

Symantec NetBackup™ Appliance Administrator's Guide

Release 2.7.1

NetBackup 52xx and 5330



Symantec NetBackup™ Appliance Administrator's Guide

Documentation version: 2.7.1

Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

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

This Symantec product may contain third party software for which Symantec 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. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

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 Symantec Corporation 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. SYMANTEC CORPORATION 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 Symantec 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.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within the company to answer your questions in a timely fashion.

Our support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about our support offerings, you can visit our website at the following URL:

www.veritas.com/support

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.veritas.com/support

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information

- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Technical Support
 - Recent software configuration changes and network changes

Licensing and registration

If your product requires registration or a license key, access our technical support Web page at the following URL:

www.veritas.com/support

Customer service

Customer service information is available at the following URL:

www.veritas.com/support

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Advice about technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact us regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Contents

Technical Support	4
Chapter 1 Overview	12
About NetBackup appliances	12
About the Master Server role	17
About the Media Server role	17
About accessing the NetBackup Appliance Web Console	18
Web browsers supported by Appliance	18
Disabling the Untrusted Connection page in Mozilla Firefox	19
About the NetBackup Appliance Shell Menu	20
About Appliance console components	21
About using the links on the title bar	21
Accessing and using help	22
About using Web browser bookmarks	23
Avoiding CSRF (Cross Site Request Forgery)	24
About the NetBackup Appliance Web Console login page	24
NetBackup Appliance home page	29
Common tasks in Appliance	31
About the NetBackup Appliance documentation	32
Chapter 2 Monitoring the NetBackup appliance	35
About monitoring the NetBackup Appliance	35
About hardware monitoring and alerts	36
Monitor > Hardware options	36
About Email notification from a NetBackup appliance	45
About Symantec Data Center Security on the NetBackup	
appliance	46
Monitor > SDCS Events	48
Viewing SDCS audit log details	50
Filtering SDCS audit logs	52
Setting the SDCS audit log retention specification	52
About Symantec Data Center Security Downloads	54
Connecting to the SDCS server	57
Revert SDCS to unmanaged mode on a NetBackup	
appliance	57

Chapter 3

Implementing third-party SSL certificates	58
Managing a NetBackup appliance from the NetBackup Appliance Web Console	60
About the Manage views	60
About storage configuration	63
Manage > Storage	67
Checking partition details	74
Resizing a partition	76
Resize dialog	78
Troubleshooting resize-related issues	79
Moving a partition	80
Move <partition> dialog	80
Moving the MSDP partition from a base disk to an expansion disk for optimum performance	81
Scanning storage devices from the NetBackup Appliance Web Console	84
Adding the storage space from a newly available disk	85
Removing an existing storage disk	86
Monitoring the progress of storage manipulation tasks	88
Scanning storage devices using the NetBackup Appliance Shell Menu	88
About Copilot functionality and share management	91
About viewing storage space information using the <code>Show</code> command	102
About storage email alerts	114
About appliance supported tape devices	115
Adding external robots to the NetBackup appliance	115
About configuring Host parameters for your appliance	116
Manage > Host > Data Buffer options	116
Configuring data buffer parameters	118
Manage > Host > Lifecycle options	118
Configuring lifecycle parameters	122
About configuring deduplication solutions	122
About BMR integration	125
Manage > Host > IPMI options	126
Manage > Appliance Restore	127
About creating an appliance checkpoint	128
About rollback to a checkpoint	134
About NetBackup appliance factory reset	141
Manage > License	153
Managing license keys on the NetBackup appliance	154

Adding a permanent license key if an evaluation license key expires	155
About the Migration Utility	157
Selection Criteria	159
Migration Job Status	163
Policy Conversion	166
Best practices to run a migration job	169
Software release updates for NetBackup Appliances	170
Guidelines to install a software update	171
Manage > Software Updates	173
Downloading and installing NetBackup appliance software from NetBackup Appliance Web Console	175
Downloading NetBackup appliance software and client packages from the NetBackup Appliance Shell Menu	178
Installing NetBackup appliance software using the NetBackup Appliance Shell Menu	183
Appliance servers to upgrade	186
Software Updates Installation Status	187
About installing an EEB	188
About installing NetBackup Administration Console and client software	189
Manage > Additional Servers	196
Managing additional servers to the appliance	196
Manage > Certificates	197

