. To do so, run the `Main > Settings > CallHome Proxy EnableTunnel` and `Main > Settings > Alerts > CallHome Proxy DisableTunnel` commands. Proxy server tunneling lets you provide a secure path through an untrusted network.

See [Settings > Alerts > CallHome](#) on page 513.

See [“Enabling and disabling Call Home from the appliance shell menu”](#) on page 216.

See [“About Call Home”](#) on page 219.

About SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It uses either the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP) for transport, depending on configuration. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMP is based on the manager model and agent model. This model consists of a manager, an agent, a database of management information, managed objects, and the network protocol.

The manager provides the interface between the human network manager and the management system. The agent provides the interface between the manager and the physical devices being managed.

The manager and agent use a Management Information Base (MIB) and a relatively small set of commands to exchange information. The MIB is organized in a tree structure with individual variables, such as point status or description, being represented as leaves on the branches. A numeric tag or object identifier (OID) is used to distinguish each variable uniquely in the MIB and in SNMP messages.

NetBackup Virtual Appliance versions 3.1 and later support SNMP V2.

Software versions 4.0 and later also support SNMP V3.

See [“About the Management Information Base \(MIB\)”](#) on page 219.

See [“Setting up SNMP notifications for a NetBackup Virtual Appliance”](#) on page 214.

See [“About NetBackup Virtual Appliance alerts”](#) on page 212.

About the Management Information Base (MIB)

Each SNMP element manages specific objects with each object having specific characteristics. Each object and characteristic has a unique object identifier (OID) that is associated with it. Each OID consists of the numbers that are separated by decimal points (for example, 1.3.6.1.4.1.48328.1).

These OIDs form a tree. A MIB associates each OID with a readable label and various other parameters that are related to the object. The MIB then serves as a data dictionary that is used to assemble and interpret SNMP messages. This information is saved as a MIB file.

You can view the details of the SNMP MIB file with the `Settings > Alerts > SNMP ShowMIB` command in the NetBackup Virtual Appliance Shell Menu.

See [“About SNMP”](#) on page 218.

See [“Setting up SNMP notifications for a NetBackup Virtual Appliance”](#) on page 214.

See [“About NetBackup Virtual Appliance alerts”](#) on page 212.

About Call Home

Your appliance can connect with a Veritas AutoSupport server and upload software information. Veritas support uses this information to resolve any issues that you might report. The appliance uses the HTTPS protocol and uses port 443 to connect to the Veritas AutoSupport server. This feature of the appliance is referred to as Call Home. It is enabled by default.

AutoSupport uses the data that Call Home gathers to provide proactive monitoring for the appliance. If Call Home is enabled, the appliance uploads information or data to the Veritas AutoSupport server at a default interval of 24 hours.

If you determine that you have a problem with your appliance, you might want to contact Veritas support. The Technical Support engineer uses the serial number of your appliance and assesses the status from the Call Home data.

To know the serial number of your appliance from the Shell Menu, run the `Monitor > Hardware ShowHealth Appliance [Product]` command.

See [“Determining the NetBackup Virtual Appliance serial number”](#) on page 301.

[Table 11-2](#) describes how a failure is reported when the feature is enabled or disabled.

Table 11-2 What happens when Call Home is enabled or disabled

Monitoring status	Failure routine
Call Home enabled	When a failure occurs, the following sequence of alerts occur: ■ The appliance uploads all the monitored information to a Veritas AutoSupport server. The list following the table contains all the relevant information. ■ The appliance generates 3 kinds of email alerts to the configured email address. ■ An error message by email to notify you of the failure once an error is detected. ■ A resolved message by email to inform you of any failure once an error is resolved. ■ A 24-hour summary by email to summarize all of the currently unresolved errors in the recent 24 hours. ■ The appliance also generates an SNMP trap.
Call Home disabled	No data is sent to the Veritas AutoSupport server. Your system does not report errors to Veritas to enable faster problem resolution.

The following list contains all the information that is monitored and sent to Veritas AutoSupport server for analysis.

- Partition information
- MSDP statistics
- NetBackup Virtual Appliance software version
- NetBackup version
- Appliance model
- Appliance configuration

See [“Enabling and disabling Call Home from the appliance shell menu”](#) on page 216.

See [“Configuring a Call Home proxy server from the NetBackup Virtual Appliance Shell Menu”](#) on page 217.

See [“Understanding the Call Home workflow”](#) on page 221.

See [“About the Product Improvement Program”](#) on page 221.

See [“About AutoSupport ”](#) on page 222.

See [“About NetBackup Virtual Appliance alerts”](#) on page 212.

Understanding the Call Home workflow

This section explains the mechanism that Call Home uses to upload data from your appliance to the Veritas AutoSupport server.

Call Home uses HTTPS (secure and encrypted protocol) with port number 443 for all communication with Veritas AutoSupport servers. For Call Home to work correctly, ensure that your appliance has Internet access either directly, or through a proxy server to reach the Veritas AutoSupport servers. AutoSupport, a mechanism that monitors the appliance proactively, uses the Call Home data to analyze and resolve any issues that the appliance may encounter.

The appliance initiates all communications. On the appliance, make sure that you enable the proxy and/or the firewall to outbound 443/TCP TLS socket connections to the following site: `https://api.appliance.veritas.com`

The appliance Call Home feature uses the following workflow to communicate with AutoSupport servers:

- Access a port to `https://api.appliance.veritas.com` every 24 hours.
- Perform a self-test operation to `https://api.appliance.veritas.com`
- If the appliance encounters an error state, all logs from past three days are gathered along with the current log.
- The logs are then uploaded to the Veritas AutoSupport server for further analysis and support. These error logs are also stored on the appliance. You can access these logs from `/log/upload/<date>` folder.
- If the error state persists three days later, the logs will be re-uploaded.

See [“About Call Home”](#) on page 219.

See [“About AutoSupport ”](#) on page 222.

See [“Enabling and disabling Call Home from the appliance shell menu”](#) on page 216.

About the Product Improvement Program

The NetBackup Virtual Appliance Product Improvement Program uses Call Home to capture installation deployment and product usage information. The information that Veritas receives becomes part of a continuous quality improvement program that helps understand how customers configure, deploy, and use the product. This information is then used to help Veritas identify improvements in product features, testing, technical support, and future requirements.

You can enable or disable the Product Improvement Program from the NetBackup Virtual Appliance Shell Menu.

The Product Improvement Program is enabled by default. However, if you have disabled Call Home, the Product Improvement Program is also disabled. You cannot enable the Product Improvement Program without Call Home.

To enable or disable the Product Improvement Program from the NetBackup Virtual Appliance Shell Menu

- 1 Log on to the NetBackup Virtual Appliance Shell Menu
- 2 To enable the Product Improvement Program, run the `Main > Settings > Alerts > CallHome NBInventory Enable` command.
- 3 To disable the Product Improvement Program, run the `Main > Settings > Alerts > CallHome NBInventory Disable` command.

See [Settings > Alerts > CallHome](#) on page 513.

See [“About Call Home”](#) on page 219.

About AutoSupport

The AutoSupport feature lets Veritas Support use your Appliance Call Home data to help resolve any issue that you report. The information allows Veritas support to minimize downtime and provide a more proactive approach to support.

The support infrastructure is designed to allow Veritas support to help you in the following ways:

- Proactive monitoring lets Veritas support to automatically create cases and fix issues.
- The AutoSupport infrastructure within Veritas analyzes the Call Home data from appliance. This analysis provides proactive customer support for failures, reducing the need for backup administrators to initiate support cases.
- With AutoSupport ability, Veritas support can begin to understand how customers configure and use their appliances, and where improvements would be most beneficial.
- Send and receive status and alert notifications for the appliance.
- Receive software status using Call Home.
- Provide more insight into the issues and identify any issues that might further occur as a result of the existing issue.
- View reports from the Call Home data to analyze patterns and see usage trends. The appliance sends health data every 30 minutes.

See [“About Call Home”](#) on page 219.

See [“About NetBackup Virtual Appliance alerts”](#) on page 212.

About storage email alerts

A software administrator can add his email account by running the Settings > Alerts > Email Software Add [Email Addresses] command to receive software alerts. If you have configured your email address to receive software alerts for a specific appliance, you will receive Appliance alerts like storage alerts, hardware monitoring alerts, and so on.

The storage alerts are generated in the following scenarios:

- When a Resize or Move operation is performed on the appliance. Once the Resize or Move operation is complete, an alert is sent to the email address specifying the operation and result. An alert is sent if the resize or move operations succeed or fail.
- When Storage sanity check fails on the appliance. Storage sanity check runs daily and also runs as a part of storage manipulation operations. Storage sanity check helps to fix some of the storage issues or reports them.

A sample alert content is provided. This alert is generated when the AdvancedDisk partition was resized to 1 TB on host nb-appliance:

Alerts from NetBackup Appliance

```
Host name:  nb-appliance
Operation:  Resize AdvancedDisk 1 TB
Status:     Succeeded
```

- NetBackup Appliance Alerts

The following sample alert is generated when the storage sanity check failed:

Alerts from NetBackup Appliance

```
Host name:  nb-appliance
Operation:  Storage sanity check
Status:     Failed
Reason:     Failed to mount the 'AdvancedDisk' partition '0'. A full file
            system check (fsck) needs to be performed on this partition.
```

- NetBackup Appliance Alerts

Appliance security

This chapter includes the following topics:

- [About Symantec Data Center Security on the NetBackup Virtual Appliance](#)
- [About data security](#)
- [About data integrity](#)
- [About data classification](#)
- [About data encryption](#)
- [About SSL usage](#)
- [About implementing ECA certificates](#)
- [About the NetBackup Virtual Appliance intrusion detection system](#)
- [About the NetBackup Virtual Appliance intrusion prevention system](#)
- [Major components of the NetBackup Virtual Appliance OS](#)
- [OS STIG hardening for NetBackup Virtual Appliance](#)
- [FIPS 140-2 conformance for NetBackup Virtual Appliance](#)
- [Disable user access to the NetBackup appliance operating system](#)
- [Manage support access to the maintenance shell](#)
- [About the appliance login banner](#)
- [Setting the appliance login banner](#)
- [Log Forwarding feature overview](#)

About Symantec Data Center Security on the NetBackup Virtual Appliance

Symantec Data Center Security: Server Advanced (SDCS) is a security solution offered by Symantec to protect servers in data centers. The SDCS software is included on the appliance and is automatically configured during appliance software installation. SDCS offers policy-based protection and helps secure the appliance using host-based intrusion prevention and detection technology. It uses the least-privileged containment approach and also helps security administrators centrally manage multiple appliances in a data center. The SDCS agent runs at startup and enforces the customized NetBackup Virtual Appliance intrusion prevention system (IPS) and intrusion detection system (IDS) policies. The overall SDCS solution on the appliance provides the following features:

- **Hardened Linux OS components**
Prevents or contains malware from harming the integrity of the underlying host system as a result of OS vulnerabilities.
- **Data protection**
Tightly limits appliance data access to only those programs and activities that need access, regardless of system privileges.
- **Hardened appliance stack**
Appliance application binaries and configuration settings are locked down such that changes are tightly controlled by the application or trusted programs and scripts.
- **Expanded detection and audit capabilities**
Provides enhanced visibility into important user or system actions to ensure a valid and complete audit trail that addresses compliance regulations (such as PCI) as a compensating control.

The SDCS implementation on the appliance operates in an unmanaged mode and helps secure the appliance using host-based intrusion prevention and detection technology. In unmanaged mode, you can monitor SDCS events from the NetBackup Virtual Appliance Shell Menu. Use the `Main_Menu > Monitor > SDCS` commands, to monitor the events logged. The events are monitored using the NetBackup Virtual Appliance IDS and IPS policies. These policies are automatically applied at the time of deployment. You can use the `SDCS > Audit View` command to filter and view specific events.

The NetBackup Virtual Appliance is in managed mode when it is connected to the SDCS server. The managed mode is not supported in the current release.

See [“About the NetBackup Virtual Appliance intrusion prevention system”](#) on page 243.

See [“About the NetBackup Virtual Appliance intrusion detection system”](#) on page 242.

See [“Viewing SDCS audit log details”](#) on page 228.

See [“Auditing the SDCS logs on the NetBackup Virtual Appliance”](#) on page 226.

Auditing the SDCS logs on the NetBackup Virtual Appliance

There are several ways to audit the SDCS logs on the NetBackup Virtual Appliance.

Basic search

To do a basic SDCS log search

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main_Menu > Monitor > SDCS` view, enter the following command:

```
Audit Search <term>
```

Where *<term>* is a word or name that you want to search in the logs for.

Filter by individual attribute

SDCS events have three main attributes:

- Date
- Severity
- Event type

You can filter the SDCS logs by each individual attribute.

To filter SDCS log entries by date

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 Go to the `Main_Menu > Monitor > SDCS` view.
- 3 (Optional) Enter the following command to view all of the events that occurred on a specific day:

```
Audit View Date <ToDate>
```

Where *<ToDate>* is the day in the DD/MM/YYYY format.

- 4 (Optional) Enter the following command to view all of the events that occurred during a specific period of time:

```
Audit View Date <ToDate>[-hh:mm:ss] [<FromDate>[-hh:mm:ss]]
```

Where *<ToDate>[-hh:mm:ss]* is the later date/time and *[<FromDate>[-hh:mm:ss]]* is the earlier date/time. For example:

```
Audit View Date 05/25/2016-13:00:00 05/25/2016-12:00:00
```

To filter SDCS log events by severity

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main_Menu > Monitor > SDCS` view, enter the following command:

```
Audit View Severity <SeverityCode>
```

Where `<SeverityCode>` is the one letter code of the severity type that you want to filter by.

See [“About SDCS event type codes and severity codes on the NetBackup Virtual Appliance”](#) on page 231.

To filter SDCS log entries by type

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main_Menu > Monitor > SDCS` view, enter the following command:

```
Audit View EventType <TypeCode>
```

Where `<TypeCode>` is the four letter code of the event type that you want to filter by.

See [“About SDCS event type codes and severity codes on the NetBackup Virtual Appliance”](#) on page 231.

Filter using multiple attributes

The best way to search for a specific type of SDCS event from a particular period of time is to use the `Audit View Filter` command.

To filter SDCS log entries by date

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main_Menu > Monitor > SDCS` view, enter the following command:

```
Audit View Filter <SeverityCode> <TypeCode> <ToDate>[-hh:mm:ss]
[<FromDate>[-hh:mm:ss]] <Search_yes/no>
```

- `<SeverityCode>`
The one letter code of the severity type that you want to filter by. Enter **ALL** if you want to include all severity codes in your filter.
- `<TypeCode>`
The four letter code of the event type that you want to filter by. Enter **ALL** if you want to include all event type codes in your filter.
- `<ToDate>[-hh:mm:ss] [<FromDate>[-hh:mm:ss]]`
Where `<ToDate>[-hh:mm:ss]` is the later date/time and `[<FromDate>[-hh:mm:ss]]` is the earlier date/time. Use the DD/MM/YYYY date format.

To filter events for a specific day, use `<ToDate>[-hh:mm:ss]` and type **NULL** for `[<FromDate>[-hh:mm:ss]]`.

To filter all events after a specific date/time, use `[<FromDate>[-hh:mm:ss]]` and type **NULL** for `<ToDate>[-hh:mm:ss]`

- `<Search_yes/no>`

Enter **yes** if you want to include a search term. Otherwise, enter **no**.

For example:

```
Audit View Filter C ALL 05/26/2016-14:00:00 05/25/2016-13:00:00
no
```

- 3 (Optional) If you entered **yes** for `<Search_yes/no>`, enter the search string when prompted.

Get more details about an event

You can use the `Audit View EventID` command to get more information about a specific SDCS event that is listed in a search or filter.

To get more details about a specific SDCS event

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main_Menu > Monitor > SDCS` view, enter the following command:

```
Audit View EventID <ID#>
```

Where `<ID#>` is the ID number of an event that was listed in your filter or search.

See [Monitor > SDCS](#) on page 411.

See [“Viewing SDCS audit log details”](#) on page 228.

Viewing SDCS audit log details

You can view the detailed information for each Symantec Data Center Security (SDCS) logged event using the `Main_Menu > Monitor > SDCS Audit View` command. [Table 12-1](#) describes the various details that displayed in the command output.

Table 12-1 SDCS log details description

Detail	Description
Event Severity	The severity of the logged event. The following severity types are displayed: ■ Information - Information about normal system operation. ■ Notice - Information about normal system operation. ■ Warning - Unexpected activity or problems that have already been handled by SDCS. These events might indicate that a service or application on a target computer is functioning improperly with the applied policy. After investigating the policy violations, you can configure the policy and allow the service or application to access the specific resources if necessary. ■ Major - Activity with more effect than Warning and less effect than Critical. ■ Critical - Indicates activity or problems that might require administrator intervention to correct.
Process ID	The ID assigned to the process.
Rule Name	The name of the policy rule that generated the event.
Process	The name of the policy applied to the agent that triggered the event.
Event Date	The date and time (YYYY-MM-DD HH:MM:SS) that the event occurred.
Event Type	The event type for the logged event. For a detailed list of all the event types and their descriptions, refer to the SDCS documentation.
Sequence Number	The sequence number of the logged event.
Event Priority	The priority (0-100) assigned to the event.
Facility	The login mechanism for the event.
Description	The detailed or consolidated description of the event.
User Name	The name of the user that was logged in when the event took place.
File Name	The path and name of the affected file.
New Size	The size of the affected file after the logged event.
Old Size	The size of the affected file before the logged event.
Operation	The type of operation that was performed on the affected file.

See [“About Symantec Data Center Security on the NetBackup Virtual Appliance”](#) on page 225.

Changing the SDCS log retention settings on the NetBackup Virtual Appliance

By default, the NetBackup Virtual Appliance stores each SDCS log entry for 30 days. You can adjust this retention period to any number of days. However, if disk space becomes a factor, you can choose to retain a set amount of log files (each log file is ~10.5 MB).

You can check the current SDCS log retention settings for the appliance at any time using the `Audit ShowSettings` command in the `Main_Menu > Monitor > SDCS` view.

To change the SDCS log retention settings

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main_Menu > Monitor > SDCS` view, enter one of the following commands:
 - To set the number of days in the retention period:
`Audit SetSettings RetentionPeriod <days>`
Where *<days>* is the specific number of days that you want the appliance to retain each log entry.
 - To set the number of log files the appliance retains:
`Audit SetSettings FileNumber <files>`
Where *<files>* is the specific number of SDCS log file that you want the appliance to retain at any given time.

See [“About Symantec Data Center Security on the NetBackup Virtual Appliance”](#) on page 225.

See [“Auditing the SDCS logs on the NetBackup Virtual Appliance”](#) on page 226.

See [“Viewing SDCS audit log details”](#) on page 228.

About SDCS event type codes and severity codes on the NetBackup Virtual Appliance

Table 12-2 SDCS severity codes

Code	Description	Details
C	Critical	Activity or problems that might require administrator intervention to correct.
E	Error	
I	Information	Information about normal system operation.
M	Major	A more serious event than Warning, but less serious than Critical.
N	Notice	Information about normal system operation.
T	Tracking	
W	Warning	Unexpected activity or problems that have already been handled by SDCS. Note: These messages might indicate that a service or application on the appliance is not functioning properly with the applied policy.

Note: You can also get this list of SDCS severity codes by typing the following command in the NetBackup Virtual Appliance Shell Menu:

```
Main_Menu > Monitor > SDCS > Audit View SeverityCodes
```

Table 12-3 SDCS event codes

Code	Description	Details
DAUD	IDS Audit	
DFWU	File Watch Unix	
DFWW	File Watch Windows	
DGEN	Generic Log	
DIPS	IPS to IDS Event	
DNTL	NT Event Log	

Table 12-3 SDCS event codes (*continued*)

Code	Description	Details
DRGW	Registry Watch	
DSYS	SysLog	
DUC2	Unix C2 Security	
DWTM	WTMP/BTMP	
MBIN	Server Error	
MCOM	Common Status	
MCON	Agent Config Status	
MEFR	File Received	
MERR	IDS Error	
MOVR	Agent Override	
MREP	File Create	
MSTA	Agent Status	
MSTD	IDS Status	
MSTP	IPS Status	
PBOP	IPS Overflow	
PCRE	IPS Create	
PDES	IPS Destroy	
PFIL	IPS File	
PMNT	IPS Mount	
PNET	IPS Network	
POSC	IPS System Call	
PPST	IPS PSET	
PREG	IPS Registry	
TRAC	Tracking/Debugging	

Note: You can also get this list of SDCS event type codes by typing the following command in the NetBackup Virtual Appliance Shell Menu from the `Main_Menu >`

`Monitor > SDCS view:`

```
Audit View EventTypeCodes
```

See [“Auditing the SDCS logs on the NetBackup Virtual Appliance”](#) on page 226.

See [Monitor > SDCS](#) on page 411.

About data security

NetBackup Virtual Appliance supports policy driven mechanisms to protect data on clients as well as NetBackup servers. The following measures are implemented to improve data security by avoiding data leaks and improving protection:

- Real-time intrusion detection mechanisms are in place to audit access to confidential data stored on NetBackup Virtual Appliance.
- Logging and real-time tracking of all restores.
- Access to the backed up data is authorized to only appliance users and processes.
- NetBackup Virtual Appliance ensures that all backup data in the Deduplication Pool (MSDP) is marked with Cyclic Redundancy Check (CRC) digital signatures when the backup takes place. A maintenance task continuously re-computes the CRC digital signatures and compares it with the original signature to detect if there has been any unwanted tampering or corruption in the Deduplication Pool.
- Unintended access to appliance storage is prevented by password protecting logins to the appliance.
- Access to shared data limited to authorized users only and NetBackup processes.
- Usage of HTTPS protocol and port 443 to connect to the Veritas AutoSupport server to upload software information using the Call Home feature. Veritas Technical Support uses this information to resolve any issues that you might report. This information is retained for 90 days and purged at the Veritas Secure Operations Center.

See [“About data integrity”](#) on page 234.

See [“About data classification”](#) on page 234.

See [“About data encryption ”](#) on page 235.

See [“About Symantec Data Center Security on the NetBackup Virtual Appliance”](#) on page 225.

See [“About the NetBackup Virtual Appliance intrusion detection system”](#) on page 242.

About data integrity

The Deduplication Pool storage in NetBackup Virtual Appliance provides the following data integrity checks to ensure that successful data restores:

Continuous end-to-end verification of backup data, stored in the Deduplication Pool

Any inadvertent data modifications that can cause data corruption are automatically detected and rectified if possible. Any unrecoverable data corruption issues are reported to the storage administrator by the NetBackup Console's Disk Reports UI (**NetBackup Administration Console > Reports > Disk Reports**).

Continuous Cyclic Redundancy Check (CRC) verification of backup data, stored in the Deduplication Pool

A CRC value is computed for each object created for the backup job in the Deduplication pool. A background process continuously verifies the CRC signatures to ensure that backup data is not tampered with and can be restored successfully when needed. The deduplication pool design naturally isolates any data corruption from uncorrupted portions of the pool, preventing corruption from spreading throughout the deduplication pool.

See [“About data security”](#) on page 233.

See [“About data classification”](#) on page 234.

See [“About data encryption ”](#) on page 235.

About data classification

A data classification represents a set of backup requirements, which makes it easier to configure backups for data with different requirements. For example, a backup with a gold classification must go to a storage lifecycle policy with a gold data classification. The NetBackup Virtual Appliance supports the same data classification attributes as NetBackup.

The NetBackup Data Classification attribute specifies the classification of the storage lifecycle policy that stores the backup. For example, a backup with a gold classification must go to a storage unit with a gold data classification.

NetBackup provides the following default data classifications:

- Platinum
- Gold
- Silver
- Bronze

This attribute is optional and applies only when the backup is to be written to a storage lifecycle policy. If the list displays **No data classification**, the policy uses the storage selection that is displayed in the **Policy storage** list. If a data classification is selected, all the images that the policy creates are tagged with the classification ID.

See [“About data security”](#) on page 233.

See [“About data integrity”](#) on page 234.

See [“About data encryption ”](#) on page 235.

About data encryption

The NetBackup Virtual Appliance offers the following encryption methodologies to protect both data at rest and in flight:

- Transmits data in encrypted formats by using secure tunnels. These configurations can be made by client-side encryption and also replication. If these options are not used, once the data is transmitted from the appliance, the network infrastructure is used for securing data in flight.

See [“About data security”](#) on page 233.

See [“About data integrity”](#) on page 234.

See [“About data classification”](#) on page 234.

See [“About SSL usage”](#) on page 239.