Chapter 4

Managing NetBackup appliance using the NetBackup Appliance Shell Menu	199
Expanding the bandwidth on the NetBackup appliance	199
About configuring the maximum transmission unit size	200
About OpenStorage plugin installation	200
Installing OpenStorage plugin	202
Uninstalling OpenStorage plugin	203
About mounting a remote NFS	204
Mounting an NFS remote drive	205
Unmounting an NFS drive	207
About running NetBackup commands from the appliance	208
About NetBackup administrator capabilities	209
Creating NetBackup administrator user accounts	214
Deleting NetBackup administrator user accounts	217
Viewing NetBackup administrator user accounts	218
About Auto Image Replication between appliances	219

About Auto Image Replication between NetBackup appliances	219
About Auto Image Replication between NetBackup appliances and deduplication appliances	224

Chapter 5 Understanding the NetBackup appliance settings 225

About modifying the appliance settings	225
Settings > Notifications	227
Settings > Notifications > Alert Configuration	227
Settings > Notification > Registration	238
Settings > Network	242
VLAN configuration for NetBackup Appliances	242
Settings > Network > Network Settings	243
Settings > Network > Fibre Transport	259
Settings > Network > Host	262
About IPv4-IPv6-based network support	264
Settings > Date and Time	265
Settings > Authentication	266
About configuring user authentication	267
About authorizing NetBackup appliance users	270
Settings > Authentication	273
Settings > Authentication > LDAP	273
Settings > Authentication > Active Directory	282
Settings > Authentication > Kerberos-NIS	285
Settings > Authentication > User Management	287
Settings > Password Management	293

Chapter 6 Troubleshooting 295

Troubleshooting and tuning appliance from the Appliance Diagnostics Center	295
Viewing log files using the Support command	300
Where to find NetBackup appliance log files using the Browse command	302
About password recovery	303
About disaster recovery	303
Gathering device logs with the DataCollect command	304
Setting a NetBackup 5330 storage shelf component to the Service Allowed mode	306

Chapter 7	Deduplication pool catalog backup and recovery	311
	Deduplication pool catalog backup policy	311
	Automatic configuration of the deduplication pool catalog backup policy	312
	Manually configuring the deduplication pool catalog backup policy	315
	Manually updating the deduplication pool catalog backup policy	316
	Recovering the deduplication pool catalog	317
Index		319

Overview

This chapter includes the following topics:

- [About NetBackup appliances](#)
- [About the Master Server role](#)
- [About the Media Server role](#)
- [About accessing the NetBackup Appliance Web Console](#)
- [About the NetBackup Appliance Shell Menu](#)
- [About Appliance console components](#)
- [About the NetBackup Appliance Web Console login page](#)
- [NetBackup Appliance home page](#)
- [Common tasks in Appliance](#)
- [About the NetBackup Appliance documentation](#)

About NetBackup appliances

NetBackup appliances provide 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.

The appliances are rack-mount servers that run on the Linux operating system. NetBackup Enterprise Server software is already installed and configured to work with the operating system, the disk storage units, and the robotic tape device.

You can determine what role you want to configure the appliance to perform. You can choose to configure a 52xx appliance as follows:

- As a master server appliance
- As a media server for use with an existing master server appliance
- As a media server for use in an existing NetBackup environment

With each of these 52xx configurations, you get the added benefit of internal disk storage.

A 5330 appliance is configured as a media server by default. You can choose to configure a 5330 appliance as follows:

- As a media server for use with an existing master server appliance
- As a media server for use in an existing NetBackup environment

Note: The 5330 appliance does not have internal disk space available for backups or storage. The space available from the Primary Storage Shelf and up to two Expansion Storage Shelves can be used for backups.

This appliance version allows for easy expansion of existing NetBackup environments that have NetBackup 7.7.1 or greater installed. The appliance also includes its own browser-based interface. This interface is used for local administration of the network, internal disk storage, tape libraries and much more.