KMS support

The NetBackup Virtual Appliance supports encryption managed by NetBackup Key Management Service (KMS) which is integrated with NetBackup Enterprise Server 7.1. KMS is supported on primary and media server appliances. Regenerating the data encryption key is the only supported method of recovering KMS on an appliance primary server.

The following describes the KMS key features:

- Does not require an additional license.
- Is a primary server-based symmetric key management service.

- Can be administered as a primary server with tape devices connected to it or to another NetBackup Virtual Appliance.
- Manages symmetric cryptography keys for tape drives that conform to the T10 standard (such as LTO4 or LTO5).
- Designed to use volume pool-based tape encryption.
- Can be used with tape hardware that has built-in hardware encryption capability.
- Can be managed by a NetBackup CLI administrator using the NetBackup Virtual Appliance Shell Menu or the KMS Command Line Interface (CLI).

About the keys used under KMS

The KMS generates keys from passcodes or auto-generates keys. [Table 12-4](#) lists the associated KMS files that hold the information about the keys.

Table 12-4 KMS files

KMS files	Description	Location
Key file or key database	This file is critical for KMS, as it contains the data encryption keys.	/usr/openv/kms/db/KMS_DATA.dat
Host Primary Key	This file contains the encryption key that encrypts and protects the <code>KMS_DATA.dat</code> key file using AES 256.	/usr/openv/kms/key/KMS_HMKF.dat
Key Protection Key	This encryption key encrypts and protects individual records in the <code>KMS_DATA.dat</code> key file using AES 256. Currently, the same key protection key is used to encrypt all of the records.	/usr/openv/kms/key/KMS_KEYF.dat

Configuring KMS

To configure KMS on an appliance primary server, you must log in as a NetBackupCLI user,

Before you proceed, ensure that the NetBackupCLI user is assigned the required RBAC permissions to configure and enable KMS. Use a NetBackup administrator account such as **nbsecadmin** to log in to the NetBackup Web UI and assign the Default Security Administrator role to the NetBackupCLI user.

For steps on managing role-based access control, see the *NetBackup Web UI Administrator's guide*.

Note: If required, you can create a new NetBackupCLI user for configuring and enabling KMS. For more information about the NetBackupCLI user, See [“About the NetBackupCLI user role”](#) on page 174.

The following describes how to configure and enable KMS on an appliance.

To configure and enable KMS on an appliance

- 1 Log in to the appliance primary server as a NetBackupCLI user.
- 2 Create an empty database using the `nbkms` command, as follows:

```
[nbcli@myappliance~]# nbkms -createemptydb
```

- 3 Start `nbkms`. For example:

```
[nbcli@myappliance~]# nbkms
```

- 4 Create a Key group. For example:

```
[nbcli@myappliance~]# nbkmsutil -createkg -kgname KMSKeyGroupName
```

- 5 Create an active key. For example:

```
[nbcli@myappliance~]# nbkmsutil -createkey -kgname KMSKeyGroupName  
-keyname KMS KeyName
```

Enabling KMS encryption for MSDP

After KMS has been configured and is running on the primary server, you can enable KMS encryption for MSDP on all of the media servers that are associated with the primary server.

Before you proceed, ensure that the NetBackupCLI user is assigned the required RBAC permissions to configure and enable KMS. Use a NetBackup administrator account such as **nbsecadmin** to log in to the NetBackup Web UI and assign the Default Security Administrator role to the NetBackupCLI user.

For steps on managing role-based access control, see the *NetBackup Web UI Administrator's guide*.

Note: If required, you can create a new NetBackupCLI user for configuring and enabling KMS. For more information about the NetBackupCLI user, See [“About the NetBackupCLI user role”](#) on page 174.

The following describes how to enable KMS encryption for MSDP on an appliance.

To enable KMS encryption for MSDP

1 Log in to the appliance media server as a NetBackup CLI user.

2 Change the following options in the order as shown:

- nbcli@myappliance:~> pdcfg
--write=/msdp/data/dpl/pdvol/etc/puredisk/contentrouter.cfg
--section=KMSTOptions --option=KMSType --value=0
- nbcli@myappliance:~> pdcfg
--write=/msdp/data/dpl/pdvol/etc/puredisk/contentrouter.cfg
--section=KMSTOptions --option=KMSServerName --value=<primary
server hostname>
- nbcli@myappliance:~> pdcfg
--write=/msdp/data/dpl/pdvol/etc/puredisk/contentrouter.cfg
--section=KMSTOptions --option=KMSKeyGroupName --value=msdp
- nbcli@myappliance:~> pdcfg
--write=/msdp/data/dpl/pdvol/etc/puredisk/contentrouter.cfg
--section=KMSTOptions --option=KeyName --value=<KMS KeyName>
- nbcli@myappliance:~> pdcfg
--write=/msdp/data/dpl/pdvol/etc/puredisk/contentrouter.cfg
--section=KMSTOptions --option=KMSEnable --value=true
- pdcfg --write=
/msdp/data/dpl/pdvol/etc/puredisk/contentrouter.cfg
--section=ContentRouter --option=ServerOptions
--value=verify_so_references,fast,encrypt

Repeat this step on all media servers that are associated with the primary server

3 Identify yourself to the system by logging on to the NetBackup web application.
Run the following command:

```
bnpbat -login -loginType WEB  
  
Authentication Broker: ApplianceHostname  
  
Authentication Port: 0  
  
Authentication Type: unixpwd  
  
LoginName: Username  
  
Password: Password
```

- 4 Ensure that the KMS is registered with NetBackup web service.

```
nbkmscmd -discoverNbkms
```

- 5 Stop and restart the NetBackup services with the following commands:

- `bp.kill_all`
- `bp.start_all`

- 6 To verify that KMS encryption for MSDP is enabled on the media server, run a backup job on the server, then run the following command:

```
crcontrol --getmode
```

About SSL usage

The Secure Socket Layer (SSL) protocol creates an encrypted connection between the appliance web server and the appliance web console, and other local servers. This type of connection allows for a more secure information transfer without the problems of eavesdropping, data tampering, or message forgery.

SSL certificates are also supported for secure communications between the appliance and various external servers, such as LDAP, HTTPs proxy, and Syslog.

Self-signed certificates

The appliance uses self-signed certificates for client and host validation. A host certificate issued by an internal CA is deployed on the primary and media servers during role configuration. The self-signed certificate is generated using a 2048 bit RSA public key that is hashed with the SHA256 algorithm and signed with RSA encryption. For secure communications, the appliance uses only TLS v1.2 and later protocols.

ECA certificates

NetBackup Virtual Appliance also supports host certificates issued by an External Certificate Authority (ECA). You can use an ECA as an alternative to the internal CA to provide host verification and security to meet your organization's standards.

Refer to the following table for different types of external certificates used in NetBackup Virtual Appliance.

Table 12-5 Types of ECA certificates

Certificate type	Description
Host certificate	The appliance's host certificate is based on the X.509 or PKCS#7 standard. The certificate is encoded in either DER (binary) or PEM (text) format. Veritas recommends that you use RSA public and private keys of length 2048 bits or higher. Note: Ensure that the SubjectAlternativeName certificate extension contains all the appliance host names and IP addresses by which the appliance is reached. Include the fully qualified host names and the short names.
Host private key (corresponding to the host certificate)	The appliance's host private key must be in PKCS#8 standard and encoded in PEM format.
(Optional) Intermediary CA certificates	Intermediary CA certificates form a certificate chain from the appliance host certificate to the root CA certificate. These certificates are only required if the host certificates are issued by a CA other than the root CA.
Root CA certificates	These include the root CA certificates of the Appliance certificate chain and its peers. If the appliance needs to interact with the hosts that have certificates from different CAs, you must have all those intermediary and root CA certificates ready in a file called cacerts.pem.

About implementing ECA certificates

NetBackup Virtual Appliance's web service uses the PKCS#12 standard and requires certificate files to be in the X.509 (.pem or .cer) format. If the certificate files are in the .der, .DER, or .p7b formats, NetBackup Virtual Appliance automatically converts the files to an accepted format.

Certificate requirements

To prevent errors while importing certificates, ensure that the external certificate files meet the following requirements.

- Certificate files are in the .pem file format and begin with "-----BEGIN CERTIFICATE-----".
- Certificate files contain the host name and FQDN in the subject alternative name (SAN) field of the certificate. If the certificate is used in an HA environment, the SAN field must contain VIP, host name, and FQDN.

- Subject name and common name fields are not empty.
- Subject fields are unique for each host.
- Subject fields contain a maximum of 255 characters.
- Server and client authentication attributes are set in the certificate.
- Only ASCII 7 characters are used in the subject and SAN fields of the certificate.
- The private key file is in the PKCS#8 PEM format and begins with -----BEGIN ENCRYPTED PRIVATE KEY----- or -----BEGIN PRIVATE KEY-----.

Register the ECA

Starting from version 4.1, you can register an ECA on both NetBackup Virtual Appliance and NetBackup using the `Settings > Security > Certificate > Import` command.

Perform the following steps to import the host certificate, host private key, and trust store to register the ECA on NetBackup and NetBackup Virtual Appliance. Both NetBackup and NetBackup Virtual Appliance layers use the same host certificate, host private key, and trust store.

- 1 Log in to the appliance as an Administrator user.
- 2 From the NetBackup Virtual Appliance Shell Menu, run the `Settings > Security > Certificate > Import` command. The following NFS and CFS share locations are now accessible:
 - NFS: `/inst/share`
 - CFS: `\\<ApplianceName>\general_share`
- 3 Upload the certificate file, trust store file, and private key file to either of the share locations and enter the paths to the files.
- 4 Choose how to access the certificate revocation list (CRL). A CRL comprises a list of external certificates that have been revoked by the ECA and should not be trusted. Select either of the following options:
 - Use the CRL location provided in the certificate file.
 - Provide the location of a CRL file (`.crl`) in the local network.
 - Do not use a CRL.
- 5 Confirm the location of the certificate files you want to register on the appliance.

Support for Copilot

Before you use the Copilot feature on an appliance deployed with external certificates, ensure the following:

- The appliance's certificate file (in `/etc/vxos-ssl/servers/certs/`) is same as the primary server's certificate file (in `/usr/opensv/var/global/appliance_certificates/`).
- The appliance's certificate file (in `/etc/vxos-ssl/servers/certs/`) is named in the `<FQDN_hostname>-self.cert.pem` format.

Run the following commands on each of the associated appliances:

```
rm /etc/vxos-ssl/servers/certs/<FQDN_hostname>-self.cert.pem

cp /etc/vxos-ssl/servers/certs/server.pem
  /etc/vxos-ssl/servers/certs/<FQDN_hostname>-self.cert.pem

tpconfig -delete -nb_appliance <Short_hostname>

/opt/NBUAppliance/scripts/copilot_users.pl --add
```

About the NetBackup Virtual Appliance intrusion detection system

The appliance intrusion detection system (IDS) consists of a custom Symantec Data Center Security (SDCS) policy that runs automatically at startup. The IDS policy is a real-time policy for monitoring significant system events and critical configuration changes, while optionally taking remediation actions on events of interest.

The following list contains some of the events that the IDS policy monitors:

- User logons, logouts, and failed log on attempts
- Sudo commands
- User addition, deletion, and password changes
- User group addition, deletion, and member modifications
- System auto-start option changes
- Modifications to all system directories and files, including core system files, core system configuration files, installation programs, and common daemon files
- NetBackup services start and stop
- Detected system attacks from UNIX rootkit file/directory detection, UNIX worm file/directory detection, malicious module detection, suspicious permission change detection, and so on

- Audit of all NetBackup Virtual Appliance Shell Menu activity, including shell operations for maintenance, root, and NetBackupCLI users.

See [“About the NetBackup Virtual Appliance intrusion prevention system”](#) on page 243.

See [“About Symantec Data Center Security on the NetBackup Virtual Appliance”](#) on page 225.

About the NetBackup Virtual Appliance intrusion prevention system

The appliance intrusion prevention system (IPS) consists of a custom Symantec Data Center Security (SDCS) policy that runs automatically at startup. The IPS policy is an in-line policy that can proactively block unwanted resource access behaviors before they can be acted upon by the operating system.

The following list contains some of the IPS policy features:

- Real-time tight confinement of the appliance operating system processes and common applications, such as the following:
 - `nscd` - which caches DNS requests to cut down on remote DNS lookups.
 - `cron`
 - `syslog-ng`
 - `klogd`
 - `rpcd` for NFS
 - `rpc.idmapd`
 - `rpc.mountd`
 - `rpc.statd`
 - `rpcbind`
- Self-Protection for the SDCS agent itself to ensure that the security features and monitoring features of SDCS are not compromised.
- Lock-down of access to system binaries, except by identified and trusted applications, users, and user groups.
- Confinements that protect the system from the applications that try to install software, such as `sbin`) or change system configuration settings, such as `hosts` file.

- Prohibits applications from executing critical system calls such as `mknod`, `modctl`, `link`, `mount`, and so on.
- Prohibits unauthorized users or applications from accessing backup data, such as `/advancedisk`, `/cat`, `/disk`, `/opt/NBUAppliance/db/config/data`, and so on.

See [“About the NetBackup Virtual Appliance intrusion detection system”](#) on page 242.

See [“About Symantec Data Center Security on the NetBackup Virtual Appliance”](#) on page 225.

Major components of the NetBackup Virtual Appliance OS

[Table 12-6](#) lists the major software components of the appliance operating system (VxOS).

Table 12-6 Major software components included in VxOS for appliance version 4.0

Software component	Version
Red Hat Enterprise Linux (RHEL)	7.9
Veritas InfoScale	7.4.2 Note: The Veritas InfoScale installation is modified and tuned for maximum performance on the appliance.
Symantec Data Center Security: Server 6.8 Advanced (SDCS)	6.8.2 (build 757)
Java Runtime Environment (JRE)	11.0.11.0.9-1
Apache Tomcat	9.0.44-1
RabbitMQ	rabbitmq-server-3.8.16-1
MongoDB	4.2.11-1

OS STIG hardening for NetBackup Virtual Appliance

The Security Technical Implementation Guides (STIGs) provide technical guidance for increasing the security of information systems and software to help prevent malicious computer attacks. This type of security is also referred to as hardening.

Starting with software version 3.2, you can enable OS STIG hardening rules for increased security. These rules are based on the following profile from the Defense Information Systems Agency (DISA):

STIG for Red Hat Enterprise Linux 7 Server - V1R4

To enable these rules, use the following command:

`Main_Menu > Settings > Security > Stig Enable`, followed by the maintenance password.

Note the following about enabling STIG:

- When the option is enabled, a list of the enforced rules appears. The command output also shows exceptions to any rules that are not enforced.
- This command does not allow individual rule control.
- Once the option is enabled, a factory reset is required to disable the associated rules.
- If Lightweight Directory Access Protocol (LDAP) is configured, it is recommended that you set it up to use Transport Layer Security (TLS) before you enable the option.

Note: If you have enabled the STIG feature on an appliance and you need to upgrade it or install an EEB on it, do not plan such installations during the 4:00am - 4:30am time frame. By following this best practice, you can avoid interrupting the automatic update of the `AIDE` database and any monitored files, which can cause multiple alert messages from the appliance.

Starting with the 4.1 release, all STIG rule lists are available in separate documents on the Veritas Support site. Two checklists are currently available, one for the OS and one for Application Security STIG. For instructions about how to obtain these documents, go to the **Latest releases** page on the [Veritas Download Center](#), navigate to **NetBackup Appliance OS** and click **Learn more**.

FIPS 140-2 conformance for NetBackup Virtual Appliance

The Federal Information Processing Standards (FIPS) define U.S. and Canadian Government security and interoperability requirements for computer systems. The National Institute of Standards and Technology (NIST) issued the FIPS 140 Publication Series to coordinate the requirements and standards for validating cryptography modules. The FIPS 140-2 standard specifies the security requirements for cryptographic modules and applies to both the hardware and the software components. It also describes the approved security functions for symmetric and asymmetric key encryption, message authentication, and hashing.

Note: For more information about the FIPS 140-2 standard and its validation program, click on the following links:

<https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf>

<https://csrc.nist.gov/projects/cryptographic-module-validation-program>

FIPS validation for Java

Starting with NetBackup Virtual Appliance 4.1, the FIPS 140-2 standard is enabled by default for all Java-based services. The FIPS validation is achieved by using SafeLogic's CryptoComply modules.

FIPS validation for MSDP and VxOS

Starting with NetBackup Virtual Appliance release 3.1.2, you can enable the FIPS 140-2 standard for MSDP and VxOS. The NetBackup Cryptographic Module, which is used by MSDP and VxOS, is FIPS validated.

Once FIPS for VxOS is enabled, the `sshd` uses the following FIPS approved ciphers:

- aes128-ctr
- aes192-ctr
- aes256-ctr

Older SSH Clients are likely to prevent access to the appliance after FIPS for VxOS is enabled. Check to make sure that your SSH client supports the listed ciphers, and upgrade to the latest version if necessary. Default cipher settings are not typically FIPS-compliant, which means you may need to select them manually in your SSH client configuration.

You can enable the FIPS 140-2 standard for NetBackup MSDP and VxOS with the following commands:

- Main Menu > Settings > Security > FIPS Enable MSDP, followed by the maintenance password.
Enabling or disabling 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 or disable this feature.

Note: If you have upgraded from a previous version of NetBackup Virtual Appliance, ensure that you enable MSDP only after your existing data has been converted to use FIPS compliant algorithms. To check the current status of the data conversion use the `crcontrol --dataconvertstate` command. Enabling MSDP before the status is set to **Finished** can cause data restoration failures.

- Main Menu > Settings > Security > FIPS Enable VxOS, followed by the maintenance password.
Enabling or disabling 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 or disable this feature.
- Main Menu > Settings > Security > FIPS Enable All, followed by the maintenance password.
Enabling or disabling 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 or disable this feature.

See [Main > Settings > Security > FIPS](#) on page 509.

Disable user access to the NetBackup appliance operating system

Depending on the security policies of your organization, you can choose to permanently disable user access to the NetBackup Virtual Appliance operating system (VxOS). You can disable user access to the VxOS by configuring its security level to `High`. Note that the following restrictions are permanently enforced in the appliance:

- Users cannot access the maintenance shell. The `Support > Maintenance` menu is not available in the shell menu.

Note: Only Veritas support personnel can be granted access to the maintenance shell to troubleshoot issues and manage operating system-related tasks. See [“Manage support access to the maintenance shell”](#) on page 249.

- Users cannot create and delete NetBackupCLI users. The `Manage > NetBackupCLI` menu is not available in the shell menu.
- Users cannot grant or revoke the NetBackupCLI role. The `Authorization > Grant_NetBackupCLI` menu is not available in the shell menu.
- Users with the NetBackupCLI role cannot log in to the appliance.

To permanently disable user access to VxOS

- 1** To view the current security level of the VxOS, use the following command:
- ```
Main_Menu > Settings > Security > SecurityLevel Show
```
- The VxOS can operate in either of the following security levels:

| Security level | Description                                                                                                                                                                                                      |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Optimal        | Access to VxOS is granted as per standard Veritas security policies. This is the default security configuration.                                                                                                 |
| High           | Access to VxOS is permanently disabled for all users.                                                                                                                                                            |
| Maintenance    | Access to VxOS is temporarily granted to Veritas support personnel through the maintenance shell. The security level is automatically reverted to <code>High</code> after the maintenance activity is completed. |

- 2** To permanently disable user access to VxOS, configure the security level to `High`. Use the following command:
- ```
Main_Menu > Settings > Security > SecurityLevel High
```

Note: After switching to the `High` security level, you cannot revert to the default (`Optimal`) security level unless you perform a factory reset of the appliance. You also must exit the current shell session and log back in to see the changes.

Manage support access to the maintenance shell

The maintenance shell in the `Support > Maintenance` menu is disabled if you configure the security level of VxOS to `High`. However, to troubleshoot issues and manage OS tasks, you can allow Veritas support personnel to enable and access the maintenance shell.

Use the commands in the `Main_Menu > Support > System` menu to manage support access to the maintenance shell. See [Support > System](#) on page 565.

Table 12-7 Commands for managing support access to the maintenance shell

Command	Description
<code>Support > System > Generate-otp</code>	Use this command to generate a ten digit one-time password (OTP), which will remain active for a period of two hours. The OTP can be shared with Veritas support personnel.
<code>Support > System > Show-otp</code>	Use this command to view the currently active OTP.
<code>Support > System > Unlock</code>	Veritas support personnel use this command to enable the maintenance shell (<code>Support > Maintenance</code>). In addition to an active OTP, Veritas support personnel require a customer case ID and support passphrase to run the <code>Unlock</code> command successfully and access the maintenance shell. Note: VxOS is temporarily configured to the <code>Maintenance</code> security level.
<code>Support > System > Lock</code>	Use this command to disable the maintenance shell. Veritas support personnel cannot access the maintenance shell and are logged out of any active session. Note: VxOS is reverted to the <code>High</code> security level.

About the appliance login banner

The NetBackup Virtual Appliance provides the ability to set a text banner that appears when a user attempts to log on to the appliance. You can use the login banner to communicate various kinds of messages to users. Typical uses for the login banner include legal notices, warning messages, and company policy information.

Once a login banner is set, it appears in each of the appliance interfaces that support it, such as the NetBackup Virtual Appliance Shell Menu and SSH. For the NetBackup Virtual Appliance Shell Menu the login banner appears before a user attempts to log on the NetBackup Virtual Appliance Shell Menu.

Use `Settings > Notifications > LoginBanner` in the NetBackup Virtual Appliance Shell Menu to configure the login banner. See [“Creating the appliance login banner”](#) on page 251.

See [“Setting the appliance login banner”](#) on page 250.

Setting the appliance login banner

The `Settings > Notifications > Login Banner` screen lets you create a customized text banner that appears when you access the appliance. You can use the login banner to communicate important information to users, such as a corporate security policy.

The login banner consists of the following two elements:

- **Login Banner Heading**
 - 250 characters maximum
 - Standard English alphabet
- **Login Banner Text**
 - Unlimited characters
 - Standard English alphabet

Note: None of the login banner settings on this screen take effect until you save them.

See [“Creating the appliance login banner”](#) on page 251.

See [“Removing the appliance login banner”](#) on page 251.

Creating the appliance login banner

The following procedures describe how to set the appliance login banner using the NetBackup Virtual Appliance Shell Menu.

To enable and create a new login banner using the NetBackup Virtual Appliance Shell Menu

- 1 Log onto the NetBackup Virtual Appliance Shell Menu.
- 2 Run the `Main > Settings > Notifications > LoginBanner Set` command.
- 3 Enter a banner heading, and then press **Enter**.
- 4 Enter the banner message text.

Once you have entered the banner message, type **end** on a new line and press **Enter**.

- 5 A preview of the login banner appears with the following message:

```
The existing login banner will be overwritten and the SSH daemon
will be restarted. Do you want to proceed? [y, n]: (y)
```

Type **y** and press **Enter** to set the login banner. Type **n** and press **Enter** to cancel any changes and exit the login banner configuration.

- 6 The following message appears:

```
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)
```

Type **y** and press **Enter** to set the login banner in the NetBackup Administration Console. Type **n** and press **Enter** to continue without changing the NetBackup login banner.

Once the login banner is enabled, you cannot make individual changes to it using the NetBackup Virtual Appliance Shell Menu. However, you can run the `LoginBanner Set` command again and overwrite the existing banner with one that contains your desired changes.

See [“Removing the appliance login banner”](#) on page 251.

See [“About the appliance login banner”](#) on page 250.

Removing the appliance login banner

The following procedure describes how to remove the appliance login banner using the NetBackup Virtual Appliance Shell Menu.

To remove the login banner using the NetBackup Virtual Appliance Shell Menu

- 1 Log onto the NetBackup Virtual Appliance Shell Menu.
- 2 Run the `Main > Settings > Notifications > LoginBanner Remove` command.
- 3 When the following message appears, select the appropriate action:

```
The existing login banner will be removed and the SSH daemon
will be restarted. Do you want to proceed? [y, n]: (y)
```

Type **y** and press **Enter** to remove the login banner. Type **n** and press **Enter** to cancel.

- 4 When the following message appears, select the appropriate action:

```
Do you want to remove the login banner from the NetBackup
Administration Console as well? [y, n]: (y)
```

Type **y** and press **Enter** to remove the NetBackup login banner. Type **n** and press **Enter** to leave the banner set in the NetBackup Administration Console.

See [“Creating the appliance login banner”](#) on page 251.

See [“About the appliance login banner”](#) on page 250.

Log Forwarding feature overview

The Log Forwarding feature lets you send appliance logs to an external log management server. Starting with software version 3.1, NetBackup Virtual Appliance support forwarding syslog. A syslog is an OS system log that contains user and system level activities in the form of events. Use this feature to help increase security and to help achieve general compliance initiatives such as HIPPA, SOX, and PCI. The currently supported log management servers are HP ArcSight and Splunk.

NetBackup appliances use the Rsyslog client to forward logs. In addition to HP ArcSight and Splunk, other log management servers that support the Rsyslog client can also be used to receive syslogs from the appliance. Refer to the log management server documentation to verify Rsyslog client support.

Secure log transmission

To secure the log transmission from the appliance to the log management server, you can use the TLS (Transport Layer Security) option. NetBackup Virtual Appliance currently supports only TLS Anonymous Authentication for log forwarding.

To enable TLS, the appliance and the log management servers each require unique preparation as follows:

- **Appliance requirements**

Before you configure and enable the log forwarding feature, the appliance requires the following certificate and private key files in the X.509 file format:

- `ca-server.pem`

A root CA certificate from which the log management server certificate is derived.

- `nba-rsyslog.pem`

A certificate for the appliance to communicate with a log management server, that also includes any intermediary CA certificates.

- `nba-rsyslog.key`

A private key that corresponds to the certificate used to communicate with the `syslog` management server.

You can upload these files to the appliance through an NFS or a CIFS share.

- **Configuration requirements for HP ArcSight servers**

You must set up an Rsyslog server with TLS settings on the HP ArcSight server to receive encrypted logs from the appliance. Then, configure the Rsyslog server to forward the decrypted logs to the HP ArcSight server. See the www.rsyslog.com website for guides on setup and configuration.

- **Configuration requirements for Splunk servers**

You must first configure TLS on these servers, and then configure the log forwarding feature on the appliance. Refer to your Splunk documentation for the appropriate TLS configuration details.

Configuration

The feature must be configured from the shell menu with the following `Main > Settings > LogForwarding` command options:

- `LogForwarding Enable`

Configures the feature functionality.

- `LogForwarding Disable`

Deletes the configuration and disables the feature.

- `LogForwarding Interval`

Sets how often logs are forwarded. Select from 0 (continuous), 15, 30, 45, or 60 minutes.

If STIG is enabled on the appliance, you cannot manually configure the Log Forwarding interval.

- `LogForwarding Share`

Opens or closes an NFS or a CIFS share on the appliance for obtaining the required certificate and private key files. The share paths are the following:

- `LogForwarding Show`
Shows the current configuration and status.

After you enter the `LogForwarding > Enable` command, prompts appear to guide you through the configuration as described in the following table:

Table 12-8 `LogForwarding > Enable` command prompts

Prompt	Description
Server name or IP	Enter the name or the IP address of the external log management server.
Server port	Enter the appropriate port number on the external log management server.
Protocol	Select either UDP or TCP.
Interval	Set how often logs are forwarded.
Enable TLS	Select to enable TLS for secure log transmissions to the log management server. Currently, only the X.509 file format is supported. The following certificate and private key files must be uploaded to the appliance to use TLS: ■ <code>ca-server.pem</code> ■ <code>nba-rsyslog.pem</code> ■ <code>nba-rsyslog.key</code>

For complete configuration and command information, refer to the following:

- See [Settings > LogForwarding](#) on page 463.
- See [“Uploading certificates for TLS”](#) on page 328.
- See [“Enabling log forwarding”](#) on page 329.
- See [“Changing the log forwarding interval”](#) on page 330.
- See [“Viewing the log forwarding configuration”](#) on page 330.
- See [“Disabling log forwarding ”](#) on page 331.

Upgrading the appliance

This chapter includes the following topics:

- [About upgrading to NetBackup Virtual Appliance software version 4.1](#)
- [Requirements and best practices for upgrading NetBackup appliances](#)
- [Pre-upgrade tasks for appliance upgrades](#)
- [Methods for downloading appliance software release updates](#)
- [Installing a NetBackup Virtual Appliance software update using the NetBackup Virtual Appliance Shell Menu](#)
- [Troubleshooting upgrade issues](#)

About upgrading to NetBackup Virtual Appliance software version 4.1

Before you begin any upgrades, review the following topics:

See [“Supported upgrade paths”](#) on page 255.

See [“About corresponding NetBackup software versions ”](#) on page 257.

Supported upgrade paths

NetBackup Virtual Appliance supports direct upgrades from version 3.1.1 or later to 4.1.

Appliances with versions 3.1 and earlier must be upgraded twice to get to version 4.1. It is recommended that these systems first be upgraded to version 3.2 or 3.3.0.1, and then upgraded to version 4.1.

Preflight check before the upgrade

For upgrades to versions 3.1.1 and later, the upgrade script runs a preflight check to determine if the appliance is ready for an upgrade. The preflight check analyzes several system parameters and provides information about what was found and whether an upgrade can proceed. If the preflight check detects any issues that fail to meet the upgrade requirements, the upgrade is not allowed to proceed. You must address all of the reported issues before the upgrade is allowed.

Refer to the following topic for more information:

See [“Pre-upgrade tasks for appliance upgrades”](#) on page 259.

Note: Upgrades to version 3.1.1 and later are not supported if you have installed Teradata binaries on the appliance. The RHEL operating system does not currently support the use of these binaries. The upgrade cannot proceed if the preflight check finds Teradata binaries on the appliance.

Appliance behavior during upgrades

The upgrade mechanism takes the following measures to ensure that the upgrade process completes successfully:

- Determines if the available update is newer than the version of software that is currently installed.
- Determines if there is enough available space on the appliance to install the release update.
- Stops the processes that are currently active on the appliance.
- Checks for any active NetBackup jobs. The upgrade proceeds only if it is determined that no active jobs are detected.

The appliance software upgrade occurs only after all of these criteria are met.

- Before the upgrade completes, a self-test is performed automatically.

If the self-test fails, the upgrade pauses and you are prompted to select one of the following:

- **Attempt again** to try the self-test again.
- **Rollback now** to roll back to the previous version.
The upgrade remains paused until you make a selection.

Note: Starting with the 3.1.2 release, if the post-upgrade self-test fails, an automatic rollback is no longer enforced. If you select **Attempt again** and the self-test still fails, the upgrade pauses again and prompts with the same options.

About corresponding NetBackup software versions

NetBackup software version 9.1 is included with NetBackup Virtual Appliance release 4.1. [Table 13-1](#) lists the corresponding NetBackup versions for the recent NetBackup Virtual Appliance software releases.

Table 13-1 Appliance software releases and the corresponding NetBackup software versions

Appliance software release	NetBackup software version
3.1	8.1
3.1.1	8.1.1
3.1.2	8.1.2
3.2	8.2
3.3.0.1	8.3.0.1
4.0	9.0
4.1	9.1

About the Appliance Install Manager

Starting with the 3.1 release, you can switch to the **Appliance Install Manager (AIM)** window for viewing the upgrade progress. This window shows the estimated completion time, the upgrade progress bar, the main upgrade steps, the upgrade logs, and other useful information.

After the first restart, AIM will not work. During that time use the VMware Remote Console to monitor the upgrade progress.

If you log on to the shell menu from the virtual machine console during an upgrade, press **Alt + F2** from the connected keyboard to open the **AIM** window.

The **AIM** window appears as soon as you start the upgrade and provides the following view modes:

- **Main**

This default view shows the main upgrade steps and task results.

- **Verbose**

This view shows the detailed upgrade logs.

To change from the **Main** view to the **Verbose** view, press the **V** key.

To change from the **Verbose** view to the **Main** view, press the **M** key.

To close the **AIM** window and return to the shell menu, press the **S** key.

To show the **AIM** window again, enter the following command:

```
Main_Menu > Manage > Software > UpgradeStatus
```

Requirements and best practices for upgrading NetBackup appliances

This topic describes the requirements and best practices that you should follow anytime you plan to upgrade appliance software.

- Always perform a full disaster recovery (DR) backup before an upgrade.
- Follow the same upgrade order for appliances as for traditional NetBackup upgrades. If you use NetBackup OpsCenter, upgrade it first. Then upgrade appliances starting with the primary server appliance, followed by all media server appliances.
- If you have multiple media servers to upgrade, you must perform the upgrade process on each individual media server.
- If a traditional NetBackup primary server is used with an appliance media server, that primary server must have the same NetBackup version or later as the media server appliance. For example, before you upgrade a media server appliance to version 4.1, first upgrade the NetBackup primary server to version 9.1.
See [“About corresponding NetBackup software versions”](#) on page 257.
- Make sure that the NetBackup primary server is active and running throughout the duration of an appliance media server upgrade. In addition, make sure that the NetBackup processes are started or running on both the primary server and the media server.
- NetBackup clients must use the same or an earlier software version as the appliance. Clients cannot run at a later version than the appliance. For example, a client with NetBackup version 9.1 can only be used with an appliance server with version 4.1 or later. Client add-ons must also be the same as the client version.

See [“About corresponding NetBackup software versions”](#) on page 257.

- Use a compatible version of the NetBackup Administration Console to manage the NetBackup services.
The NetBackup Administration Console is backward-compatible. A patch release (x.x.x.x) console is compatible with a major (x.x) or minor NetBackup release (x.x.x) that shares the same first and second digits.

Upgrade time estimation

Table 13-2 Upgrade scenarios and related time estimations

Model	Upgrade path	Estimated base time	Additional time considerations
■ NetBackup Virtual Appliance with the combined primary and media server role ■ NetBackup Virtual Appliance with the media server role	3.1.1 -> 4.1	2.5 - 3 hours	The upgrade time may change due to the hardware or system load of your environment.

Pre-upgrade tasks for appliance upgrades

To prepare for an upgrade, the following tasks must be performed on each appliance that you plan to upgrade:

Run the Appliance Upgrade Readiness Analyzer

To help ensure a successful upgrade, download and run the latest available version of the Appliance Upgrade Readiness Analyzer (analyzer tool).

To download the analyzer tool, see the following article:

https://www.veritas.com/support/en_US/article.100040055

The following describes the recommended best practices for when to use the analyzer tool:

- Run the analyzer tool prior to your upgrade maintenance window.
Do this to ensure that you have enough time to implement any required changes that are reported in the analyzer tool results.
- Run the analyzer tool again right before you upgrade.
Do this to verify whether any changes within your environment since the previous analysis could impact the upgrade.

Stop all backup jobs and run a software self-test

The preflight check verifies whether there are any active jobs. To help ensure a successful upgrade, perform the following:

- Log on to the NetBackup Administration Console as the administrator.
- Before primary server upgrades, pause all jobs and any SLPs (Storage Lifecycle Policies).
- Before media server upgrades, stop all jobs that are currently running and suspend the jobs that may start during the upgrade. You must prevent jobs from attempting to start on the media server during an upgrade.
- After all jobs have been stopped or suspended and all SLPs have been paused, run the following command from the NetBackup Virtual Appliance Shell Menu for a validation test:

```
Support > Test Software
```

The software self-test result must show **Pass**.

Note: This command performs a backup and a restore test to the `/tmp` directory. If the `/tmp` directory for the appliance you are upgrading is on the NetBackup exclude list, you must remove it from that list before you run the self-test command. Otherwise, the self-test fails.

Delete previously downloaded release updates, client packages, and client add-ons

To make sure that there is enough space for the installation of the new version, all previously downloaded release updates, client packages, and client add-ons must be removed from the appliance before the upgrade.

If you do not delete the previously downloaded packages and the `/inst` directory on the appliance does not contain enough space, the preflight check notifies you of the problem and prevents the upgrade. Even if enough space exists to allow the upgrade to start, the upgrade may fail if the old client add-ons are not removed.

Note: As a best practice, always remove downloaded packages after all appliances and clients have been upgraded.

The following list describes the package removal method for appliances:

- On the appliance to be upgraded, check for all downloaded release updates and client packages by entering the following command:

```
Manage > Software  
> List Downloaded.
```

- To remove each downloaded release update and client package, enter the following command: `Manage > Software > Delete update_name`. Where `update_name` is the release update or the client package file name.
- To see a list of all downloaded client add-ons, enter the following command: `Manage > Software > List AddOns`.
- To remove each downloaded client add-on, enter the following command: `Manage > Software > Rollback eeb_name`. Where `eeb_name` is the client add-on file name.

Note: You must include the `.rpm` extension when you enter the client add-on file name.

Methods for downloading appliance software release updates

NetBackup appliance software release updates are available from the Veritas support website. Appliance software and client packages can be downloaded through the NetBackup Virtual Appliance Shell Menu or manually through a share. Updates must first be downloaded onto the appliance before you can initiate an upgrade.

The following describes the methods you can use to download appliance software release updates:

- [Downloading software updates directly to a NetBackup appliance](#)
- [Downloading software updates to a NetBackup appliance using a client share](#)

Downloading software updates directly to a NetBackup appliance

Use the following procedure to download a software release update to an appliance using the NetBackup Virtual Appliance Shell Menu.

To download software release updates directly onto the appliance

- 1 Open an SSH session and log on to the appliance as an administrator using the NetBackup Virtual Appliance Shell Menu.
- 2 To determine if a software update is available from the Veritas Support website, enter the following command:

```
Main_Menu > Manage > Software > List AvailablePatch
```

- 3 To download an available appliance software update, enter the following command:

```
Main_Menu > Manage > Software > Download
SYMC_NBAPP_update-<release-version>.x86_64.rpm
```

Where *release* is the software release number and *version* is the version number of the software release. For example:

```
Main_Menu > Manage > Software > Download
SYMC_NBAPP_update-3.1.x86_64.rpm
```

- 4 To verify that the rpm has downloaded successfully, enter the following command:

```
Main_Menu > Manage > Software > List Downloaded
```

See [“Requirements and best practices for upgrading NetBackup appliances”](#) on page 258.

See [“Downloading software updates to a NetBackup appliance using a client share”](#) on page 262.

Downloading software updates to a NetBackup appliance using a client share

Use this procedure to download the software release updates or client packages to an appliance using a CIFS or an NFS client share.

Note: If downloading the software updates directly to the appliance fails, use this method to download the appliance software release update or client package onto the appliance.

To download software release updates or client packages to the appliance using a CIFS or an NFS client share:

- 1 Open an SSH session and log on to the appliance as an administrator using the NetBackup Virtual Appliance Shell Menu.

- 2 To open an NFS or a CIFS share, enter the following command:

```
Main_Menu > Manage > Software > Share Open
```

- 3 Map or mount the appliance share directory as follows:

- Windows CIFS share

```
\\<appliance-name>\incoming_patches
```
- UNIX NFS share

```
mkdir -p /mount/<appliance-name>
mount <appliance-name>:/inst/patch/incoming
mount/<appliance-name>
```

- 4 Copy the release update or client package to the mounted share.

Note: During the copy process, do not run any commands on the appliance. Doing so can cause the copy operation to fail.

- 5 After you have successfully copied the release update or client package into the mounted share, unmap or unmount the shared directory.
- 6 On the appliance, enter the following command to close the NFS and the CIFS shares:

```
Main_Menu > Manage > Software > Share Close
```

If you run any of the following commands before you close the share, the downloaded release update or client package is moved from the share directory location to its proper location. However, you must still run the `Share Close` command to ensure that the NFS and the CIFS shares are closed.

- `List Version`
- `List Details All`
- `List Details Base`
- `Share Open`
- `Share Close`

- 7 To list the available release updates or client packages on the appliance, enter the following command and note the name of the downloaded files:

```
Main_Menu > Manage > Software > List Downloaded
```

Running this command validates and moves the release update or the client package from the share directory to its proper location. You are not notified that this move has occurred.

See [“Requirements and best practices for upgrading NetBackup appliances”](#) on page 258.

See [“Downloading software updates directly to a NetBackup appliance”](#) on page 261.

Installing a NetBackup Virtual Appliance software update using the NetBackup Virtual Appliance Shell Menu

Use the following procedure to start the appliance upgrade.

Note: If you have enabled the STIG feature on an appliance and you need to upgrade it or install an EEB on it, do not plan such installations during the 4:00am - 4:30am time frame. By following this best practice, you can avoid interrupting the automatic update of the `AIDE` database and any monitored files, which can cause multiple alert messages from the appliance.

To install a downloaded release update using the NetBackup Virtual Appliance Shell Menu

- 1 Check to make sure that the following required updates and pre-upgrade tasks have already been performed:
 - All jobs have been stopped or suspended and all SLPs have been paused.
 - The `Support > Test Software` command has been run and it returned a **Pass** result.
- 2 Log in to the NetBackup Virtual Appliance Shell Menu.

Note: Veritas recommends that you log in using the shell menu from the virtual machine console, for example, the Virtual Machine Console in the vSphere Web Client, instead of an SSH session.

- 3 Make sure that you have downloaded and have run the latest version of the Appliance Upgrade Readiness Analyzer tool. The analyzer tool must produce a `pass` result before you can continue to the next step.
- 4 To install the software release update, run the following command:


```
Main_Menu > Manage > Software > Install patch_name
```


Where *patch_name* is the name of the release update to install. Make sure that this patch name is the one that you want to install.
- 5 Monitor the preflight check and watch for any **Check failed** messages.
 - If no **Check failed** messages appear, you are prompted to continue to the next step to start the upgrade.

- If any **Check failed** messages appear, the upgrade is not allowed. You must resolve the reported failures, then launch the upgrade script again so that the preflight check can verify that the failures have been resolved.
 - If any **Check failed** messages indicate that a RHEL version third-party plug-in was not found, you must obtain the plug-in from the appropriate vendor.
- 6** After all preflight check items have passed, and before the upgrade begins, you must first select how the upgrade process should respond if any errors occur during the upgrade. The following prompt appears:

```
If an error occurs during the upgrade, do you want to
immediately enforce an automatic rollback? [yes, no]
```

Enter **yes** to immediately enforce an automatic rollback.

Enter **no** to pause the upgrade process and investigate the errors.

- 7** After all preflight check items have passed, you may need to trust the CA certificate and the host ID-based certificate to start the upgrade process.

To trust and deploy the CA certificates, do the following:

- Verify the CA certificate detail and enter **yes** to trust the CA certificate, as follows:

```
To continue with the upgrade, verify the following CA
certificate detail and enter "yes" to trust the CA certificate.
CA Certificate Details:
    Subject Name : /CN=nbatd/OU=root@abc.example.com/O=vx
    Start Date   : Jul 14 12:59:18 2017 GMT
    Expiry Date  : Jul 09 14:14:18 2037 GMT
    SHA1 Fingerprint : 31:E9:97:2E:50:11:51:7C:D6:25:7F:32:86:3D:
                        6B:D5:33:5C:11:E2
```

```
>> Do you want to trust the CA certificate? [yes, no] (yes)
```

- If the security level of the primary server is **Very High**, you must manually enter an authorization token to deploy the host ID-based certificate on the appliance, as follows:


```
>> Enter token:
```
- If the security level of the primary server is **High** or **Medium**, the authentication token is not required. The host ID-based certificate is automatically deployed onto the appliance.

For more information about security certificates, refer to the chapter "Security certificates in NetBackup" in the *NetBackup Security and Encryption Guide*.

- 8 Primary server upgrades from software versions 3.1.1 and earlier require you to provide a Veritas Usage Insights registration key. To obtain the registration key, follow the onscreen instructions.
- 9 To check the upgrade status before the **AIM** window appears, enter the following command:

```
Main_Menu > Manage > Software > UpgradeStatus
```

During the upgrade process, after the first reboot occurs, you may experience that you cannot log in to the appliance using the SSH method. This issue may exist for up to 2 hours while the upgrade proceeds. To continue monitoring the upgrade process during this time period, log in to the appliance through the VMware Remote Console. When the upgrade process has installed all of the updates, a login prompt will appear.

After the second restart, you can open the AIM window to view the upgrade progress and the estimated remaining time.

- 10 If problems are detected during the post-upgrade self-test, the **AIM** window shows the upgrade status as **Paused**. Other SSH sessions and email notifications also indicate this status.

To clear the **Paused** status, perform the following tasks:

- Press the **V** key to switch to the **Verbose** view to see the logs. If there are any Unique Message Identification (UMI) codes for the errors, search for them on the [Veritas Support website](#) to get more detailed information.
- Try to fix the problem that the **AIM** window reports.
If you need to use the shell menu, log on to the NetBackup Virtual Appliance Shell Menu through an SSH session. When the **AIM** window appears, press the **S** key to close it.
- Go back to the **AIM** window on the IPMI console.
If you tried fixing the problem, press the **A** key to attempt the self-test again. If you cannot fix the problem, contact Veritas Support or press the **R** key to roll back the appliance to the previous software version.

- 11** After the upgrade has completed, the **AIM** window shows a summary of the upgrade results.

After the disk pools are back online, the appliance runs a self-diagnostic test. Refer to the following file for the test results:

```
/log/selftest_report_<appliance_serial>_<timedate>.txt
```

If SMTP is configured, an email notification that contains the self-test result is sent.

- 12** For HA setups only:

Troubleshooting upgrade issues

If the upgrade fails or if you experience other upgrade issues, access the following information to help resolve the issues.

- [Rollback after NetBackup Virtual Appliance upgrade failure causes inactive media server](#)
- [Preflight checkpoint creation failure prevents NetBackup Virtual Appliance upgrade from starting](#)
- [Old checkpoints remain after interrupting a NetBackup Virtual Appliance upgrade or rollback](#)
- [AIM window hangs when upgrade process fails in early stages of NetBackup Virtual Appliance upgrade](#)

NetBackup client upgrades with VxUpdate

This chapter includes the following topics:

- [About VxUpdate](#)
- [VxUpdate repository management](#)
- [Deployment policy management](#)
- [Manually initiating upgrades from the primary server using VxUpdate](#)
- [Manually initiating upgrades from the client using VxUpdate](#)
- [Deployment job status](#)

About VxUpdate

Veritas introduces VxUpdate as the replacement for LiveUpdate. The main component of VxUpdate is the new deployment policy that serves as a client upgrade tool. With the release of VxUpdate, Veritas no longer supports LiveUpdate.

With support for policies, Veritas provides a simplified tool for client upgrades. No additional external tools are required and the configuration is in a familiar policy-based format, similar to a backup policy. Signed packages are verified and installed into the VxUpdate repository on the primary server. Once the packages are installed, they become available for use with deployment policies. Additionally, you can use the deployment policies to automate the installation of emergency engineering binaries, as provided by Veritas.

Note: You can only cancel queued deployment jobs. Once a VxUpdate job enters the active state it cannot be canceled.

The deployment policies are not located with the other policies in the NetBackup Administrative Console. Deployment policies are located in the NetBackup Administration Console under **Deployment Management > Deployment Policies**.

To successfully create and use deployment policies, Veritas recommends:

Table 14-1

Step	Action	Additional information
1	Populate the NetBackup repository	See “VxUpdate repository management” on page 269.
2	Create the deployment policy	See “Deployment policy management” on page 272.
3	(Optional) Manually run the upgrade from the primary server or the client	See “Manually initiating upgrades from the primary server using VxUpdate” on page 276. See “Manually initiating upgrades from the client using VxUpdate” on page 281.

VxUpdate repository management

The appliance `VxUpdate` commands control the VxUpdate package repository contents. Do not attempt to manually modify or update the repository without the use of the `VxUpdate` commands. If you populate the repository with all the client packages for all platforms, you need approximately 20 GB of space on the appliance primary server. This amount does not include any engineering binaries or hotfixes. Note that this is the approximate amount of space that is required for all packages for all platforms for each NetBackup version.

The `AddPkg` option verifies and populates the repository with supported VxUpdate client and NetBackup EEB packages. Veritas signs the VxUpdate packages. Attempts to populate the repository with unofficial or unsigned packages fails. These packages are referenced in the deployment policies that install NetBackup on target hosts. When you use the `AddPkg` option to populate the repository, be mindful of the required disk space. The primary server must have enough disk space to store packages for the NetBackup versions and platforms that are specified in deployment policies.

The package types you can load into the repository include:

- VxUpdate client packages
You can upgrade NetBackup clients to a newer version of NetBackup with VxUpdate. These packages are slightly different from standard NetBackup client

packages. The packages include additional components to support the various VxUpdate operations.

- **Emergency binaries (EEBs) and hotfixes**
You can use VxUpdate to deploy emergency binaries and hotfixes to NetBackup 8.1.2 and later clients. You can obtain VxUpdate formatted EEBs from Support in the same way you obtain traditional EEBs. These EEBs are only for NetBackup version 8.1.2 and later. Any client hotfixes that Veritas creates for NetBackup 8.1.2 and later releases include VxUpdate formatted fixes.

VxUpdate formatted packages are available from the [Veritas Support](#) licensing portal. Emergency binaries and hotfixes are obtained from the standard locations. You should download the VxUpdate versions of these packages and place them in a location accessible to the primary server. Once they are accessible to your primary server, you can add them to the VxUpdate package repository.

Downloading Veritas approved NetBackup client packages

- 1 Go to the [Veritas Support](#) licensing portal.
- 2 Enter your user name and password.
- 3 Select **Licensing**.
- 4 Enter or select your account number.
- 5 Select **Apply Filters**
- 6 Select your account number from the resulting table.

This action presents a listing of your entitlements. From here, you have the ability to download the associated software.
- 7 Select **Downloads**
- 8 Use the filter options to limit the results to the NetBackup product line and the appropriate product version.

Add your filters and select **Apply Filters**.
- 9 Under **Actions**, select the download icon
- 10 In the resulting table, select the VxUpdate packages and then select **Download**.

The client packages follow the naming convention shown:
`vxupdate_nbclient_version_operatingsystem_platform.sja`
- 11 Download the files to a local machine, then upload the files to `/inst/patch/incoming` on the appliance. Next, upload the files to the appliance as follows:
 - On the machine with the downloaded files, log in to the NetBackup Virtual Appliance Web Console and navigate to **Manage > Software Updates**.

- Select the downloaded files and upload them to the appliance.
- 12 Run the following command to verify that all packages have been downloaded and extracted:

```
Main > Manage > Software > List Downloaded
```

- 13 After you have verified that all of the downloaded and extracted packages are listed, add the packages to the NetBackup package repository.

See [the section called “Adding packages to the VxUpdate package repository”](#) on page 271.

Adding packages to the VxUpdate package repository

VxUpdate can only use the Veritas signed packages that you add to the VxUpdate package repository. Use the VxUpdate `AddPkg` option to add packages to the repository. This command also adds metadata to the EMM database and places the packages in the repository directory structure on the file system. You can use the `ListPkgs` option to list the contents of the package repository to verify that a package was added.

To add packages to the repository

- 1 On the appliance primary server, log in to the NetBackup Virtual Appliance Shell Menu as an administrator and navigate to the following menu:

```
Main > Manage > Software > VxUpdate
```

- 2 Run the `AddPkg package_name` option, where `package_name` is the client package name.

Example: `AddPkg vxupdate_nbclient_8.2_suse_ppc64le.sja`

- 3 To view the repository and verify that the package was added, run the `ListPkgs` option.
- 4 To see the package details, run the `ShowPkgDetails n` option, where `n` is the package ID number.

Deleting packages from the VxUpdate package repository

You can delete packages from the repository either when they are no longer needed or to conserve disk space. For example, delete the NetBackup 8.1.2 packages once all of the clients are upgraded to that version. Use the `DelPkg` option to delete packages. To verify that a package was deleted, use the `ListPkgs` option to list all existing packages.

To delete packages from the repository

- 1 On the appliance primary server, log in to the NetBackup Virtual Appliance Shell Menu as an administrator and navigate to the following menu:

Main > Manage > Software > VxUpdate

- 2 To view a list of the packages in the repository, run the `ListPkgs` option and take note of the ID number that identifies each package.
- 3 Run the `DelPkg ID` option to delete any unused packages.

Example: `DelPkg 1`

See [Manage > Software > VxUpdate](#) on page 359.

Deployment policy management

Use the procedures that are shown to create, modify, and delete your deployment policies.

Creating a deployment policy

Note: You must add packages to the VxUpdate repository before you can create a working deployment policy. You can create deployment policies without packages in the repository, but those policies fail to run successfully. More information about the management of the VxUpdate repository is available.

- 1 In the NetBackup Administration Console, in the left pane, select **Deployment Management > Deployment Policies**.
- 2 From the **Actions** menu, select **New Deployment Policy**.
- 3 Enter a unique name for the new policy in the **Add a New Deployment Policy** dialog box.
- 4 Click **OK**.
- 5 Specify the information that is shown on the **Attributes** tab in the **Change Deployment Policy** window:
 - **Package:** Select the package that you want deployed from the drop-down menu.

Note: Specifying a package that supports external certificate authority certificates presents you with an additional tab titled **Security**. That tab is covered later in this procedure.

- **Media server:** Specify the media server from drop-down. The media server that is specified is used to connect and transfer files to the NetBackup hosts that are included in the policy. The media server also caches the files from the NetBackup repository. The media server must be version NetBackup 8.1.2 or later. Since the repository resides on the primary server, the primary server is the default value for the media server field.
 - **Java GUI and JRE:** Specify if you want the Java GUI and the JRE upgraded on the target systems. The three options include:
 - **INCLUDE:** Install or upgrade the Java GUI and JRE components on the specified computers.
 - **EXCLUDE:** Exclude the Java GUI and JRE components from the specified computer. Any preexisting NetBackup Java GUI and JRE packages are removed.
 - **MATCH:** Preserve the current state of the Java GUI and JRE components. The components are upgraded if they are present on the pre-upgraded system. The components are not installed if they are not present on the pre-upgraded system.
 - (Conditional): Select the **Limit simultaneous jobs** option and specify a value for **jobs** to limit the total number of concurrent jobs that can run at a time. The minimum value is 1 and the maximum value is 999.
 If the check box is selected, the default value is 3. If you do not select the check box, no limit is enforced for the simultaneous upgrade jobs.
 You can set unlimited simultaneous upgrade jobs through command line interface by setting the value as 0.
 - **Select hosts:** Select hosts from the **Available hosts** list and select **Add** to add hosts to the deployment policy. The list is generated from hosts in the host database and backup policies. Once you select **Add**, the hosts are shown under **Selected hosts**.
- 6** Select the **Schedules** tab in the **Change Deployment Policy** window.
 You can see a summary of all schedules within that policy.
- 7** Select **New**.
- 8** Specify the information that is shown in the **Add Deployment Schedule** window.
- **Name:** Enter a name for the new schedule.
 - **Type:** Specify the type of schedule you want created.
 Schedule types:
 - Precheck

Performs the various precheck operations, including confirming there is sufficient space on the client for the update. The precheck schedule type does not exist for EEB packages.

- **Stage**
Moves the update package to the client, but does not install it. Also performs the precheck operation.
- **Install**
Installs the specified package. Also performs the precheck and the stage package operations. If you already performed the stage package operation, the install schedule does not move the package again.

Note: Please be aware that adding multiple different schedule types to the same deployment schedule window has unpredictable results. VxUpdate has no defined behavior to determine which schedule type runs first. If a single deployment schedule window has precheck, stage, and install jobs, there is no way to specify the order in which they run. The precheck or the stage schedules can fail, but the install completes successfully. If you plan to use precheck, stage, and install schedules, it is recommended that you create separate schedules and separate windows for each.

- **Starts:** Specify the date and time you want the policy to start in the text field or with the date and the time spinner. You can also click the calendar icon and specify a date and time in the resulting window. You can select a schedule by clicking and dragging over the three-month calendar that is provided at the bottom of the window.
- **Ends:** Specify the date and time you want the policy to end as you specified the start time.
- **Duration:** Optionally, you can specify a duration in days, hours, minutes, and seconds instead of an end time for the policy. The minimum value is 5 minutes and the maximum is 99 days.
- Select **Add/OK** and the schedule is created. Select **OK** to save and create your policy.

- 9** A **Security** tab appears when you select a deployment package that contains support for external certificate authorities.

By default, the **Use existing certificates when possible** option is selected. This option instructs NetBackup to use the existing NetBackup CA or external CA certificates, if available.

Note: If you specify this option and certificates are not available, your upgrade fails.

Deselecting the **Use existing certificates when possible** option lets you specify the location for external certificate authority information for both UNIX and Linux computers and Windows computers.

Deselecting this option does not allow the user to change the security configuration settings during the upgrade.

- 10** Windows clients have **Use Windows certificate store** selected by default.

You must enter the certificate location as *Certificate Store Name\Issuer Distinguished Name\Subject Distinguished Name*.

Note: You can use the `$hostname` variable for any of the names in the certificate store specification. The `$hostname` variable evaluates at run time to the name of the local host. This option provides flexibility when you push NetBackup software to a large number of clients.

Alternatively, you can specify a comma-separated list of Windows certificate locations. For example, you can specify:

```
MyCertStore\IssuerName1\SubjectName,
MyCertStore\IssuerName2\SubjectName2,
MyCertStore4\IssuerName1\SubjectName5
```

Then select the Certificate Revocation List (CRL) option from the radio buttons shown:

- **Do not use a CRL.** No additional information is required.
- **Use the CRL defined in the certificate.** No additional information is required.
- **Use the CRL at the following path:** You are prompted to provide a path to the CRL.

- 11** For both UNIX and Linux clients and Windows clients that select the **From certificate file path (for file-based certificates)** option, specify the information as shown:

- **Certificate file:** This field requires you to provide the path to the certificate file and the certificate file name.
- **Trust store location:** This field requires you to provide the path to the trust store and the trust store file name.
- **Private key path:** This field requires you to provide the path to the private key file and the private key file name.
- **Passphrase file:** This field requires you to provide the path of the passphrase file and the passphrase file name. This field is optional.
- Then specify the correct CRL option for your environment:
 - **Do not use a CRL.** No additional information is required.
 - **Use the CRL defined in the certificate.** No additional information is required.
 - **Use the CRL at the following path:** You are prompted to provide a path to the CRL.

To change a deployment policy

- 1 Right click on the deployment policy and select **Change**.
- 2 Navigate through the deployment policy tabs and make any necessary changes to the policy.
- 3 Select **OK** and the policy is updated.

Deleting a deployment policy

- 1 Right click on the deployment policy and select **Delete**.
- 2 Select **OK**.
- 3 Confirm the deletion of the policy.

Manually initiating upgrades from the primary server using VxUpdate

You can manually initiate upgrades with VxUpdate using one of two methods. You can manually initiate an upgrade based on an existing policy. You can also initiate an upgrade without an associated policy.

Manually initiate deployment policies when you are logged into the primary server locally and need to force an immediate update. Or you can initiate an immediate upgrade for emergency binaries. VxUpdate also provides the ability to launch upgrades from the client with the command line. More information is available.

See [“Manually initiating upgrades from the client using VxUpdate”](#) on page 281.

To manually initiate an upgrade of all clients in a policy from the administration console

- 1** In the NetBackup Administration Console, navigate to **Deployment Management > Deployment Policies**.
- 2** In the middle pane, expand the primary server, and select the policy you want to run.
- 3** Right-click on the policy you want to start, and select **Manual Deployment**.
- 4** Alternatively, after selecting the policy you want to run, you can select **Actions > Manual Deployment**.

To manually initiate an upgrade of a specific client in a policy from the administration console

- 1** Select **NetBackup Management > Host Properties > Clients** in the NetBackup Administrative Console.
- 2** Right click on the host you want to upgrade in the right pane.
- 3** Select **Upgrade Host**.
- 4** In the **Upgrade Host** dialog:
 - Select the package you want to use from the **Package** drop-down.

Note: Specifying a package that supports external certificate authority certificates presents you with an additional button titled **Configure**. That button is covered in the next step.

- Specify the type of schedule you want to run from the **Type** drop-down.
- Select the media server you want to use from the **Media server** drop-down.
- Confirm that the host you want upgraded is listed under **Selected hosts**.

- 5 (Conditional) If present, click on the **Configure** button to configure external certificate authority information.

By default, the **Use existing certificates when possible** option is selected. This option instructs NetBackup to use the existing NetBackup CA or external CA certificates, if certificates available.

Note: If you specify this option and certificates are not available, the upgrade fails.

Deselecting the **Use existing certificates when possible** option lets you specify the location for external certificate authority information for both UNIX and Linux computers and Windows computers.

Deselecting this option does not allow the user to change the security configuration settings during the upgrade.

- 6 Windows clients have **Use Windows certificate store** selected by default.

You must enter the certificate location as *Certificate Store Name\Issuer Distinguished Name\Subject Distinguished Name*.

Note: You can use the `$hostname` variable for any of the names in the certificate store specification. The `$hostname` variable evaluates at run time to the name of the local host. This option provides flexibility when you push NetBackup software to a large number of clients.

Alternatively, you can specify a comma-separated list of Windows certificate locations. For example, you can specify:

```
MyCertStore\IssuerName1\SubjectName,
MyCertStore\IssuerName2\SubjectName2,
MyCertStore4\IssuerName1\SubjectName5
```

Then select the Certificate Revocation List (CRL) option from the radio buttons shown:

- **Do not use a CRL.** No additional information is required.
- **Use the CRL defined in the certificate.** No additional information is required.
- **Use the CRL at the following path:** You are prompted to provide a path to the CRL.

- 7 For both UNIX and Linux clients and Windows clients that select the **From certificate file path (for file-based certificates)** option, specify the information as shown:

- **Certificate file:** This field requires you to provide the path to the certificate file and the certificate file name.
- **Trust store location:** This field requires you to provide the path to the trust store and the trust store file name.
- **Private key path:** This field requires you to provide the path to the private key file and the private key file name.
- **Passphrase file:** This field requires you to provide the path of the passphrase file and the passphrase file name. This field is optional.
- Then specify the correct CRL option for your environment:
 - **Do not use a CRL.** No additional information is required.
 - **Use the CRL defined in the certificate.** No additional information is required.
 - **Use the CRL at the following path:** You are prompted to provide a path to the CRL.

8 Select **OK** to launch the upgrade.

Note: You can also launch an upgrade job from the **Policies** section of the NetBackup Administrative Console. Select **NetBackup Management > Policies** in the NetBackup Administrative Console. In the middle pane, select **Clients**. Then right-click on the client you want to upgrade in the right pane and select **Upgrade Host**. Then follow the procedure shown.

To manually initiate an upgrade from the command line for all clients in a policy

Use this procedure to manually start an upgrade for all clients in a policy.

Note: This procedure starts the upgrade for all clients in the specified policy. You can start an upgrade on selected clients. More information is available.

[To manually initiate an upgrade from the command line for selected clients in a policy](#)

- 1 Open a command prompt and navigate to the directory shown:

Windows: `install_path\netbackup\bin`

UNIX or Linux: `/usr/opensv/netbackup/bin`

- 2 Use the `nbinstallcmd` command as shown to launch a policy:

```
nbinstallcmd -policy policy_name -schedule schedule
[-master_server primary]
```

Where *policy_name* is the name of the deployment policy, *schedule* is the name of the schedule, and *primary* is the name of the primary server.

To manually initiate an upgrade from the command line for selected clients in a policy

Use this procedure to manually start an upgrade for selected clients in a policy.

Note: This procedure starts the upgrade on selected clients in the specified policy. You can start an upgrade for all clients in a policy. More information is available.

[To manually initiate an upgrade from the command line for all clients in a policy](#)

- 1 Open a command prompt and navigate to the directory shown:

Windows: `install_path\netbackup\bin`

UNIX or Linux: `/usr/opensv/netbackup/bin`

- 2 Use the `nbinstallcmd` command as shown:

```
nbinstallcmd -policy policy_name -schedule schedule
{-host_filelist filename|-hosts client1, client2, clientN}
```

Where:

- *policy_name* is the name of the deployment policy
- *schedule* is the name of the schedule
- *filename* is the name of a file that contains a list of clients to upgrade.
- *client1, client2, clientN* is a list of clients to upgrade.

You can manually initiate the upgrade of a single client from the command line without an associated policy. The options required for the `nbinstallcmd` command vary depending on your security configuration. Please refer to the `nbinstallcmd` command documentation for a list of all possible options and examples of command usage.

[NetBackup Commands Reference Guide](#)

Manually initiating upgrades from the client using VxUpdate

Manually initiate deployment jobs when you are logged into the client locally and want to force an immediate update. You can either use a deployment policy to initiate an immediate upgrade or specify an upgrade without an associated policy. You can use the upgrade to update the NetBackup version or for other upgrades such as emergency binaries.

Among the reasons for a client initiated upgrade using VxUpdate is mission critical systems with specific maintenance windows. One example of these systems is database servers with limited available down time.

Note: You can only launch updates on the local client. You cannot use the `nbinstallcmd` command on a client to launch jobs on other clients. If you want to launch updates on other clients, you must initiate them from the primary server.

VxUpdate also provides the ability to launch upgrades from the primary server with the command line. More information is available.

See [“Manually initiating upgrades from the primary server using VxUpdate”](#) on page 276.

The `nbinstallcmd` version on a back-level host is not the current `nbinstallcmd` version when you initiate a non-policy based upgrade directly on the target client or media server. Refer to the [NetBackup Commands Reference Guide](#) for the currently installed version of NetBackup for the exact format of `nbinstallcmd` command.

Because of this older version of `nbinstallcmd`, exceptions to normal VxUpdate behavior include:

- If your primary server uses both NetBackup certificate and an external certificate, and your target media server or client is at NetBackup 8.1.2: Running a non-policy based upgrade directly on the target host is not supported. You must upgrade with one of the options shown:
 - Upgrade the client or the media server using VxUpdate from the primary server.
 - Create a policy on the primary server. Then run policy-based `nbinstallcmd` on the target client or media server.
 - Disable the external certificate on your primary server before starting the non-policy-based upgrade on the target host. You may turn on the external certificate after the upgrade completes successfully.

- If the client or the media server is at NetBackup 8.2 or earlier, the `-components` flag is not available. This flag was introduced in NetBackup 8.3 to enable optional installation of the NetBackup Java GUI and JRE. When you run an ad-hoc `nbinstallcmd` on a client or a media server at NetBackup 8.2 or earlier, the `-components javagui_jre` option defaults to `MATCH`. This value causes the upgrade to match the Java GUI and JRE status of the pre-upgrade host. If the pre-upgrade host had Java GUI and JRE installed, it remains installed after upgrade. If the pre-upgrade host did not have Java GUI and JRE installed, it is not installed after upgrade.

To start a client initiated deployment job based on an existing policy

- 1 Navigate to the binary directory from a command prompt.

UNIX or Linux: `/usr/openv/netbackup/bin`

Windows: `install_path\netbackup\bin`

- 2 Use the `nbinstallcmd` as shown:

```
nbinstallcmd -policy policy -schedule schedule -master_server  
name
```

Example: `nbinstallcmd -policy all_clients -schedule install812
-master_server primary1`

If the job initiated successfully, you are returned to the command prompt without an error message.

- 3 Monitor upgrade status with the NetBackup administrator and the Activity Monitor in the NetBackup Administrative Console.

You can start a client initiated deployment job without an associated policy from the command line. The options required for the `nbinstallcmd` command vary depending on your security configuration. Please refer to the `nbinstallcmd` command documentation for a list of all possible options and examples of command usage.

[NetBackup Commands Reference Guide](#)

Deployment job status

Monitor and review deployment job status in the Activity Monitor in the NetBackup Administration Console. The **Deployment** job type is the new type for VxUpdate policies. Deployment policy parent jobs that exit with a status code 0 (zero) indicate that all the child jobs successfully completed. Parent jobs that finish with a status code 1 indicate that one or more of the child jobs succeeded, but at least one failed. Any other status code indicates failure. Review the status of the child jobs to

determine why they failed. Otherwise, there are no differences between deployment jobs and other NetBackup jobs.

Your deployment job may receive a status code 224. This error indicates that the client's hardware and operating system are specified incorrectly. You can correct this error by modifying the deployment policy with the `bpplclients` command found in:

UNIX or Linux: `/usr/opensv/netbackup/bin/admincmd`

Window: `install_path\netbackup\bin\admincmd`.

Use the syntax shown:

```
bpplclients deployment_policy_name -modify client_to_update -hardware
new_hardware_value -os new_os_value
```

Deployment policies use a simplified naming scheme for operating system and hardware values. Use the values as shown for the `bpplclients` command:

Table 14-2 Deployment policy operating system and hardware

Operating system	Hardware
hpux	ia64
debian	x64
redhat	x64
suse	x64
redhat	ppc64le
suse	ppc64le
redhat	zseries
suse	zseries
aix	rs6000
solaris	sparc
solaris	x64
windows	x64

Security certificates are not deployed as part of the VxUpdate upgrade if the **Security Level for certificate deployment** is set to **Very High**. This setting is located in the **NetBackup Global Security Settings** in the NetBackup Administration Console.

If you cannot communicate with your clients after you use VxUpdate to upgrade your clients, please ensure that the proper security certificates were issued during upgrade. You may need to manually deploy the certificates. Refer to the following article that is shown for additional details:

Appliance restore

This chapter includes the following topics:

- [About appliance restore](#)
- [Creating an appliance checkpoint from the appliance shell menu](#)
- [Rollback to an appliance checkpoint from the appliance shell menu](#)
- [About NetBackup Virtual Appliance factory reset](#)
- [Factory reset best practices](#)
- [How to factory reset the NetBackup Virtual Appliance](#)

About appliance restore

Appliance Restore implies that you want to restore the appliance to a specific state. That state can be an original factory state or a state that is determined through the use of checkpoints. You can create a checkpoint, rollback the appliance to a checkpoint that you choose, or initiate a factory reset.

Note: Factory reset is not supported on a NetBackup Virtual Appliance with the primary server role.

The following list describes the four different types of checkpoints:

- A factory reset checkpoint. This checkpoint is created after a newly deployed appliance is first boot up. This checkpoint creation process takes about 15 minutes.
- A pre-upgrade checkpoint is created before you install a software upgrade. You can use this type of checkpoint as a rollback checkpoint in case a software upgrade fails.

- A user-directed checkpoint is created after an appliance has been upgraded to a new software version. A user-directed checkpoint is a checkpoint that you create at any point in time using the application user interface. If an existing user-directed checkpoint already exists it is replaced by any new checkpoint that you create.

See [“Creating an appliance checkpoint from the appliance shell menu”](#) on page 286.

See [“Rollback to an appliance checkpoint from the appliance shell menu”](#) on page 288.

See [“How to factory reset the NetBackup Virtual Appliance”](#) on page 292.

Creating an appliance checkpoint from the appliance shell menu

Use the following procedure to create a user-directed checkpoint from the appliance shell menu.

Note: If a user-directed checkpoint already exists, the checkpoint that you are about to create replaces the existing checkpoint. Only one user-directed checkpoint can exist at any given time.

To create a new checkpoint from the appliance shell menu

- 1 Log on to the appliance as an administrator and open the appliance shell menu.
- 2 Enter the following command to

```
Main_Menu > Support > Checkpoint Create
```

The following interactive process begins. The shell menu informs you of any existing checkpoints before you can create a new checkpoint. In the following example, no existing checkpoints exist.

```
Creating an Appliance Checkpoint allows the user to easily
rollback the entire system back to a point-in-time to undo any
misconfiguration or system failure that might have occurred. An
Appliance Checkpoint captures the following components:
```

- 1) Appliance Operating System
- 2) Appliance Software
- 3) NetBackup Software
- 4) Networking Configuration
- 5) Any previously applied patches
- 6) Backup data is not reverted

```
There are no checkpoints in the system.
```

```
There is no user checkpoint. Please continue to create a user checkpoint
```

```
>> Would you like to proceed? (yes/no) yes
```

- 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.

```
- [Info] Deleting checkpoint: USER
- [Info] CREATING USER CHECKPOINT
- [Info] Creating checkpoint. This operation can take 10 to
15 minutes.
```

```
Please wait...
```

```
- [Info] Appliance Checkpoint creation was successful
```

Rollback to an appliance checkpoint from the appliance shell menu

The following procedure describes how to roll back an appliance to a checkpoint from the appliance shell menu.

To roll back to an existing checkpoint from the appliance shell menu

- 1 Log on to the appliance as an administrator and open the appliance shell menu.
- 2 Enter the following command:

```
Main_Menu > Support > Checkpoint Rollback
```

The following interactive process begins. The 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) Networking Configuration
- 5) Any previously applied patches
- 6) 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 2016  
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.

A reboot of the appliance is required to complete the
checkpoint rollback. Reboot automatically after rollback (yes/no)?

Automatically rebooting the appliance after the rollback will not
provide you with an opportunity to review the progress/final
status of the rollback. Are you sure you would like to automatically
reboot the appliance (yes/no) yes

- 5 Enter **Yes** a second time to confirm that you want to restart the appliance automatically after the rollback operation completes.

ROLLBACK OPTIONS AND SUMMARY

Rollback to checkpoint name : [USER]

Auto reboot after rollback? : [YES]

Appliance will make the following version changes:

+-----+			
Appliance	Current Version	Reverted Version	
+-----+			
nb-appliance	NetBackup 8.1Beta7	NetBackup 8.1Beta7	
	Appliance 3.1	Appliance 3.1	
+-----+			

- 6 Enter **Yes** to begin the rollback to a checkpoint operation.

The following status is provided once the rollback operation is started.

Rollback to checkpoint? (yes/no) yes

- [Info] Stopping NetBackup Services...please wait.
- [Info] PERFORMING REVERT TO USER CHECKPOINT
- [Info] This takes approx. 15 to 20 mins. Please wait...
- [Info] Rollback to Appliance Checkpoint (User directed checkpoint) successful.

A reboot of the appliance is required to complete the checkpoint rollback. Reboot now? (Type REBOOT to continue) REBOOT
Rebooting the appliance now...

- [Info] Rebooting app2.Veritas.com

Please reconnect to the appliance shell menu to continue using this appliance.

The system is going down for reboot NOW!

About NetBackup Virtual Appliance factory reset

The purpose of an appliance factory reset is to return your appliance to a clean, unconfigured, and factory state. By default, a factory reset discards all storage configuration and backup data. However, before you initiate the factory reset, you

can elect to retain the storage configuration, network configuration and backup data if any currently exists. In addition, you can elect to restart the appliance after the reset completes.

Note: This operation is not supported on a NetBackup Virtual Appliance primary server.

Note: If you run a factory reset of the appliance, note the following:

A factory reset disables WAN optimization for all network interface bonds if you retain your network configuration. After the factory reset completes, you can then enable WAN optimization again for the network interface bonds.

If you *do not* 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.

The following components are reset:

- Appliance operating system
- Appliance software
- NetBackup software
- Any applied patches
- (Optional) Networking configuration
- (Optional) Storage configuration and data

See [“How to factory reset the NetBackup Virtual Appliance”](#) on page 292.

Factory reset best practices

This topic contains best-practice information about factory reset operations.

- If you choose the Storage Reset option during a factory reset, the data or storage may not be deleted. This situation happens if one or more partitions are in use or some processes continue to access the partition. To remove the storage in this scenario, run the `Support > Storage Reset` command after performing a factory reset.

The following is an example of an error message that is displayed when storage is not reset:

- [Error] Failed to unmount the 'Configuration' partition '0' because the partition is currently in use. Restarting the appliance and retrying the operation may help to resolve the issue. Contact Veritas Technical Support if the issue persists.

Note: The Storage Reset command is only available when the appliance is in a factory state.

- Make sure to stop all running backup, duplication, or restore jobs before performing a Factory Reset. NetBackup storage objects, storage units, disk pools, and storage servers on the primary server that belong to the media server appliance are not cleaned up if a Factory Reset operation is performed while backup, duplication or restore jobs are still in progress.

How to factory reset the NetBackup Virtual Appliance

Note: Factory reset is not supported on a NetBackup Virtual Appliance primary server.

The following procedure describes how to start a factory reset operation from the appliance shell menu.

Note: A factory reset operation returns the password to the original, default value.

To begin a factory reset from the appliance shell menu

- 1 Log on to the appliance as an administrator and open the appliance shell menu.
- 2 Enter `Main_Menu > Support > FactoryReset`. This command shows the following messages and requires you to answer the following questions before the factory reset begins.

```
- [Info] Disable interrupt (CTRL-C), quit, and suspend signals
+-----+
|  Appliance Factory Reset  |
+-----+

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) Networking configuration (optionally retain)
5) 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, MSDP, and Share partitions.
    -- Resets the storage partitions.
- [Warning] Performing a factory reset interrupts all share activity and removes
and resets all share data. Unmount all the shares on clients before continuing
with this operation.
>> Do you want to delete images and reset backup data? [yes/no] (yes) 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) 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 **Factory Reset Summary** is shown. The following is an example of the summary:

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]
```

```
>> WARNING: An appliance factory reset cannot be reversed! Continue
with factory reset?? (yes/no)
```

- 4 The following warning appears. If you want to begin the factory reset operation, enter **Yes**.

```
WARNING: An appliance factory reset cannot be reversed!
Continue with factory reset?? (yes/no) yes
```

The factory reset continues and info messages are shown.

Next steps

After the factory reset is complete, do one of the following:

- If you reset both the network configuration and the storage configuration, perform the initial configuration again with the `Main > Appliance > Configure` command.
- If you reset the network configuration but did not reset the storage configuration, run the following commands to reconfigure the IP address, hostname, and appliance role:

```
Main Menu > Network > Configure IPAddress Netmask GatewayIPAddress
[InterfaceNames]
```

```
Main > Network > Hostname Set Name
```

```
Main > Appliance > Media PrimaryServer
```

- If you did not reset the network configuration, run the following commands to reconfigure the hostname and appliance role:

```
Main > Network > Hostname Set Name
```

```
Main > Appliance > Media PrimaryServer
```

See [“About NetBackup Virtual Appliance factory reset”](#) on page 290.

Decommissioning and Reconfiguring

This chapter includes the following topics:

- [About decommissioning a NetBackup Virtual Appliance](#)
- [Decommissioning a NetBackup Virtual Appliance with the media server role](#)

About decommissioning a NetBackup Virtual Appliance

To decommission an appliance means to remove or eliminate the appliance from the backup environment. When you decide which appliance to decommission, you must make sure that the appliance is not configured as a backup destination for any clients.

You may need to decommission an appliance for any of the following reasons:

- The appliance has issues and needs to be reset to factory settings.
- The appliance is no longer needed (down-sizing your backup environment).
- The appliance may need to be removed from the network domain for troubleshooting.

After you determine that you need to decommission a media appliance, you can provision a new appliance to act as a target for all backups. With this technique the load is decreased on the existing appliance and moved to the new appliance. The existing can be removed from the domain eventually.

Decommissioning a NetBackup Virtual Appliance with the media server role

When you decommission a media server appliance it means all of the backup images that are stored on the disk are lost. You can use Factory Reset command to decommission and reset a NetBackup Virtual Appliance media server.

To decommission a media server appliance

- 1 Open an SSH session on the media server appliance.
- 2 Log on as admin.
- 3 Run the following command and follow any additional prompts to reset the appliance to factory default settings.

```
Main_Menu > Support > FactoryReset
```

To decommission a non-appliance media server, you must log in to the NetBackup Virtual Appliance Shell Menu from a primary appliance. Use the procedure below to decommission a non-appliance media server.

To decommission a non-appliance media server

- 1 Open an SSH session to the primary appliance.
- 2 Log on as admin.
- 3 Enter the following command to remove media appliance:

```
Main_Menu > Appliance > Remove MediaServer TargetMediaServer
```

The variable *MediaServer* is the host name of the non-appliance media server that you want to decommission. Specify **NONE** for the *TargetMediaServer* variable.

- 4 Enter *Yes*, to confirm that you want to remove this media server.

Note: If the media server that you are about to decommission has a deduplication pool storage unit configured, you must manually expire the images on that storage unit before you attempt to remove the media server.

- 5 From the decommissioned media server, run the following command and follow any additional prompts to reset the appliance to factory default settings.

```
Main_Menu > Support > FactoryReset
```


Troubleshooting

This chapter includes the following topics:

- [About troubleshooting the NetBackup Virtual Appliance](#)
- [About contacting Technical Support](#)
- [Determining the NetBackup Virtual Appliance serial number](#)
- [About disaster recovery](#)
- [About NetBackup support utilities](#)
- [Troubleshooting NetBackup Virtual Appliance initial deployment issues](#)
- [Error messages displayed on the NetBackup Virtual Appliance Shell Menu](#)
- [NetBackup status codes applicable for NetBackup Virtual Appliance](#)
- [Installing an EEB](#)
- [Rolling back an EEB using the NetBackup Virtual Appliance Shell Menu](#)

About troubleshooting the NetBackup Virtual Appliance

If you experience any issues with your NetBackup Virtual Appliance, use the following steps as a guide to help you resolve the problem. You can also find troubleshooting information for specific issues from the [Appliances page](#) on the Technical Support website. Use the search function to look for articles relating to your particular issue.

If you cannot resolve the problem on your own, it is important that you can define the problem and collect any supporting information. When you reach this point, you

should contact Technical Support. A technical support representative works with you to diagnose the problem and produce a satisfactory resolution.

Table 17-1 Steps for troubleshooting NetBackup Virtual Appliance problems

Step	Action	Description
Step 1	Note the error message	To note what has gone wrong with the appliance you can use the following options: ■ Error messages are usually the vehicle for telling you something went wrong. Refer to the appliance error message documentation and confirm the recommended action. See “Error messages displayed on the NetBackup Virtual Appliance Shell Menu” on page 312. ■ If you don’t see an error message in an interface, but still suspect a problem, you can: ■ Check the NetBackup Virtual Appliance reports and logs. The logs show you what went wrong and the operation that was ongoing when the problem occurred. See “About NetBackup Virtual Appliance log files” on page 321.
Step 2	Identify what you were doing when the problem occurred	Ask the following questions: ■ What operation was tried? ■ What method did you use? For example, more than one way exists to install software on a client. Also more than one possible interface exists to use for many operations. Some operations can be performed with a script. ■ If a client was involved, what type of client was it? ■ Have you performed the operation successfully in the past? If so, what is different now? ■ What is the software version level? ■ Do you use operating system software with the latest fixes supplied?

Table 17-1 Steps for troubleshooting NetBackup Virtual Appliance problems
(continued)

Step	Action	Description
Step 3	Record all information	Capture potentially valuable information: ■ Progress logs ■ Reports ■ Utility Reports ■ Debug logs ■ Check for error or status messages in the system log and Event Viewer application in case of a Windows computer. Note: To start the Event Viewer, from the Start menu, click All Programs > Administrative Tools > Event Viewer. ■ Error or status messages in dialog boxes See “About NetBackup Virtual Appliance log files” on page 321.
Step 4	Correct the problem	If you define the issue as a NetBackup Virtual Appliance issue, you can find additional troubleshooting information from the Appliances page on the Technical Support website. Use the search bar at the top of the page to look for articles relating to specific issues. If you define the issue as a NetBackup issue, you can use the following information to correct it: ■ Take the corrective action as recommended by the status code or message. See “NetBackup status codes applicable for NetBackup Virtual Appliance” on page 317. For more information, refer to the <i>NetBackup Status Code Reference Guide</i>. ■ If no status code or message exists, or the actions for the status code do not solve the problem, use additional troubleshooting procedures to isolate common problems. See “About NetBackup support utilities” on page 306. See the <i>NetBackup Troubleshooting Guide</i> for additional information specific to NetBackup.
Step 5	Complete a problem report for Technical Support	If you can identify the logs that can help resolve the issue, collect the appropriate logs. If you cannot identify the required logs for resolving the problem, contact Technical Support to get advice on which logs to collect. If your troubleshooting is unsuccessful, prepare to contact Technical Support by filling out a problem report. See “About contacting Technical Support” on page 300. See “About NetBackup Virtual Appliance log files” on page 321.

Table 17-1 Steps for troubleshooting NetBackup Virtual Appliance problems
(continued)

Step	Action	Description
Step 6	Contact Technical Support	The Veritas Technical Support website has a wealth of information that can help you solve NetBackup Virtual Appliance problems. Access Technical Support at the following URL: www.veritas.com/support See “About contacting Technical Support” on page 300.

See “About disaster recovery” on page 302.

See “Enabling and disabling VxMS logging” on page 325.

About contacting Technical Support

The Technical Support website has a wealth of information that can help you solve NetBackup Virtual Appliance problems. You can access Technical Support at the following URL:

www.veritas.com/support

When you report an issue to Support, keep the following information at hand:

- Run the `Monitor > Hardware ShowHealth Appliance [Product]` command to detect the serial number of your appliance and note it down for future use.
See “Determining the NetBackup Virtual Appliance serial number” on page 301.
- Refer to the appliance error message documentation and confirm the recommended action.
See “Error messages displayed on the NetBackup Virtual Appliance Shell Menu” on page 312.
See “NetBackup status codes applicable for NetBackup Virtual Appliance” on page 317.
- Gather device logs using the `Datacollect` command.
See “Gathering device logs on a NetBackup virtual appliance” on page 326.
- Ensure that Call Home is enabled and the proxy settings provided are correct.
See “Enabling and disabling Call Home from the appliance shell menu” on page 216.
See “Configuring a Call Home proxy server from the NetBackup Virtual Appliance Shell Menu” on page 217.

See “About troubleshooting the NetBackup Virtual Appliance” on page 297.

Determining the NetBackup Virtual Appliance serial number

The serial number of a virtual appliance is assigned by the AutoSupport servers. After the initial configuration of an appliance, the serial number is not assigned.

```
Compute Node abc.veritas.com

Time Monitoring Ran: Thu Nov 02 2016 22:10:10 PDT
```

Hardware monitor information		
Name	Manufacturer	Serial
NBU VA ROBO	Veritas	Not Assigned

- Before you determine the serial number, you need to make sure the following:
- CallHome is enabled on your appliance.
 - The appliance has access to public network either directly or through a proxy to the AutoSupport servers.

When you connect your appliance to public network, AutoSupport detects the appliance through Call Home service and a serial number is assigned to your appliance.

Use the following procedure to determine the serial number of an appliance using the NetBackup Virtual Appliance Shell Menu.

To determine the serial number of an appliance server using the NetBackup Virtual Appliance Shell Menu

- 1 Log on to the administrative NetBackup Virtual Appliance Shell Menu using your login credentials.
- 2 From the `Main_Menu>` command prompt, type `Monitor` and press **Enter**.

The command prompt changes to `Monitor>`.

- 3 Type the following command: `Hardware ShowHealth Appliance Product`, and then press **Enter**.

For example, `Monitor> Hardware ShowHealth Appliance Product`

The serial number of your appliance appears, as seen in the following example:

```
Compute Node abc.veritas.com
```

```
Time Monitoring Ran: Thu Nov 03 2016 22:53:49 PDT
```

```
+-----+
|           Hardware monitor information           |
|+-----+-----+-----+-----+-----+-----+ |
|| Name           | Manufacturer | Serial           | |
|+-----+-----+-----+-----+-----+-----+ |
|| NBU VA ROBO    | Veritas      | VRTSV1FE80404849 | |
|+-----+-----+-----+-----+-----+-----+ |
|                                                         |
+-----+
```

See [“About troubleshooting the NetBackup Virtual Appliance”](#) on page 297.

See [“About contacting Technical Support”](#) on page 300.

About disaster recovery

Numerous situations can cause fatal conditions and result in the need for disaster recovery. In a disaster recovery situation, it is critical to determine the cause of the disaster and recover as much data from the appliance as possible. Therefore, before you attempt to recover your appliance, contact Technical Support.

The environment that you have configured around your appliance plays an important role on the level of recovery you can achieve. An environment that consists of a standalone appliance offers the least number of recovery solutions. However, the appliance offers solutions to help you replicate your backup data to another location so that there is a much better chance that it can be recovered.

To protect the NetBackup catalog, use the following solutions:

- For appliances with the combined primary and media server role
 By default, the appliance creates an inactive backup policy that uses a Storage Lifecycle Policy (SLP) to protect the NetBackup catalog. The SLP backs up the data to AdvancedDisk and then duplicates it to MSDP. You are then able to use Auto Image Replication to save your catalog backup off site. Veritas recommends that you use this replication-based strategy for disaster recovery (DR) due to the combined primary and media server role of the appliance. To use this catalog backup policy, you need to activate it in the NetBackup Administration Console.
- For appliances with the primary server role
 By default, the primary server appliance does not contain a catalog backup policy. To protect the NetBackup catalog, configure a catalog backup before using NetBackup for regular client backups.

Veritas recommends that you review the following sections from within the NetBackup documentation before you operate the appliance:

- *NetBackup Administration Guide, Volume I*
 - In Section 5, "Configuring Backups", review the following topics:
 - "Creating backup policies"
 - "Protecting the NetBackup Catalog"
 - "Strategies that ensure successful NetBackup catalog backups"
 - Review the topics within Section 3, "Configuring Storage".
- *NetBackup Troubleshooting Guide*
 Review Chapter 8, "Disaster Recovery" for help with understanding disaster recovery fundamentals.

The Troubleshooting Guide is located at the following location:

<http://www.veritas.com/docs/DOC5332>

See ["About the NetBackup Virtual Appliance deduplication pool catalog backup policy"](#) on page 113.

See ["About troubleshooting the NetBackup Virtual Appliance"](#) on page 297.

See ["Recovering a NetBackup appliance primary server using NetBackup catalog restore"](#) on page 303.

Recovering a NetBackup appliance primary server using NetBackup catalog restore

This section details how to recover a NetBackup Virtual Appliance primary server using the NetBackup catalog restore function.

The following information is mandatory to complete this task:

- Copy of the NetBackup catalog from the affected primary server.

Note: Make sure to set the passphrase for the NetBackup catalog backup policy. The passphrase is needed for a catalog recovery.

- Host name of the affected primary server.
- Network configuration.
- Time zone of the affected primary server.

Note: This procedure requires that you have a copy of your NetBackup catalog stored on a separate server or computer. You need the catalog backup to recover the affected primary server.

To recover an appliance primary server using NetBackup catalog restore

- 1 Once you have completed the deployment, log on to the NetBackup Virtual Appliance Shell Menu on the primary server and create an NetBackup CLI user.


```
Main_Menu > Manage > NetBackupCLI > Create
```
- 2 Copy the NetBackup catalog files that were stored off-site onto the primary server.
- 3 Log out of the NetBackup Virtual Appliance Shell Menu, then log on as the NetBackup CLI user you created earlier.
- 4 Run `bp.kill_all`.
- 5 Run `nbhostidentity -import -infile` with the package file of the `.drpkg`
- 6 Run `bp.start_all`, then verify that the token, certifications, and security settings have been restored.
- 7 Perform the initial configuration on the appliance.

Note: Make sure to keep the same host name and time zone of the primary as before the disaster.

- 8 Run `bpsetconfig` to add the line: `MEDIA_SERVER=<media_server_name>` and register media servers on the new primary server. Use `Ctrl + D` to exit and save this entry.

9 Run `nbemmcmd` to add the media server's record to the EEM database manually:

```
nbemmcmd -addhost -machinename <media_server_name> -machinetype
media -primarieserver <primary_server_name> -operatingsystem linux
-netbackupversion <NetBackup_version>
```

10 Restart the NetBackup services on the media server.

Note: To ensure proper communication between the primary and the media server, you must perform this step before you create the MSDP storage information on the media server as described in the following step.

11 Create the media server AdvancedDisk and MSDP storage information using the following commands:

■ **AdvancedDisk**

```
nbdevconfig -creatests -storage_server <media_server_name>
-stype AdvancedDisk -media_server <media_server_name> -st 5
nbdevconfig -createdp -dp dp_adv_<media_server_name> -stype
AdvancedDisk -storage_servers <media_server_name> -dvlist
dvlist.txt
bpstuaadd -label stu_adv_<media_server_name> -dp
dp_adv_<media_server_name> -cj 20 -odo 1 -okrt 0 -nodevhost
-M <primary_server_name>
```

■ **MSDP**

```
nbdevconfig -creatests -storage_server <media_server_name>
-stype PureDisk -media_server <media_server_name> -st 9
nbdevconfig -createdp -dp dp_disk_<media_server_name> -stype
PureDisk -storage_servers <media_server_name> -dvlist
dvlist.txt
bpstuaadd -label stu_disk_<media_server_name> -dp
dp_disk_<media_server_name> -cj 20 -odo 1 -okrt 0 -nodevhost
-M <primary_server_name>
```

12 Restore the NetBackup catalog by performing one of the following actions:

- Run the `bprecover -wizard` command.
- Use the NetBackup Catalog Recovery Wizard in the NetBackup Administrator's Console.

13 Run `bp.kill_all` and `bp.restart_all` to finish recovering the primary server.

14 Synchronize the MSDP storage server password as follows:

- For software versions 3.3.0.1 and later, log in to the appliance shell menu on the primary server and run the following command:

```
Main_Menu > Appliance > ShowDeDupPassword
```

- For software versions 3.1 through 3.2, log in to the appliance shell menu on the primary server and run the following command:

```
Main_Menu > Appliance > ShowDeDupPassword
```

Log in to the appliance primary server as a NetBackup CLI user and run the following command:

```
tpconfig -update -storage_server <primary host name> -stype  
PureDisk -sts_user_id root -media_server <primary hostname>,  
then enter the dedupe password from the previous command output.
```

About NetBackup support utilities

The NetBackup Virtual Appliance provides the following support utilities to help diagnose NetBackup problems:

- [NetBackup Domain Network Analyzer \(NBDNA\)](#)
- [NetBackup Support Utility \(NBSU\)](#)

See “[NetBackup status codes applicable for NetBackup Virtual Appliance](#)” on page 317.

See “[About troubleshooting the NetBackup Virtual Appliance](#)” on page 297.

NetBackup Domain Network Analyzer (NBDNA)

You can run the NBDNA utility on a NetBackup Virtual Appliance to perform the following tasks:

- Identify the NetBackup domain configuration to resolve network-related issues
- Identify NetBackup performance issues
- Ensure the behavior of the host name lookup is functional
- Ensure that the connectivity between NetBackup hosts and the appliance is established and functional based on their role within the NetBackup domain
- Generate the reports that are meant for Veritas Technical Support.

The NBDNA utility provides the following types of information in its output:

```
Running audit as Media Server.
```

```
Collection Version: x.x
```

```
Collection Time: Tuesday, October 7, 2010 at 19:17:11 PM
      NBU Release: NetBackup-RedHat2.6.18 7.7.1
      NBU Version: 7.7.1
NBU Major Version: 7
NBU Minor Version: 7
NBU Release Update: 1
      NBU Patch Type: Release Update
      NBU GlobDB Host: "host name"
      Is GlobDB HOST? No
      UNAME:
      Hostname: sample.name.veritas.com
      Host's Platform: Linux
      Perl Architecture: Linux
```

Initialization completed in 14.040101 seconds.

Brief Description of What It Does (for type 1):

- ```

```
- 1) Perform basic self checks.
  - 2) Check connectivity to Primary (and EMM) server.
  - 3) If SSO configured, get list of media servers sharing devices.
  - 4) Get list of all clients which could send data here for backup.
  - 5) Test NBU ports for basic connectivity between media servers sharing devices.
  - 6) Test NBU ports for basic connectivity between media server and clients it backs up.
  - 7) Perform service level tests for phase 2
  - 8) Capture data for reports; save reports.
  - 9) Save data to report files.
- ```
-----
```

Discovering and mapping the NetBackup domain network for analysis by extracting data from current system's configuration.

(To see more details, consider using '-verbose' switch.)

Probing Completed in 2.867581 seconds.

Initiating tests...

COMPLETED. Thank you for your patience.

```
/log/dna/sample.name.veritas.com.NBDNA.20100907.191711.zip
Archive created successfully!
Return /log/dna/sample.name.veritas.com.NBDNA.20100907.191711.zip
to Veritas Support upon request.
```

See [Support > NBDNA](#) on page 549.

See [“NetBackup Support Utility \(NBSU\)”](#) on page 308.

See [“About troubleshooting the NetBackup Virtual Appliance”](#) on page 297.

NetBackup Support Utility (NBSU)

You can use the `NBSU` utility to gather appropriate diagnostic information about NetBackup and the operating system.

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 the appropriate diagnostic information based on the operating system and the NetBackup environment.

You can use the `Support > NBSU` command to create or remove the NetBackup configuration support files that the NBSU utility uses.

See [Support > NBSU](#) on page 555.

See [“NetBackup Domain Network Analyzer \(NBDNA\)”](#) on page 306.

See [“About troubleshooting the NetBackup Virtual Appliance”](#) on page 297.

Troubleshooting NetBackup Virtual Appliance initial deployment issues

Before you can begin troubleshooting a NetBackup Virtual Appliance initial deployment failure, you need to determine when the problem occurred. A failure can occur during either of the following processes:

- The OVF deployment wizard operations in the vSphere Client or the vSphere Web Client

If an error occurs in the OVF deployment wizard, the only way to fix it is to restart the deployment. Before you do so, make sure that you verify the information that you entered in the deployment wizard. You can also reference the VMware documentation for help with specific error messages.
- The NetBackup Virtual Appliance automatic configuration

Note: This only applies to the combined primary and media server.

If an error occurs during the automatic configuration process, the OVF deployment wizard behaves as if the deployment was successful. However, if you log on to the NetBackup Virtual Appliance Shell Menu and run the `Main > Appliance > Status` command, the appliance appears to be in a factory state and is not configured as a primary appliance.

The following are a few common reasons for the automatic configuration to fail:

- Typos in the deployment wizard
- Incorrect IP addresses
- Incorrect host name or DNS information

You can check the `boot` log for additional details to help determine the exact error that occurred. Use the following steps to view the `boot` log:

- Log on to the NetBackup Virtual Appliance Shell Menu and enter the `Main > Support > Logs > Browse` command.
- At the `LOGROOT/>` prompt, enter `cd OS` and then `less boot.log`.

The most straightforward method to resolve configuration errors is to redeploy the appliance, making sure that you enter the correct information in the deployment wizard.

However, if you have encountered multiple failures or want to try to resolve the issue from the NetBackup Virtual Appliance Shell Menu, use the following procedure to manually complete the configuration process.

- If errors did not occur during the initial deployment, but during the initial configuration from the shell menu, you need to record the UMI code and refer to the corresponding technical article on the support website.

To manually configure the appliance networking from the NetBackup Virtual Appliance Shell Menu

Note: This procedure only applies to the combined primary and media server.

- 1 Open an SSH session to the appliance to log on to the NetBackup Virtual Appliance Shell Menu.

The logon is `admin`, and the default password is `P@ssw0rd`.

If you cannot open an SSH session to the appliance, you can attempt to log on from the vSphere (Web) Client. Navigate to the deployed appliance and select the **Console** tab to access the shell menu.

If you still cannot log on, return to the OVF deployment wizard and redeploy the appliance.

- 2 Navigate to the `Main > Network` view and enter the following command to configure the IP address of a single network that you want your appliance to connect to:

```
Configure IPAddress Netmask GatewayIPAddress eth1
```

Where *IPAddress* is the new IP address, *Netmask* is the netmask that corresponds to the IP address, and *GatewayIPAddress* is the IP address of the default gateway for the interface.

The *IPAddress* and the *GatewayIPAddress* can be an IPv4 or IPv6 address. Only global-scope and unique-local IPv6 addresses are allowed.

Remember that you should not use both IPv4 and 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`

- 3 From the `Main > Network` view, use the following command to set the appliance DNS domain name:

```
DNS Domain Name
```

Where *Name* is the new domain name for the appliance.

- 4 From the `Main > Network` view, use the following command to add the DNS name server to your appliance configuration:

```
DNS Add NameServer IPAddress
```

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

The address can be either IPv4 or IPv6. Only global-scope and unique-local IPv6 addresses are allowed.

- 5 From the `Main > Network` view, use the following command to set the host name for your appliance:

```
Hostname Set Name
```

Where *Name* is a short host name or a fully qualified domain name (FQDN) for the appliance. As a best practice, Veritas recommends that you use FQDN.

Note: If you plan to configure Active Directory (AD) authentication on this appliance, the host name must be 15 characters or less. Otherwise, AD configuration can fail.

- 6 Use one of the following commands to set the role of the appliance:

```
Main > Appliance > Primary
```

```
Main > Appliance > Media
```

You are prompted to change the default passwords.

Change each user account password as prompted.

Review the following password policy before setting a new password:

- Passwords must contain at least eight characters.
- Passwords must contain at least one lowercase letter (a-z) and one number (0-9).
- Dictionary words are considered weak passwords and are not accepted.
- The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.

Note: If you enter five consecutive invalid passwords for any user account, the appliance aborts the role configuration process automatically. You must run the command again.

Note: If you enable the STIG feature after completing the initial configuration, you may be prompted to change the new passwords you entered here to meet the requirements of the STIG password policy.

- 7 Use the following command to verify that the networking and the role configuration were successful:

```
Main > Appliance > Status
```

The command output should contain a message similar to the following:

```
Appliance Version is 4.1.
```

```
Appliance is configured as primary appliance.
```

- 8 If this appliance is a NetBackup Virtual Appliance primary server, run the following command to resize the NetBackup catalog to 900 GB:

```
Main > Manage > Storage > Resize NetBackupCatalog 900 GB
```

- 9 If everything completed successfully, return to the initial deployment procedure and complete the remaining steps for the appliance configuration.

If none of these steps resolved your issue, you can find additional troubleshooting information for specific appliance issues from the [NetBackup Virtual Appliance page](#) on the Veritas Support website. Use the search bar at the top of the page to look for articles relating to specific issues.

If you still need assistance, contact Veritas Support.

See [“About contacting Technical Support”](#) on page 300.

See [“About troubleshooting the NetBackup Virtual Appliance”](#) on page 297.

Error messages displayed on the NetBackup Virtual Appliance Shell Menu

[Table 17-2](#) lists some of the common error messages that you may come across while working from the NetBackup Virtual Appliance Shell Menu:

Table 17-2 Common error messages in the NetBackup Virtual Appliance Shell Menu

Error messages	Explanation / Recommended action
Failed to get NetBackup version	Make sure that the NetBackup services are up and running on the appliance. If you encounter this issue, restart the NetBackup services.

Table 17-2 Common error messages in the NetBackup Virtual Appliance Shell Menu *(continued)*

Error messages	Explanation / Recommended action
Failed to access disk storage	This problem can arise due to multiple issues. For example, if the disks are offline or the disk volume is disabled. In these scenarios: ■ Collect <code>DataCollect</code> log ■ Check <code>/log/app_vxul/409-9-*.log</code> for the actual disk group and volume-related errors.
Failed license check for AdvancedDisk storage	Make sure that a valid license for the NetBackup Flexible Disk Option is installed on the media server.
Failed license check for Deduplication storage	Make sure that a valid license for NetBackup Deduplication Option is installed on the media server
Failed to create Deduplication storage unit	Check if the storage unit or the corresponding disk volume already exists on the media server. If they do exist, verify if the storage unit or the corresponding disk volume is currently used. If the storage is redundant only then use the NetBackup Administration Console or the <code>nbdecommission</code> utility to delete them. These tools are available on the NetBackup primary server. Check the NetBackup Virtual Appliance VxUL (unified) logs with the <code>Support > Logs > VxLogView Module ALL</code> command for more precise error information.

[Table 17-3](#) lists error messages that are specific to the `Manage > Software view` commands.

Table 17-3 Manage > Software view

Error message	Explanation	Recommended action
The installation failed because the patch does not exist or you did not run the <code>List downloaded</code> command to check for the downloaded patch.	The installation has failed as the patch you are trying to download does not exist or is not up-to-date.	Please identify and try to install the correct patch on the appliance. Run the <code>List downloaded</code> command to check for the downloaded patch and install the correct patch.
	The source of the error cannot be found.	Please contact Veritas Technical Support.
Invalid Appliance mode.	The appliance mode in <code>bp.conf</code> file is not correct.	Please check the appliance mode in <code>bp.conf</code> and contact Veritas Support.

Table 17-3 Manage > Software view (*continued*)

Error message	Explanation	Recommended action
Please provide a valid EEB name.	This error message is only for the rollback of EEB. The EEB name is not valid.	Please check that the EEB name you have used.
Patch <code><rpm name></code> signature check failed.	Signature error found in the <code>rpm</code> (installer package) .	Please check if the <code>md5</code> number of the <code>rpm</code> (installer package) is correct. It's commended to re-download the <code>rpm</code> .
NetBackup jobs are currently in progress. Stop all NetBackup jobs and then try the upgrade again.	The upgrade requires stopping all NetBackup jobs.	Please stop the NetBackup jobs, before upgrading the appliance software.
Unable to gather backup job summary information. This may indicate that some processes are not running and that you should restart your appliance.	The upgrade process checks to see if there are any active NetBackup jobs. The upgrade process only proceeds if it is determined no active jobs are detected. If the backup job summary cannot be complied it means that some of the process are not running.	Please check if the NetBackup services are running correctly.
Self-Test failed, please resolve this issue first!	The self-test has failed due to an unexpected error.	Please run the <code>Support > Test software</code> command to see the detailed error message.

[Table 17-4](#) lists error messages that are specific to the `Main_Menu > Network view` commands.

Table 17-4 Main_Menu > Network view

Error message	Explanation	Recommended action
Failed to configure DNS settings or host name Resolution entries due to some unexpected error.	This error message is displayed when there is a problem in setting the DNS information. This error may occur because the script did not return valid input or some unexpected condition occurs.	Please gather the device logs using the <code>DataCollect</code> command and Contact support.

Table 17-4 Main_Menu > Network view (*continued*)

Error message	Explanation	Recommended action
Failed to load Host Configuration settings due to some unexpected error.	This message appears when there is a problem in getting the DNS information for the appliance. This error may occur because the script did not return a valid input or some unexpected condition occurs.	Please gather the device logs using the <code>DataCollect</code> command and Contact support.
Cannot set the hostname "Name". An internal error occurred in Appliance. Check the logs to see the detailed reason.	This error can occur for the following reasons: ■ The appliance IP address is not configured when setting the host name. ■ If you try to use "nb-appliance" either as a short name or as the host name in a fully qualified domain name (FQDN). ■ Other internal errors	Try the following actions to resolve this issue: ■ Configure the appliance IP address before the host name is configured. ■ Use a host name other than the short name "nb-appliance" and the FQDNs "nb-appliance.domain.com". ■ If the above actions do not resolve the problem, collect all the <code>Vxul</code> logs by using the <code>DataCollect</code> command and contact Technical Support.

[Table 17-5](#) lists error message that are specific to the `Main_menu > Network > WANOptimization` view commands.

Table 17-5 Main_Menu > Network > WANOptimization view

Error code and error message	Explanation	Recommended action
<V-409-925-11> Invalid result returned.	Cannot get the WAN optimization status because of an unexpected error or because a service may be down.	Restart the web service by starting the NetBackup Virtual Appliance Shell Menu. Then run the following command: <pre>Support > InfraServices > Start WebServer</pre> If the issue continues, contact technical support.
<V-409-925-14> Cannot disable WAN Optimization for network port {{port}}.	The specified network interface does not exist.	Remove the name of the network port that you want to disable from the parameters that you are entering on the command line.
<V-409-925-15> Cannot enable WAN Optimization for network port {{port}}.	The specified network interface does not exist.	Remove the name of the network port that you want to enable from the parameters that you are entering on the command line.

Table 17-6 lists error messages that are specific to the `Main_menu > Settings` view commands.

Table 17-6 `Main_menu > Settings` view

Error code and error message	Explanation	Recommended action
V-409-810-0014: Failed to perform the operation because of an internal error. Contact Veritas Technical Support.	The appliance cannot perform the operation because of an internal error.	Contact Veritas Technical Support.
V-409-810-0015: Failed to enable the Deduplication service because of an internal error. Contact Veritas Technical Support.	The appliance cannot load the target port configuration because of an internal error.	Contact Veritas Technical Support.
V-409-810-0019: Failed to perform the operation because of an internal error. Contact Veritas Technical Support.	The appliance cannot perform the operation because of an internal error.	Contact Veritas Technical Support.

Table 17-7 `Main_menu > Support > FibreTransport` view

Error code and error message	Explanation	Recommended action
V-409-810-0006: Failed to configure the chunk size for optimized duplication and replication because the appliance role is not set. Before you can configure the chunk size for optimized duplication, you must first set the appliance role.	The Fibre Transport (FT) chunk size cannot be configured and used before the appliance role is set.	Set the appliance role.
V-409-810-0007: Failed to set the chunk size for optimized duplication and replication because of an internal error. Contact Veritas Technical Support.	The FT chunk size cannot be configured and used because of an internal error.	Contact Veritas Technical Support.
V-409-810-0016: Failed to perform the operation because of an internal error. Contact Veritas Technical Support.	The appliance cannot perform the operation because of an internal error.	Contact Veritas Technical Support.

Table 17-8 Main_menu > Manage > FibreChannel view

Error code and error message	Explanation	Recommended action
V-409-810-0002: Failed to restart the Deduplication service because of an internal error. Contact Technical Support.	The appliance cannot be configured as a target host for Optimized Duplication and Auto Image Replication over FC because of an internal error.	Contact Veritas Technical Support.
V-409-810-0011: Unable to configure the port <i>Slot:Port</i> as an FC Initiator port. The port is reserved for %s and cannot be changed. For more information about reserved HBA ports, refer to the NetBackup Appliance Fibre Channel Guide.	The port is reserved for use as target mode ports for SAN Client FTMS, and cannot be used as a initiator port for Optimized Duplication and Auto Image Replication over FC.	Use another port that can be used as a initiator port for Optimized Duplication and Auto Image Replication over FC. Refer to the <i>NetBackup Appliance Fibre Channel Guide</i> for the available ports.
V-409-810-0012: Cannot find the port <i>Slot:Port</i> . Invalid HBA port identifier. Check the HBA ports on the appliance and make sure to enter a valid slot number (1-6) and a valid port number (1-2).	The appliance cannot find the port specified by the user. The user must have entered an invalid slot number, port number, or both.	Refer to the <i>NetBackup Appliance Fibre Channel Guide</i> for the available ports.
V-409-810-0014: Failed to perform the operation because of an internal error. Contact Veritas Technical Support.	The appliance cannot perform the operation because of an internal error.	Contact Veritas Technical Support.
V-409-810-0020: Failed to perform the operation because of an internal error. Contact Technical Support.	The appliance cannot perform the operation because of an internal error.	Contact Veritas Technical Support.

See [“NetBackup status codes applicable for NetBackup Virtual Appliance”](#) on page 317.

See [“About troubleshooting the NetBackup Virtual Appliance”](#) on page 297.

NetBackup status codes applicable for NetBackup Virtual Appliance

This section lists the NetBackup error that can occur while, working with a NetBackup Virtual Appliance. It helps you to resolve the issues based on the corresponding error messages:

Table 17-9 NetBackup status codes

NetBackup status code	Message	Explanation
13	file read failed	A read of a file or socket failed.
48	client host name cannot be found	The system function <code>gethostbyname()</code> failed to find the client's host name.
83	media open error	The tape manager (<code>bptm</code>) or disk manager (<code>bpdm</code>) did not open the device or file that the backup or restore must use.
84	media write error	The system's device driver returned an I/O error while NetBackup wrote to removable media or a disk file.
89	problems encountered during setup of shared memory	The NetBackup processes use shared memory for some operations. This status is returned when an error is encountered in the initialization of the shared memory by the operating system's APIs.
213	no storage units available for use	The NetBackup resource broker (<code>nbrb</code>) did not find any storage units available for use. Either all storage units are unavailable or all storage units are configured for On demand only. In addition, the policy and schedule does not require a specific storage unit.
242	operation would cause an illegal duplication	If the request is processed, it causes a duplicate entry (for example, in the catalog or the configuration database). A duplicate catalog entry is usually due to a mistake in the specification of media IDs for NetBackup catalog backups.
1500	Invalid storage unit	The storage unit or storage unit group specified for one or more destinations in storage lifecycle policy is not valid.

For more information on NetBackup status codes, refer to *NetBackup™ Status Codes Reference Guide*.

See [“Error messages displayed on the NetBackup Virtual Appliance Shell Menu”](#) on page 312.

Installing an EEB

You should perform this procedure from a computer that is connected to the appliance as well as to the Internet.

To install an appliance emergency engineering binary using the NetBackup Virtual Appliance Shell Menu

- 1 Copy the EEB from your local computer to the mapped directory.
- 2 Unmap or unmount the directory after you have successfully downloaded the EEB.
- 3 From the appliance, enter the following command to close the NFS and the CIFS shares:

```
Main_Menu > Manage > Software > Share Close
```

Once the EEB is downloaded on to the share directory that you defined, it is moved to the proper location. You are not notified that this move has occurred.

If you run the `List EEBs` command before you run the `Share Close` command, the update is still moved from the share directory location to its proper location. Make sure that you have run the `Share Close` command to ensure that you close the NFS and the CIFS shares.

- 4 Enter the following command to list the EEBs that are available for downloading

```
Main_Menu > Manage > Software > List Downloaded
```

- 5 Enter the following command to install the release update.

```
Main_Menu > Manage > Software > Install patch_name
```

Where *patch_name* is the name of the EEB to install. You must make sure that the name you enter matches the EEB name that you uploaded on the appliance.

Before you proceed with the installation of the EEB, ensure that there are no jobs running on the appliance.

See [“Rolling back an EEB using the NetBackup Virtual Appliance Shell Menu”](#) on page 319.

Rolling back an EEB using the NetBackup Virtual Appliance Shell Menu

With the Rollback feature enabled, you can use the `Software > List` command with the `Software > Rollback` command to view the currently installed EEBs and roll back any of them.

If you determine that you need to roll back one or more EEBs, you must know the name of the EEB so that you can define which EEB you want to roll back. To see the list of EEBs that are currently installed, you can run the following `List` command:

```
Main_Menu > Manage > Software > List EEBs
```

The output from this command produces a list of EEB names that appear similar to the following:

```
NBAPP_EEB_3.x.x.x-0
```

To roll back the EEB file, `NBAPP_EEB_3.x.x.x-0`, run the following command:

```
Main_Menu > Manage > Software > Rollback NBAPP_EEB_3.x.x.x0
```

The process prompts you to confirm that you want to roll back that particular EEB. That is your chance to verify that the EEB name is correct. If it is, then click the **Y** key for yes. If it is not the correct EEB, click the **N** key for no and enter a new EEB name.

You cannot specify more than one EEB with this command. If you have multiple EEBs to roll back, then you have to roll back each EEB individually.

See [“Installing an EEB”](#) on page 318.

See [Manage > Software > Rollback](#) on page 354.

Appliance logging

This chapter includes the following topics:

- [About NetBackup Virtual Appliance log files](#)
- [Viewing log files using the Support command](#)
- [Where to find NetBackup Virtual Appliance log files using the Browse command](#)
- [Enabling and disabling VxMS logging](#)
- [Gathering device logs on a NetBackup virtual appliance](#)
- [About forwarding logs to an external server](#)

About NetBackup Virtual Appliance log files

Log files help you to identify and resolve any issues that you may encounter with your appliance.

NetBackup Virtual Appliance has the ability to capture software-, system-, and performance-related data. Log files capture information such as appliance operation, issues, and other details.

[Table 18-1](#) describes the methods you can use to access the appliance log files.

Table 18-1 Viewing log files

From	Access methods	Log details
NetBackup Virtual Appliance Shell Menu	You can use the <code>Main > Support > Logs > Browse</code> command to open the <code>LOGROOT/></code> prompt. You can use the <code>ls</code> and <code>cd</code> commands to traverse the appliance log directories. See “Viewing log files using the Support command” on page 323.	■ Appliance command log ■ Appliance debug log ■ NetBackup logs, Volume Manager logs, and the NetBackup logs that are contained in the <code>openv</code> directory ■ Appliance operating system (OS) installation log ■ NetBackup administrative web user interface log and the NetBackup web server log
NetBackup Virtual Appliance Shell Menu	You can use the <code>Main > Support > Logs > VxLogView Module <i>ModuleName</i></code> command to access the appliance VxUL (unified) logs. You can also use the <code>Main > Support > Share Open</code> command and use the desktop to map, share, and copy the VxUL logs. See “Viewing log files using the Support command” on page 323.	Appliance unified logs: ■ All ■ CallHome ■ Checkpoint (For upgrade issues) ■ Commands ■ Common ■ Config ■ CrossHost ■ Database ■ HWMonitor ■ Network ■ RAID ■ Seeding ■ SelfTest ■ Storage ■ SWUpdate ■ Trace ■ TaskService ■ AuthService
NetBackup Virtual Appliance Shell Menu	You can use the <code>Main > Support > DataCollect</code> command to collect the storage device logs. See “Gathering device logs on a NetBackup virtual appliance” on page 326.	Appliance storage device logs

Table 18-1 Viewing log files (*continued*)

From	Access methods	Log details
NetBackup-Java applications	If you encounter problems with the NetBackup-Java applications, you can use the scripts in this section to gather the required information for contacting support.	Logs relating to the NetBackup-Java applications

See [“Enabling and disabling VxMS logging”](#) on page 325.

See [“About troubleshooting the NetBackup Virtual Appliance”](#) on page 297.

Viewing log files using the Support command

You can use the following section to view the log file information.

To view logs using the `Support > Logs > Browse` **command:**

- 1 Enter browse mode using the `Main_Menu > Support > Logs` followed by the `Browse` command in the NetBackup Virtual Appliance Shell Menu. The `LOGROOT/>` prompt appears.
- 2 To display the available log directories on your appliance, type `ls` at `LOGROOT/>` prompt.
- 3 To see the available log files in any of the log directories, use the `cd` command to change directories to the log directory of your choice. The prompt changes to show the directory that you are in. For example, if you changed directories to the `os` directory, the prompt appears as `LOGROOT/os/>`. From that prompt you can use the `ls` command to display the available log files in the `os` log directory.
- 4 To view the files, use the `less <FILE>` or `tail <FILE>` command. Files are marked with `<FILE>` and directories with `<DIR>`.

See [“Where to find NetBackup Virtual Appliance log files using the Browse command”](#) on page 324.

To view NetBackup Virtual Appliance unified (VxUL) logs using the `Support > Logs` **command:**

- 1 You can view the NetBackup Virtual Appliance unified (VxUL) logs with the `Support > Logs > VXLogView` command. Enter the command into the shell menu and use one of the following options:
 - `Logs VXLogView JobID job_id`
Use to display debug information for a specific job ID.

Where to find NetBackup Virtual Appliance log files using the Browse command

- `Logs VXLogView Minutes minutes_ago`
Use to display debug information for a specific timeframe.
- `Logs VXLogView Module module_name`
Use to display debug information for a specific module.

- 2** If you want, you can copy the unified logs with the `Main > Support > Logs > Share Open` command. Use the desktop to map, share, and copy the logs.

Note: The NetBackup Virtual Appliance unified logs are not the same as the NetBackup unified logs, such as `nbpem` or `nbjm`. NetBackup Virtual Appliance has its own set of unified logs.

You can also use the `Main_Menu > Support > Logs` commands to do the following:

- Upload the log files to Veritas Technical Support.
- Set log levels.
- Export or remove CIFS and NFS shares.

See [Support > Logs](#) on page 540.

See [“About NetBackup Virtual Appliance log files”](#) on page 321.

Where to find NetBackup Virtual Appliance log files using the Browse command

Table 18-2 provides the location of the logs and the log directories that are accessible with the `Support > Logs > Browse` command.

Table 18-2 NetBackup Virtual Appliance log file locations

Appliance log	Log file location
Selftest report	<DIR> APPLIANCE selftest_report
Host change log	<DIR> APPLIANCE hostchange.log
NetBackup logs, Volume Manager logs, and the NetBackup logs that are contained in the <code>openv</code> directory	<DIR> NBU ■ <DIR> netbackup ■ <DIR> openv ■ <DIR> volmgr

Table 18-2 NetBackup Virtual Appliance log file locations (*continued*)

Appliance log	Log file location
Operating system (OS) installation log	<DIR> OS boot.log boot.msg boot.omsg messages
NetBackup deduplication (PDDE) configuration script log	<DIR> PD pdde-config.log
Device logs	/tmp/DataCollect.zip (software versions up to 3.1.2) /log/DataCollect.zip (software versions 3.2 and later) You can copy the DataCollect.zip to your local folders using the Main > Support > Logs > Share Open command.

See [“Viewing log files using the Support command”](#) on page 323.

See [“About NetBackup Virtual Appliance log files”](#) on page 321.

See [“About troubleshooting the NetBackup Virtual Appliance”](#) on page 297.

Enabling and disabling VxMS logging

The following procedures explain how to enable or disable VxMS logging from the NetBackup Virtual Appliance Shell Menu.

Note: Due to the size of the VxMS logs, Veritas recommends that you only enable VxMS logging when it is necessary to troubleshoot an issue. Disable VxMS logging again when the issue is resolved.

Use the `Support > Logs > GetLevel` command to check your current VxMS log setting.

To enable VxMS logging

- 1 From the `Support > Logs` view of the NetBackup Virtual Appliance Shell Menu, run the following command:

```
SetLevel VxMS 1
```

- 2 Verify that VxMS logging has been enabled with the `GetLevel` command. If the VxMS logs are enabled, the `GetLevel` command output displays the following:

```
VxMS log level is set to 1
```

To disable VxMS logging

- 1 From the `Support > Logs` view of the NetBackup Virtual Appliance Shell Menu, run the following command:

```
SetLevel VxMS 0
```

- 2 Verify that VxMS logging has been disabled with the `GetLevel` command. If the VxMS logs are disabled, the `GetLevel` command output displays the following:

```
VxMS log level is set to 0
```

See [“About NetBackup Virtual Appliance log files”](#) on page 321.

See [“About troubleshooting the NetBackup Virtual Appliance”](#) on page 297.

Gathering device logs on a NetBackup virtual appliance

You can use the `DataCollect` command from the `Main > Support` shell menu to gather device logs. You can share these device logs with the Veritas Support team to resolve device-related issues.

The `DataCollect` command collects the following logs:

- Release information
- Disk performance logs
- Command output logs
- CPU information
- Memory information
- Operating system logs

- Patch logs
- Storage logs
- File system logs
- AutoSupport logs
- Sysinfo logs

To gather device logs with the DataCollect command

- 1 Log on to the NetBackup Virtual Appliance Shell Menu.
- 2 From the `Main > Support` view, type the following command to gather device logs:

```
DataCollect
```

For appliance software versions up to 3.1.2, the appliance generates the device log in the `/tmp/DataCollect.zip` file.

For appliance software versions 3.2 and later, the appliance generates the device log in the `/log/DataCollect.zip` file.

- 3 Copy the `DataCollect.zip` to your local folders using the `Main > Support > Logs > Share Open` command.
- 4 You can send the `DataCollect.zip` file to the Veritas Support team to resolve your issues.

See [“Where to find NetBackup Virtual Appliance log files using the Browse command”](#) on page 324.

See [“About NetBackup Virtual Appliance log files”](#) on page 321.

About forwarding logs to an external server

This feature can forward NetBackup Virtual Appliance system logs (syslogs) to an external log management server.

The following two types of log servers are supported:

- Arcsight
- Splunk

NetBackup Virtual Appliance uses the Rsyslog client to forward logs. In addition to HP ArcSight and Splunk, other log management servers that support the Rsyslog client can also be used to receive syslogs from the appliance. Refer to the log management server documentation to verify Rsyslog client support.

You can view, enable, and disable log forwarding from the NetBackup Virtual Appliance Shell Menu.

See [Settings > LogForwarding](#) on page 463.

See [“Uploading certificates for TLS”](#) on page 328.

See [“Enabling log forwarding”](#) on page 329.

See [“Changing the log forwarding interval”](#) on page 330.

See [“Viewing the log forwarding configuration”](#) on page 330.

See [“Disabling log forwarding ”](#) on page 331.

For information about Log Forwarding security, refer to the following topic.

See [“Log Forwarding feature overview”](#) on page 252.

Uploading certificates for TLS

Use TLS to secure the log transmissions from the appliance to the log server. TLS is optional for log forwarding. However, Veritas recommends that you enable TLS for security purposes.

NetBackup Virtual Appliance currently only supports the following:

- TLS Anonymous Authentication for log forwarding.
- X.509 file format for certificate files.

Before you enable TLS, you must first do the following:

- Deploy the configured certificate and private key files from the Certificate Authority (CA) server onto your log server.
- Upload valid certificates to opened NFS and CIFS shares on the appliance.
For log forwarding security information, see the *NetBackup Appliance Security Guide*.

To upload the certificate

- 1 Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the `Main > Settings > LogForwarding` view.
- 2 To open NFS and CIFS shares on the appliance, enter the following command:

```
Share Open
```
- 3 On the server where the certificates reside, mount an NFS or a CIFS share to the appliance as follows:
- 4 Upload two certificates and one private key file. The certificate file names are as follows:

- `ca-server.pem`
- `nba-rsyslog.pem`
- `nba-rsyslog.key`

5 To close the shares on the appliance, enter the following command:

```
Share Close
```

See [“About forwarding logs to an external server”](#) on page 327.

See [“Enabling log forwarding”](#) on page 329.

See [“Changing the log forwarding interval”](#) on page 330.

See [“Viewing the log forwarding configuration”](#) on page 330.

See [“Disabling log forwarding ”](#) on page 331.

Enabling log forwarding

This procedure describes how to enable the log forwarding feature.

To enable log forwarding

1 Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the `Main > Settings > LogForwarding` view.

2 To enable log forwarding, enter the following command:

```
Enable
```

Specify the following:

- **Server name or IP address:** Enter the name or the IP address of the external log management server.
- **Server port:** Enter the port number of the external log management server.
- **Protocol:** Select either **UDP** or **TCP**. **TCP** is the default.
- **Interval:** Enter the forwarding interval in minutes. The options are **0**, **15**, **30**, **45**, or **60**. The default is **15**. If you set the interval to **0**, appliance continuously forwards syslogs to the target server.
- **TLS:** Select either **Yes** or **No**. **Yes** is the default.

Note: Enabling TLS requires that you upload two certificates and one private key to the appliance.

See [“Uploading certificates for TLS”](#) on page 328.

3 Verify the configuration summary, and type `yes` to complete the configuration.

See [“About forwarding logs to an external server”](#) on page 327.

See [“Uploading certificates for TLS”](#) on page 328.

See [“Changing the log forwarding interval”](#) on page 330.

See [“Viewing the log forwarding configuration”](#) on page 330.

See [“Disabling log forwarding ”](#) on page 331.

Changing the log forwarding interval

This procedure describes how to change the log forwarding interval.

To change the current log forwarding interval

1 Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the `Main > Settings > LogForwarding` view.

2 To change the log forwarding interval, enter the following command:

```
Interval
```

3 Enter the new log forwarding interval, then press **Enter**.

4 Verify the interval summary, and type `yes` to complete the change.

See [“About forwarding logs to an external server”](#) on page 327.

See [“Uploading certificates for TLS”](#) on page 328.

See [“Enabling log forwarding”](#) on page 329.

See [“Viewing the log forwarding configuration”](#) on page 330.

See [“Disabling log forwarding ”](#) on page 331.

Viewing the log forwarding configuration

This procedure describes how to view the current log forwarding configuration.

To view the current log forwarding configuration

1 Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the `Main > Settings > LogForwarding` view.

2 To view the current configuration, enter the following command:

```
Show
```

See [“About forwarding logs to an external server”](#) on page 327.

See [“Uploading certificates for TLS”](#) on page 328.

See [“Enabling log forwarding”](#) on page 329.

See [“Changing the log forwarding interval”](#) on page 330.

See [“Disabling log forwarding ”](#) on page 331.

Disabling log forwarding

This procedure describes how to disable the log forwarding feature and remove the current configuration.

To disable log forwarding

1 Log on to the NetBackup Virtual Appliance Shell Menu and navigate to the `Main > Settings > LogForwarding` view.

2 To disable log forwarding, enter the following command:

```
Disable
```

3 Enter `yes` to disable log forwarding.

See [“About forwarding logs to an external server”](#) on page 327.

See [“Uploading certificates for TLS”](#) on page 328.

See [“Enabling log forwarding”](#) on page 329.

See [“Changing the log forwarding interval”](#) on page 330.

See [“Viewing the log forwarding configuration”](#) on page 330.

Commands overview

This chapter includes the following topics:

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

About the NetBackup Virtual Appliance Shell Menu

The NetBackup Virtual 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.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

Logging in to the NetBackup Virtual Appliance Shell Menu

The following procedure explains how to log in to the NetBackup Virtual Appliance Shell Menu (shell menu).

To log in to the shell menu

- 1 Connect to the shell menu.
- 2 Enter the user name and password for the appliance.

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

Note: If you log in to the appliance shell menu using the Terminal utility application on an Apple Mac machine, some commands may not work because of a conflict with a locale setting. To avoid this issue, disable the **Set locale environment variables on startup** option in the Terminal application. In an active Terminal session, select **Terminal > Preferences > Profiles > Advanced**. The option appears in the "International" section.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

Using the NetBackup Virtual Appliance Shell Menu

This section details the use, options, and organization of the NetBackup Virtual 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 Virtual 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 brackets (`<>`) 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.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

About the NetBackup Virtual Appliance Shell Menu command views

When you enter the NetBackup Virtual 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 19-1 NetBackup Virtual Appliance commands and views from the `Main_Menu` view

Command	Explanation
<code>Appliance</code>	Enter the <code>Appliance</code> view to manage your primary and media appliances.
<code>Exit</code>	Exit the current shell and log out.
<code>Manage</code>	Enter the <code>Manage</code> view to manage your appliance.
<code>Monitor</code>	Enter the <code>Monitor</code> view to monitor appliance activities.
<code>Network</code>	Enter the <code>Network</code> view to administer your network.

Table 19-1 NetBackup Virtual Appliance commands and views from the Main_Menu view *(continued)*

Command	Explanation
Reports	Enter the Reports view to examine the running and historical state of the host.
Settings	Enter the Settings view to change the appliance settings.
Shell	This command appears on all of the other command views. Use the following commands to do the following:, command line history information, and to return to the main menu. ■ Shell Help Displays the help for using the shell menu. ■ Shell History [Limit] 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. ■ Shell Main Returns to the main menu.
Support	Enter the Support view to enable and administer support capabilities on your appliance.
Return	This command is not present on the Main_Menu view, however, it appears on all other views. Use this command to return to the previous menu.

See “About the NetBackup Virtual Appliance Shell Menu” on page 332.

See “Using the NetBackup Virtual Appliance Shell Menu” on page 333.

See “Logging in to the NetBackup Virtual Appliance Shell Menu ” on page 332.

Appliance commands

This appendix includes the following topics:

- [Appliance > Primary](#)
- [Appliance > Media](#)
- [Appliance > ShowDedupPassword](#)
- [Appliance > Status](#)
- [Appliance > Configure](#)

Appliance > Primary

Appliance > Primary – Configure the appliance as a NetBackup primary appliance

SYNOPSIS

Primary

DESCRIPTION

This command configures your appliance as a NetBackup primary server.

This command is available on the following types of appliances:

- Combined primary and media server for remote offices and branch offices (ROBO)
- Primary server

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

Primary

Configure your appliance as a NetBackup primary server.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Appliance > Media

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

SYNOPSIS

Media *PrimaryServer*

DESCRIPTION

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

This command is available on the NetBackup Virtual Appliance media server for data centers (DC).

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 *PrimaryServer*

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

PrimaryServer is the primary server host name. You can provide the following information in this field:

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

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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 Virtual Appliance Shell Menu does not display the new password. The `ShowDedupPassword` option displays the original password that was created during the installation process.

This command is available on the following types of appliances:

- Combined primary and media server for remote offices and branch offices (ROBO)
- Media server for data centers (DC)

OPTIONS

ShowDedupPassword

Display the NetBackup deduplication password of the domain.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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 the appliance role and network settings.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Appliance > Configure

`Appliance > Configure` – Perform the initial configuration for a NetBackup Virtual Appliance.

SYNOPSIS

`Configure`

DESCRIPTION

This command launches a wizard to help you perform the initial configuration for a NetBackup Virtual Appliance. The wizard contains the steps for the following:

- Network settings (IPv4 is required for AutoSupport services)
- Host name
- Storage, if applicable.
- Primary server (required for media server)

Note: This command is only available when the appliance is newly deployed or in a factory reset state. After you have completed the initial configuration, this command is no longer available until you perform a factory reset without preserving the network and storage.

Note: This command is not available on two combined primary and media server (ROBO) product files that that supports automatic initial configuration. For those ROBO product files, the initial configuration is first partially done from within the VMware vSphere (Web) Client, and then from the shell menu.

See [“NetBackup Virtual Appliance product files \(OVF templates\)”](#) on page 29.

OPTIONS

`Configure`

Use this command to perform the initial configuration for a NetBackup Virtual Appliance.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Manage commands

This appendix includes the following topics:

- [Manage > Software > Delete](#)
- [Manage > Software > Download](#)
- [Manage > Software > List](#)
- [Manage > Software > Install](#)
- [Manage > Software > Share](#)
- [Manage > Software > Readme](#)
- [Manage > Software > Rollback](#)
- [Manage > Software > Cancel](#)
- [Manage > Software > DownloadAnalyzer](#)
- [Manage > Software > DownloadProgress](#)
- [Manage > Software > UpgradeStatus](#)
- [Manage > Software > VxUpdate](#)
- [Manage > Storage > Show](#)
- [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 > OpenStorage > Install](#)
- [Manage > OpenStorage > List](#)
- [Manage > OpenStorage > Readme](#)
- [Manage > OpenStorage > Share](#)
- [Manage > OpenStorage > Uninstall](#)
- [Manage > MountPoints > List](#)
- [Manage > MountPoints > Mount](#)
- [Manage > MountPoints > Unmount](#)
- [Manage > License > Add](#)
- [Manage > License > List](#)
- [Manage > License > ListInfo](#)
- [Manage > License > Remove](#)
- [Manage > Certificates > Generate](#)
- [Manage > Certificates > Delete](#)
- [Manage > NetBackupCLI > Create](#)
- [Manage > NetBackupCLI > Delete](#)
- [Manage > NetBackupCLI > List](#)

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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 file name of the update that you want to download.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Manage > Software > List

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

SYNOPSIS

```
List AddOns  
List AvailableAnalyzer  
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 AvailableAnalyzer  
    Use this command to check the Veritas site for any Appliance Upgrade  
    Readiness Analyzers that are available.  
  
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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Manage > Software > Install

Manage > Software > Install – Use to install a software update, hotfix/patch, or firmware update.

SYNOPSIS

```
Install update_name
```

DESCRIPTION

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

OPTIONS

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

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Manage > Software > DownloadAnalyzer

Manage > Software > DownloadAnalyzer – Download the Appliance Upgrade Readiness Analyzer tool.

SYNOPSIS

```
DownloadAnalyzer file_name
```

DESCRIPTION

Use this command to download the Appliance Upgrade Readiness Analyzer tool.

OPTIONS

```
DownloadAnalyzer file_name
```

Download a specific version of the analyzer tool, where *file_name* is the file name of the tool version that you want to download.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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:

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 for the Media Server Deduplication Pool (MSDP) partition by using the **Show** command are not accurate. 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`, `NDMPLog`, `NetBackupVxupdateRepository`. 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
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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 one or multiple storage disks at a time. The disk size must be a multiple of 0.5 TB or 512 GB.

The total capacity of the disks gets added to the `Unallocated space`.

This command is available on the following types of appliances:

- Combined primary and media server for remote offices and branch offices (ROBO)
- Media server for data centers (DC)
- Primary server

OPTIONS

Add

Launch the wizard for adding one or more disks. The wizard lists all the `New Available` disks to let you choose from the list of disks to add to the appliance storage. The total capacity of the selected disks gets added to the `Unallocated space`.

Note: The appliance only lists the `New Available` disks with a size that is a multiple of 0.5 TB or 512 GB.

```
Add [DiskID]
```

Add a storage disk, where `[DiskID]` is the SCSI ID of the disk, for example, `SCSI(0:3)`. The Disk ID appears when you run the `Show Disk` command. After a disk is added, the total capacity of the disk gets added to the `Unallocated space`.

Note: The appliance can only add `New Available` disks, and the disk size must be a multiple of 0.5TB or 512 GB.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Manage > Storage > Create

Manage > Storage > Create—Use this command to create a new standard share.

SYNOPSIS

Create Share Standard

DESCRIPTION

Note: The Copilot feature is only supported on a NetBackup Virtual Appliance with the media server role.

This command exists under the `Main > Manage > Storage` view. The `Create` command lets you create a standard share.

OPTIONS

Create Share Standard

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

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Manage > Storage > Delete

Manage > Storage > Delete—Use this command to delete existing standard shares.

SYNOPSIS

```
Delete Share ShareName
```

DESCRIPTION

Note: The Copilot feature is only supported on a NetBackup Virtual Appliance with the media server role.

This command exists under the `Main > Manage > Storage` view. The `Delete` command lets you create a standard share.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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

Note: The Copilot feature is only supported on a NetBackup Virtual Appliance with the media server role.

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'.
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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)
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

Starting with release 4.0, you can move the NetBackup VxUpdate repository to any other disk volume.

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.

Note: The NetBackup Catalog partition cannot be moved on a combined primary and media server appliance.

- *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 `SCSI(0:3)`
- *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 `SCSI(0:4)`.
- *[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 MSDP SCSI(0:3) SCSI(0:4) 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.
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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`. If disks do not contain partitions, you can remove them when they are in the **In Use** status.

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.

This command is available on the following types of appliances:

- Combined primary and media server for remote offices and branch offices (ROBO)
- Media server for data centers (DC)
- Primary server

OPTIONS

`Remove`

Launch a wizard for removing disks. The wizard lists all the disks that can be removed.

`Remove [DiskID]`

Remove an existing disk and change the state to `New Available`. Retrieve the disk SCSI ID by running the `Show Disk` command. For example, a sample Disk ID is `SCSI(0:3)`.

EXAMPLES

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

```
Storage > Remove SCSI(0:6)
```

```
- [Info] Performing sanity check on disks and partitions...(5 mins approx)
```

```
- [Info] Checking the type of 'SCSI(0:6)' disk...
- [Info] Checking the state of 'SCSI(0:6)' disk...
- [Info] Removing the 'SCSI(0:6)' 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

SCSI(0:1)	System	512 GB	-	In Use
SCSI(0:2)	Base	2.01 TB	-	In Use
SCSI(0:6)	Base	2 TB	-	New Available

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

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Manage > Storage > Resize

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

SYNOPSIS

`Resize Partition Size Unit`

DESCRIPTION

Starting with release 4.0, you can resize the VxUpdate repository upward from its minimum of 10 GB. The maximum size of the partition is dependent on the amount of all unallocated storage.

This command enables you to resize 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.

This command is available on the following types of appliances:

- Combined primary and media server for remote offices and branch offices (ROBO)
- Media server for data centers (DC)
- Primary server

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.

See [“Resizing a partition”](#) on page 101.

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.
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

OPTIONS

`Scan`

Use to refresh the storage disks and devices information.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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 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/share)

For CIFS: (\\nbuappliance\general_share)

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#)
on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Manage > OpenStorage > Share

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

SYNOPSIS

Share Open

Share Close

DESCRIPTION

The `Share Open` command enables you to share a directory for uploading plugin files. 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\general_share`

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

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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)
```

SEE ALSO

See [“About mounting a remote NFS”](#) on page 203.

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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)
```

SEE ALSO

See [“Mounting a remote NFS drive”](#) on page 204.

See [“Unmounting an NFS drive”](#) on page 206.

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#)
on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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'.

SEE ALSO

See [“Mounting a remote NFS drive”](#) on page 204.

See [“Unmounting an NFS drive”](#) on page 206.

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Manage > License > Add

Manage > License > Add — Add a license key.

SYNOPSIS

Add

DESCRIPTION

You can use this command to add a license key.

See [“Managing license keys on the NetBackup Virtual Appliance”](#) on page 84.

OPTIONS

Add *LicenseFilename*

Use to add a license key.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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`

Note: This command is available only on configured appliances.

OPTIONS

Generate *hostname*

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

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Monitor commands

This appendix includes the following topics:

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

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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]
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

	total	used	free	shared	buff/cache	available
Mem:	32419964	13166556	12879844	75484	6373564	13227264
Swap:	15359996	0	15359996			
Total:	47779960	13166556	28239840			

	total	used	free	shared	buff/cache	available
Mem:	32419964	13165912	12880464	75484	6373588	13227904
Swap:	15359996	0	15359996			
Total:	47779960	13165912	28240460			

	total	used	free	shared	buff/cache	available
Mem:	32419964	13165808	12880556	75484	6373600	13228004
Swap:	15359996	0	15359996			
Total:	47779960	13165808	28240552			

	total	used	free	shared	buff/cache	available
Mem:	32419964	13165800	12880564	75484	6373600	13228012
Swap:	15359996	0	15359996			
Total:	47779960	13165800	28240560			

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Monitor > SDCS

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

SYNOPSIS

Audit

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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 Primary 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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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]
```

DESCRIPTION

Use this command to do the following:

- Display the appliance components that are monitored, including the appliance model, network information, MSDP statistics and partition information.
- View the errors that are related to the appliance components. You can use this information to notify Veritas Technical Support of the errors.
- View the performance and status of various components of the appliance.

OPTIONS

```
Hardware ShowComponents
```

Display all the components that are monitored on an appliance.

```
Hardware ShowErrors
```

Display all the errors that are related to the monitored components.

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

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

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

```
(All/Product/Network/Partition/MSDP/Memory/GeneralCPU) [all]
```

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

Hardware ShowHealth Appliance Product

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 Oct 18 2016 02:29:15 PDT

Hardware monitor information		
Name	Manufacturer	Serial
NBU VA ROBO	Veritas	VRTSV1FE80404849

SEE ALSO

- See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.
- See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.
- See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.
- See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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 > 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.

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, *GatewayIPAddress* is the default gateway IP address, and [*InterfaceNames*] is the name of the device.

This device can be an interface or a bond.

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. 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 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
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

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
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

Hostname Show

Display the host name.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

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.

EXAMPLES

Use the following example to assign an IPv6 address to a specific interface:

```
IPv6 9ffe::9 64 eth1
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.
- 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.

If the selected interfaces are configured with IP addresses, an error message is displayed to indicate that a single interface must be configured with an IP address to create the bond.

`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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

Show Status

View the following network status information:

- Device status
- Routing status

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Network > TimeZone

Network > TimeZone – Set the time zone.

SYNOPSIS

TimeZone Reset

TimeZone Set

TimeZone Show

DESCRIPTION

Use this command to set the time zone for the appliance, based on its physical location. You can also reset the time zone to America/Los Angeles or show the currently configured time zone.

OPTIONS

TimeZone Reset

Reset the time zone to America/Los Angeles.

TimeZone Set

Set the time zone.

TimeZone Show

Show the currently configured time zone.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

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

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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 if you retain your network configuration. After the factory reset completes, you can then enable WAN optimization again for the network interface bonds.

If you *do not* 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 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 `Network > LinkAggregation` from the shell menu to comprise the 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.

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

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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          nbsvcmom:      Running
postprimary:   Running       spad:          Running
spool:         Running       vmd:           Running Responding
vnetd:         Running
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Settings commands

This appendix includes the following topics:

- [Settings > Deduplication](#)
- [Settings > LifeCycle](#)
- [Settings > LogForwarding](#)
- [Settings > NetBackup](#)
- [Settings > NetBackup DNAT](#)
- [Settings > NetBackup NATServers](#)
- [Settings > Password](#)
- [Settings > SystemLocale](#)
- [Settings > Share](#)
- [Settings > Sysctl](#)
- [Settings > Notifications > LoginBanner](#)
- [Settings > Security > Authentication > AccountStatus](#)
- [Settings > Security > Authentication > LDAP](#)
- [Settings > Security > Authentication > ActiveDirectory](#)
- [Settings > Security > Authentication > Kerberos](#)
- [Settings > Security > Authentication > LocalUser](#)
- [Main > Settings > Security > Authentication > CIFSShare](#)
- [Settings > Security > Authorization](#)

- [Main > Settings > Security > Certificate](#)
- [Main > Settings > Security > STIG](#)
- [Main > Settings > Security > FIPS](#)
- [Main > Settings > Security > SecurityLevel](#)
- [Settings > Alerts > CallHome](#)
- [Settings > Alerts > SNMP](#)
- [Settings > Alerts > Email](#)
- [Settings > Alerts > Hardware](#)

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 MSDP_ENCRYPTION *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 F-1 Deduplication parameters and default values

Setting	Default	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 (disabled) or 1 (enabled)	Specify whether you want files compressed. By default, this option is enabled.

Table F-1 Deduplication parameters and default values (*continued*)

Setting	Default	Possible values	Action
DONT_SEGMENT_TYPES	N/A	Any file extension	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. Example: <pre>DONT_SEGMENT_TYPES = mp3,avi</pre> This setting prevents NetBackup from analyzing and managing segments within the file types that do not deduplicate globally.
ENCRYPTION	0	0 (disabled) or 1 (enabled)	Specify whether to encrypt data. Enable this option to encrypt data that is written directly to this media server, or from an MSDP pool which also has the <code>ENCRYPTION</code> or the <code>MSDP_ENCRYPTION</code> option enabled. By default, this option is disabled. If you enable this parameter on all hosts, the data is encrypted during transfer and in the storage.

Table F-1 Deduplication parameters and default values (*continued*)

Setting	Default	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.
MSDP_ENCRYPTION	0	0 (disabled) or 1 (enabled)	Specify whether to encrypt MSDP data. Enable this option to encrypt all data that is written to the MSDP pool, regardless of the source. When enabled, this option overrides the ENCRYPTION option. By default, this option is disabled.

Table F-1 Deduplication parameters and default values (*continued*)

Setting	Default	Possible values	Action
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.
OPTDUP_COMPRESSION	1	0 (disabled) or 1 (enabled)	Specify whether to compress optimized duplication data. By default, this option is enabled.
OPTDUP_ENCRYPTION	0	0 (disabled) or 1 (enabled)	Specify whether to encrypt optimized duplication data. By default, this option is disabled. If you enable this option on all hosts, the data is encrypted during transfer and on the storage.
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	This parameter applies to the PureDisk Deduplication Option only. It does not affect NetBackup deduplication. The <code>WSRetryCount</code> parameter lets you configure the amount of retries that are attempted in case the Web service fails or times out.

Table F-1 Deduplication parameters and default values (*continued*)

Setting	Default	Possible values	Action
WS_TIMEOUT	120	Integer	This parameter applies to the PureDisk Deduplication Option only. It does not affect NetBackup deduplication. 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.

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 *Value*

Specify whether you want files compressed. Where *Value* is `Enable` (default), or `Disable`.

When you run the `Settings > Deduplication> Show` command, the current setting appears as 0 when disabled or 1 when enabled.

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 data. Enable this option to encrypt data that is written directly to this media server, or from an MSDP pool which also has the ENCRYPTION or the MSDP ENCRYPTION option enabled. Where *Value* is Enable or Disable (default).

When you run the Settings > Deduplication> Show command, the current setting appears as 0 when disabled or 1 when enabled.

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 MSDP_ENCRYPTION Value

Specify whether you want to encrypt data. Enable this option to encrypt all data that is written to the MSDP pool, regardless of the source. When enabled, this option overrides the ENCRYPTION option. Where *Value* is Enable or Disable (default).

When you run the Settings > Deduplication> Show command, the current setting appears as 0 when disabled or 1 when enabled.

Deduplication Tune OPTDUP_BANDWIDTH Value

The maximum bandwidth that is allowed for optimized duplication. Where *Value* is the maximum bandwidth in KBs/sec.

Deduplication Tune OPTDUP_COMPRESSION *Value*

Specify whether to compress optimized duplication data. Where *Value* is *Enable* (default), or *Disable*.

When you run the `Settings > Deduplication> Show` command, the current setting appears as 0 when disabled or 1 when enabled.

Deduplication Tune OPTDUP_ENCRYPTION *Value*

Specify whether to encrypt optimized duplication data. Where *Value* is *Enable* or *Disable* (default).

When you run the `Settings > Deduplication> Show` command, the current setting appears as 0 when disabled or 1 when enabled.

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
MSDP_ENCRYPTION	: 0

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

If STIG is enabled on the appliance, you cannot manually configure the Log Forwarding interval.

LogForwarding Share Open

Open NFS and CIFS shares to `/inst/share` 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/share` on the appliance for security purposes.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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 CertificateUsage Show 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

Note: The `Tape` and `FT` options do not apply to the virtual appliance. Modifying those parameters does not affect appliance operation.

Note: You cannot add additional media servers to the NetBackup Virtual Appliance combined primary and media server.

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 primary 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 the NetBackup Virtual Appliance primary server.

`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 the NetBackup Virtual Appliance primary server.

NetBackup AdditionalServers Show

View the list of NetBackup additional servers excluding media servers.

Note: Only available on the NetBackup Virtual Appliance primary server.

NetBackup AdditionalServers ShowAll

View the list of all NetBackup additional servers. This list includes media servers.

Note: Only available on the NetBackup Virtual Appliance primary server.

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 CertificateUsage Show *Certificate*

View the Certificate Authority (CA) that is currently in use 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_PROXYDEFAULTRECVMTO *Time*

Adjust the timeout value for the DPS proxy default. The *Time* variable contains the timeout value. The default value is 800.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Settings > NetBackup DNAT

Settings > NetBackup DNAT – Enable/Disable Destination Network Address Translation (DNAT) on NetBackup Virtual Appliance primary and media servers

SYNOPSIS

Enable

Disable

DESCRIPTION

This command lets you enable or disable DNAT on NetBackup Virtual Appliance primary and media servers that communicate with (NAT)-enabled clients.

OPTIONS

NetBackup DNAT Enable

Enable DNAT on NetBackup Virtual Appliance primary or media servers that communicate with DNAT-enabled clients.

Note: Before enabling DNAT on a NetBackup Virtual Appliance primary 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 Virtual Appliance primary 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 > NetBackup NATServers

Settings > NetBackup NATServers – Add server names to NetBackup Network Address Translation (NAT) Servers list on NetBackup Virtual Appliance primary servers

SYNOPSIS

Add
Delete
Show

DESCRIPTION

This command lets you add server names to the NetBackup NAT Servers list on NetBackup Virtual Appliance primary servers.

Note: The `NetBackup NATServers` commands are available only on NetBackup Virtual Appliance primary servers and NetBackup Virtual Appliance combined primary and media servers.

OPTIONS

`NetBackup NATServers Add`
Add server names to the NetBackup NAT Servers list.

`NetBackup NATServers Delete`
Delete server names from the NetBackup NAT Servers list.

`NetBackup NATServers Show`
Show the current server names in the NetBackup NAT Servers list.

Settings > Password

`Settings > Password` – Change the local user password.

SYNOPSIS

`Password UserName`

DESCRIPTION

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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 Virtual 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!

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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 Virtual Appliance Shell Menu
- 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:

```
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
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Settings > Security > Authentication > AccountStatus

Settings > Security > Authentication > AccountStatus – manage locked accounts on the appliance.

SYNOPSIS

```
ListLockedAccounts
```

```
UnlockAccounts Users
```

DESCRIPTION

When STIG is enabled on an appliance, a user account is automatically locked after entering three consecutive incorrect passwords within 15 minutes. The user account is locked to prevent unauthorized access to the appliance. Use the `AccountStatus` command to perform the following tasks:

- View a list of accounts that are locked
- Unlock accounts and reinstate user access to the appliance

OPTIONS

The following commands and options are available under `Authentication > AccountStatus`:

```
ListLockedAccounts
```

View a list of locked user accounts. Users in the list are restricted from logging in to the appliance through SSH and the NetBackup Web UI.

```
UnlockAccounts Users
```

Unlocks accounts and reinstates user access to the appliance through SSH and NetBackup Web UI. Here, *Users* is a comma-separated list of users whose accounts have been locked.

EXAMPLE

The following shows an example of the output for the `AccountStatus > ListLockedAccounts` command.

```
nbapp2b1.AccountStatus> ListLockedAccounts
```

Account	Locked On	Locked Until
adm1	2021-03-15	2021-3-22
adm2	2020-04-15	2021-3-22

Command Successful!

nbapp2b1.AccountStatus>

SEE ALSO

- See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.
- See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.
- See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.
- See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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/share` or `\<Appliance_Hostname>\general_share` 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 (.).
 - `*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 (,).

- 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.

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/share` or `\<Appliance_Hostname>\general_share`. 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/share` or `\<Appliance_Hostname>\general_share`.

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!

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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`:

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

- *NisServer* - 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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.
- Manage the password expiry of local users and NetBackupCLI 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.

PasswordExpiry

Manage the password expiry of all local users and NetBackupCLI users.

Note: Only the system Admin user can manage the password expiry of all local users and NetBackupCLI users.

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

`PasswordExpiry Age UserName Days`

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.

Note: You cannot run this command if STIG is enabled on your appliance. STIG enforces hardening rules to increase the security of your appliance.

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

`PasswordExpiry Now UserName`

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.

- View the password expiry information.

`PasswordExpiry Show UserName`

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

- 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.

`PasswordExpiry Warn UserName Days`

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.

Note: You cannot run this command if STIG is enabled on your appliance. STIG enforces hardening rules to increase the security of your appliance.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Main > Settings > Security > Authentication > CIFSShare

Main > Settings > Security > Authentication > CIFSShare – Manage access to general CIFS shares.

SYNOPSIS

AllowAccess

RemoveAccess

ShowAccess

DESCRIPTION

The **admin** user is given access to all general CIFS shares by default. However, you must manually manage access to general CIFS shares for all other local users and Active Directory users and user groups.

You can use the `CIFSShare` command to perform the following tasks:

- Allow users or groups to access general CIFS shares.
- Restrict users or groups to access general CIFS shares.
- List allowed users and groups with access to general CIFS shares

OPTIONS

The following commands and options are available under `Authentication > CIFSShare`:

`CIFSShare AllowAccess Users <Users> <CIFSShareName>`

Allow users to access a general CIFS share. Here, `<Users>` is a comma-separated list of users and `<CIFSShareName>` is the name of the CIFS share to which you want to grant access. You can enter the users in a comma-separated list in the `<domain_name>\<user_name>` format or the `<user_name>` format.

`CIFSShare AllowAccess Groups <Groups> <CIFSShareName>`

Allow user groups to access a general CIFS share. Here, `<Groups>` is a comma-separated list of user groups and `<CIFSShareName>` is the name of the CIFS share to which you want to grant access.

```
CIFSShare RemoveAccess Users <Users> <CIFSShareName>
```

Restrict users from accessing a general CIFS share. Here, *<Users>* is a comma-separated list of users and *<CIFSShareName>* is the name of the CIFS share to which you want to remove access. You can enter the users in the comma-separated list in the *<domain_name>\<user_name>* format or the *<user_name>* format.

```
CIFSShare RemoveAccess Groups <Groups> <CIFSShareName>
```

Restricts users in user groups from accessing a general CIFS share. Here, *<Groups>* is a comma-separated list of user groups and *<CIFSShareName>* is the name of the CIFS share to which you want to remove access.

```
CIFSShare ShowAccess [<CIFSShareName>]
```

Lists all users and user groups with access general CIFS shares. If you provide the *<CIFSShareName>* option, only users and user groups with access to the particular CIFS share are displayed.

EXAMPLES

The following shows an example of the output for the `CIFSShare ShowAccess`:

```
CIFSShare> ShowAccess
```

Share Type	Share Name	Share Status	Allowed Users / Groups
CIFS	install	Closed	
CIFS	logs	Closed	admin, domain\user1, domain\user2
CIFS	incoming_patches	Closed	admin
CIFS	incoming_plugins	Closed	admin
CIFS	logforwarding	Closed	admin

Command was successful!

```
CIFSShare> ShowAccess logs
```

Share	Share	Share	Allowed Users / Groups

Type	Name	Status	
CIFS	logs	Closed	admin,domain\user1,domain\user2

Command was successful!

SEE ALSO

- See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.
- See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.
- See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.
- See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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 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 Virtual Appliance 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 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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Main > Settings > Security > Certificate

Main > Settings > Security > Certificate – Manage an external certificate on NetBackup and NetBackup Virtual Appliance.

SYNOPSIS

Import

Show

DESCRIPTION

The `Certificate` command allows you to manage an external certificate on NetBackup and NetBackup Virtual Appliance.

OPTIONS

Import

Import external certificate files to NetBackup and NetBackup Virtual Appliance. Both NetBackup and NetBackup Virtual Appliance layers use the same certificate file, trust store file, and private key file.

Note: Ensure that you upload the certificate file and trust store file in the PEM, DER, or P7B format, and the private key file in the PEM or DER format.

Show

Shows the details of the certificates used in the NetBackup and NetBackup Virtual Appliance layers.

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. See [“OS STIG hardening for NetBackup Virtual Appliance”](#) on page 245.

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.

Status

See the current status of the option.

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. See [“FIPS 140-2 conformance for NetBackup Virtual Appliance”](#) on page 246.

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 > SecurityLevel

Main > Settings > Security > SecurityLevel – Manage the security level on NetBackup Virtual Appliance.

SYNOPSIS

High

Show

DESCRIPTION

The `SecurityLevel` command lets you view and set the security level on NetBackup appliances to restrict user access to the appliance operating system (VxOS).

OPTIONS

`SecurityLevel High`

When the security level is set to `High`, the following restrictions are enforced in the appliance shell menu:

- Users cannot access the maintenance shell to troubleshoot issues or manage OS tasks (the `Support > Maintenance` menu is not available in the shell menu).
- Users cannot create and delete NetBackupCLI users (the `Manage > NetBackupCLI` menu is not available from the shell menu).
- Users cannot grant or revoke the NetBackupCLI role (the `Authorization > Grant NetBackupCLI` menu is not available from the shell menu).
- Users with the NetBackupCLI role cannot log in to the appliance.

Note: After switching to the `High` security level, you cannot revert to the default (`Optimal`) security level unless you perform a factory reset of the appliance. You also must exit the current shell session and log back in to see the changes.

`SecurityLevel Show`

Displays the current security level of the NetBackup Virtual Appliance operating system (VxOS). The VxOS can operate in either of the following security levels:

- `Optimal`: Access to VxOS is granted as per standard Veritas security policies. This is the default security configuration.
- `High`: Access to VxOS is disabled for all users.

- **Maintenance:** Access to VxOS is temporarily granted to Veritas support personnel through the maintenance shell. The security level is automatically reverted to `High` after the maintenance activity is completed.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Settings > Alerts > CallHome

Settings > Alerts > CallHome — Manage CallHome settings.

SYNOPSIS

```
CallHome Diagnose
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 Show
CallHome Test
```

DESCRIPTION

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 Diagnose

Run this command to create a diagnosis report that lists the possible causes for CallHome Test failures. The report is stored in the following location:

```
/log/autosupport/callhome/Callhome_diagnosis_<datetime>.txt
```

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. By default, the HTTP protocol is used to communicate with the proxy server.

Note: If you want to use the HTTPS protocol, ensure that you enter **https://** before the proxy server name. To ensure successful communication with the proxy server, add the latest CA certificate used by the proxy server by running the Settings > Security > Certificate > AddCACertificate command.

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 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
```

Note: `NBInventory` refers to the NetBackup Product Improvement Program

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Settings > Alerts > SNMP

Settings > Alerts > SNMP – Add SNMP information on your appliance that enables the host to send SNMP notifications for monitoring.

SYNOPSIS

```
SNMP Clear  
SNMP Disable  
SNMP Enable  
SNMP Set Server [Community] [Port]  
SNMP Show  
SNMP ShowMIB
```

DESCRIPTION

The NetBackup Virtual Appliance uses the SNMPv2-SMI or SNMPv3-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.

OPTIONS

```
SNMP Clear  
    Clears all of the previously stored SNMP settings.  
  
SNMP Disable  
    Disables the ability to send SNMP notifications (traps) for monitoring.  
  
SNMP Enable [version]  
    V2  
    Enable the ability to send SNMP version 2 notifications (traps) for monitoring.  
    V3
```

Enable the ability to send SNMP version 3 notifications (traps) for monitoring.

`SNMP Set Community Server [Port] Security`

Community

Sets the SNMP Community string. The default setting is *public*. This setting is required for SNMP V2, and is optional for SNMP V3.

Server [Port]

Sets the SNMP server name and the port assignment. The default setting is 162.

Note: NetBackup Virtual Appliance supports all of the SNMP servers in the market. However, the ManageEngine™ SNMP server and the HP OpenView SNMP server are tested and certified.

Security

Lets you configure the following security parameters when SNMP version 3 is enabled:

- `noAuthNoPriv [Username]`
Sets the security level to no authentication and no privileges for a specific SNMP user.
- `AuthNoPriv [Username] [Authentication Protocol] [Authentication Password]`
Sets the security level to authentication with no privileges for a specific SNMP user. Authentication Protocol can be set to SHA256 or SHA512. An Authentication Password is required.
- `AuthPriv [Username] [Authentication Protocol] [Encryption Policy] [Authentication Password] [Encryption Passphrase]`
Sets the security level to authentication with privileges for a specific SNMP user. Authentication Protocol can be set to SHA256 or SHA512. Encryption Policy can be set to AES128, AES192, or AES256. An Authentication Password and an Encryption Passphrase are required.

Rules for Username, Authentication Password, and Encryption Passphrase:

- Username can have 1-32 characters.
Authentication Password and Encryption Passphrase must have 8 or more characters.
- Username, passwords, and passphrases may include uppercase letters, lowercase letters, numbers, and the following punctuation marks: period, hyphen/dash, underscore.

- Spaces, commas, and special characters are not allowed.

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
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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 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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Support commands

This appendix includes the following topics:

- [Support > Checkpoint](#)
- [Support > DataCollect](#)
- [Support > Disk](#)
- [Support > Errors](#)
- [Support > FactoryReset](#)
- [Support > InfraServices](#)
- [Support > InstantAccess](#)
- [Support > iostat](#)
- [Support > LogBrowser](#)
- [Support > Logs](#)
- [Support > Maintenance](#)
- [Support > Messages](#)
- [Support > NBDNA](#)
- [Support > nbperfchk](#)
- [Support > NBSU](#)
- [Support > Processes](#)
- [Support > Reboot](#)
- [Support > Service](#)

- [Support > Shutdown](#)
- [Support > Storage Create NDMPLogPartition](#)
- [Support > Storage SanityCheck](#)
- [Support > Storage Reset](#)
- [Support > System](#)
- [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.

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 Virtual Appliance Shell Menu:

- 1 Log on to the appliance as an administrator and open the NetBackup Virtual Appliance Shell Menu.
- 2 Enter the following command to create a user-directed checkpoint:

`Main_Menu > Support > Checkpoint Create`

An interactive process begins. The NetBackup Virtual 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 checkpoint creation process.

To roll back to an existing checkpoint from the NetBackup Virtual Appliance Shell Menu

- 1 Log on to the appliance as an administrator and open the NetBackup Virtual 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 Virtual 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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

DataCollect v2

Use to gather appliance datacollect logs.

DataCollect v2 Cleanstart

Use to delete all previous appliance datacollect logs and gather a new datacollect log.

DataCollect v2 Status

Use to check the progress for any current datacollect process.

DataCollect v2 Upload

Use to upload the latest datacollect log to the Veritas server.

EXAMPLES

The following procedure is executed after you run the DataCollect command.

```
abc123.Support> DataCollect
Gathering release information
Gathering disk performance logs
Gathering command output 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
```

```
All logs have been collected in /tmp/DataCollect.zip
Log file can be collected from the appliance shared folder - \\abc123.company.com\logs\APPLIANCE
Share can be opened using Main->Support->Logs->Share Open
```

```
=====End of DataCollect=====
```

SEE ALSO

- See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.
- See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.
- See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.
- See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

Note: If you upgrade to version 4.0 from versions 3.1 through 3.3.0.1, you cannot perform a factory reset and retain the backup data. The backup data cannot be retained because the data format was updated during a previous upgrade. The new data format cannot be reverted and the older software versions cannot recognize the new data format. Therefore, the software version still reverts back to an older version, but all of the data will be removed.

See [“How to factory reset the NetBackup Virtual Appliance”](#) on page 292.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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 service.

Start Webserver

Start the web server service.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Support > InstantAccess

`Support > InstantAccess` – Use to set the operational level of Instant Access and show the status.

SYNOPSIS

`Decrease`

`Restore`

`Status`

DESCRIPTION

These commands exist under the `Main > Support > InstantAccess` view. You can use these commands to decrease or restore the operational level of Instant Access and to show its current status.

OPTIONS

`Decrease`

Lowens the operational level of Instant Access by disabling its self-test function. Use only if necessary to help reduce the amount of time to upgrade appliance software.

`Restore`

Returns Instant Access to its full operational level by enabling its self-test function.

`Status`

Shows the current operating level of the self-test function for Instant Access.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Support > LogBrowser

Support > LogBrowser – Show and control Log Transfer Console processes.

SYNOPSIS

Start time

Status

Stop

DESCRIPTION

Use this command to manage the log transfer web service, which is used by the Log Transfer Console to download the logs to your local system.

OPTIONS

Start time

Start the log transfer web service. You can set the amount of time from 1 to 720 minutes. The default time is 720. When the set time expires, the log transfer web service stops automatically.

Status

Show the current status of the log transfer web service.

Stop

Stop the log transfer web service manually.

Support > Logs

Support > Logs – Manage logging setting, view and share logs files.

SYNOPSIS

```
Browse  
Delete Date LogType  
GetLevel  
ProcessLogLevel Option Action  
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`

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/ALL

GetLevel

Use to view the current log level settings for the following:

- NetBackup Legacy
- NetBackup Unified Debug
- NetBackup Unified Diagnostic
- NetBackup VolMgr
- MSDP
- AutoSupport
- VxMS
- WebGUI

ProcessLogLevel *Option Action*

Use to set the process log level for specific NetBackup processes.

Where *Option* is *NetBackupUnified*, *NetBackupLegacy*, or *MSDP*. When you select *NetBackupUnified Set* or *NetBackupUnified SetAll*, you must also select either *Debug* or *Diagnostic*.

Where *Action* is *Restore*, *RestoreDefault*, *Save*, *Set*, *SetAll*, *Show*, or *ShowAll*.

For example, to set this option for *NetBackupUnified* and set the `nbemm` process for *Debug* at a log level of 1, you would enter the following:

```
ProcessLogLevel NetBackupUnified Set nbemm Debug 1
```

SetLevel *Option Level*

Use to set a specific log level.

Where *Option* is one of the following:

- *NetBackupLegacy*
- *NetBackupUnified*
- *NetBackup VolMgr*
- *MSDP*
- *AutoSupport*
- *VxMS*
- *WebGUI*

Where *Level* is any number from 0 (lowest logging level) to 10 (highest logging level). When you select *NetBackupUnified*, you must also select either *Debug* or *Diagnostic*.

For example, to set the level for *NetBackupUnified Diagnostic* to a log level of 2, you would enter the following:

```
SetLevel NetBackupUnified Diagnostic 2
```

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/Common/Config/Database/HWMonitor/Network/Seeding/SelfTest
/Storage/SWUpdate/Commands/CrossHost/Trace/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 ###-###-###

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

You are prompted to change the default password as part of initial configuration.

Use the following command to reset the password anytime after you have completed the initial configuration:

```
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.

Note: The maintenance shell is disabled if you configure the security level of VxOS to `High`. To troubleshoot issues and manage OS tasks, you can allow Veritas support personnel to enable and access the maintenance shell.

Use the commands in the `Main_Menu > Support > System` menu to manage support access to the maintenance shell.

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:
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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*.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Support > Service

`Support > Service` – Use this command to manage services on a host. When you use this command you must specify the name of the service.

SYNOPSIS

`Service Disable`

`Service Enable`

`Service Restart`

`Service Show`

`Service Stop`

DESCRIPTION

Use this command to manage services on a host. You must specify the name of the service.

OPTIONS

`Service Disable ServiceName`

Use this command to disable the nfs, nmb, or the smb service.

For security reasons, if you disable any of these services, they remain disabled even after the host is rebooted or upgraded.

`Service Enable ServiceName`

Use this command to enable the nfs, nmb, or the smb service.

`Service Restart ServiceName`

Use this command to restart a service on the appliance, where *ServiceName* is the name of the service that you want to restart. For example, network, nfs, nmb, or smb.

`Service Show`

Use this command to show the current status of the nfs, nmb, and smb services.

`Service Stop ServiceName`

Use this command to stop the nfs, nmb, or the smb service.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Support > Storage Create NDMPLogPartition

Support > Storage Create NDMPLogPartition – Create a partition for the NDMP logs.

SYNOPSIS

```
Storage Create NDMPLogPartition
```

DESCRIPTION

This command creates a partition for the NDMP logs. When NDMP is enabled during your backup operations, the NDMP logs are saved to the system disk by default and have limited storage space. If you need additional space, you can use this command to create the NDMP log partition and move the current NDMP log data to that partition.

Note: All NetBackup jobs must be stopped before you begin, and you must have at least 100 GB of available storage space on the appliance.

OPTIONS

```
Storage Create NDMPLogPartition
```

Use this command to create a partition for the NDMP logs and move the current NDMP log data to that partition.

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.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

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 primary 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.
```

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Support > System

`Support > System` – Used to manage the maintenance shell and authorize access to Veritas support personnel.

SYNOPSIS

`Generate-otp`

`Show-otp`

`Lock`

`Unlock`

DESCRIPTION

The `Main_Menu > Support > System` menu is enabled when the security level of an appliance is configured to `High`. Use the commands in this menu to enable or disable the maintenance shell and authorize access to Veritas support personnel.

For more information about maintenance shell, see the *NetBackup Appliance Security Guide*.

OPTIONS

`Generate-otp`

Use this command to generate a ten digit one-time password (OTP). The OTP can be shared with Veritas support personnel to allow access to the maintenance shell.

`Show-otp`

Use this command to view the currently active OTP.

`Unlock`

Veritas support personnel use this command to enable the maintenance shell.

`Lock`

Use this command to disable the maintenance shell.

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.

Support > Test

Support > Test – Test the current status of the various appliance components.

SYNOPSIS

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 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 Software]` command for a Primary appliance.

```
xyz123.Support> Test Software
```

Running Validation tests on Primary 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]

SEE ALSO

See [“About the NetBackup Virtual Appliance Shell Menu”](#) on page 332.

See [“About the NetBackup Virtual Appliance Shell Menu command views”](#) on page 334.

See [“Logging in to the NetBackup Virtual Appliance Shell Menu ”](#) on page 332.

See [“Using the NetBackup Virtual Appliance Shell Menu”](#) on page 333.