NetBackup appliances support the following features:

- Two interfaces for appliance configuration and management:
 - The NetBackup Appliance Web Console is a web-based graphical user interface. This interface is compatible with Internet Explorer versions 9.0 and later, and Mozilla Firefox versions 21.0 and later.
 - The NetBackup Appliance Shell Menu is a command line driven interface. For a complete description of all appliance commands, refer to the following document:
Symantec NetBackup Appliance Command Reference Guide
- Copilot enables Oracle database administrators to work with NetBackup appliance administrators to perform a streamlined backup and restore process of Oracle databases.
See [“About Copilot functionality and share management”](#) on page 91.
- The NetBackup 5330 Appliance now supports a second Expansion Storage Shelf. You can add a second shelf to a new or an existing system.
Refer to the *NetBackup 5330 Appliance Hardware Installation Guide* for instructions on how to install a second shelf.

- The Primary Storage Shelf and the Expansion Storage Shelf now support 6TB disks, an enhancement over the previous 3TB disks.

Note: Individual storage shelves contain either the 3TB disks or the 6TB disks, but not both.

For more information on the hardware enhancements, refer to the *NetBackup 5330 Appliance Product Description Guide*.

- Starting with NetBackup appliance version 2.7.1, you can use the fully qualified domain name (FQDN) as the appliance host name.
- Media Server Deduplication Pool (MSDP) is supported on all 52xx and 5330 appliances. MSDP offers up to the maximum available capacity on a 52xx and 5330 appliance.
- Starting with NetBackup appliance version 2.7.1, NetBackup appliances support NetBackup Cloud Storage for data backups and restores from cloud service vendors. For complete details, refer to the following document:
NetBackup Cloud Administrator's Guide
- Backup of VMware virtual machines. NetBackup appliance supports direct backup of VMware virtual machines. The appliance can back up virtual machines without a separate Windows system as backup host.
- Symantec Data Center Security (SDCS) integration. The SDCS agent is installed and configured when you initially configure your appliance. By default, SDCS operates in unmanaged mode and helps secure the appliance using host-based intrusion prevention and detection technology. In managed mode, this agent ensures that the appliance audit logs are sent to an external SDCS server to be validated and verified.
- BMR integration. When the appliance is configured as a master server, you can enable Bare Metal Restore (BMR) from the NetBackup Appliance Web Console.
- IPv4-IPv6 network support. The NetBackup appliances are supported on a dual stack IPv4-IPv6 network. The NetBackup appliance can communicate with, back up, and restore an IPv6 client. You can assign an IPv6 address to an appliance, configure DNS, and routing to include IPv6 based systems. The NetBackup Appliance Web Console can be used to enter information about both IPv4 and IPv6 addresses.
- ACSLS Support. This feature facilitates configuration of NetBackup ACS robotics on the NetBackup appliance. The appliance administrator can change the ACSLS entries in the `vm.conf` file on the local appliance.

- NetBackup SAN Client and Fibre Transport. SAN Client is a NetBackup optional feature that provides high-speed backups and restores of NetBackup clients. Fibre Transport is the name of the NetBackup high-speed data transport method that is part of the SAN Client feature. The backup and restore traffic occurs over a SAN, and NetBackup server and client administration traffic occurs over the LAN.
- NetBackup preinstalled. Simplifies the deployment and integration into an existing NetBackup environment.
- Tape out option. The appliance includes a gigabit, dual-port Fibre Channel host bus adapter (HBA).
Multiple FC ports can be used for tape out, as long as they are solely dedicated to the tape out function. For more information, refer to the *Symantec NetBackup Appliance Network Ports Reference Guide*.
- Hardware component monitoring. The appliance can monitor key hardware components such as the CPU, disks, memory, power supply modules, and fans. In addition, the appliance provides an optional Call Home feature that allows proactive monitoring and messaging of these NetBackup components.
- The NetBackup appliances support 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. And for the latest NetBackup appliance compatibility information, refer to the Hardware Compatibility List on the Symantec Support website.
www.netbackup.com/compatibility
- Flexible hardware configuration. The appliance can be ordered in a variety of configurations to provide the necessary Ethernet ports. Along with the built-in Ethernet ports on the motherboard, expansion cards can be specified to provide additional 1 GB or 10 GB Ethernet ports. Dual-port and quad-port expansion cards are supported.

For more information about hardware configuration, refer to the *Symantec NetBackup Hardware Installation Guide* and *Symantec NetBackup Appliance and Symantec Storage Shelf Product Description* for the appropriate platform.

The following describes how you can incorporate this appliance into your current NetBackup environment:

Replace unsupported media servers	Replace an existing media server that runs on a platform that is not supported in NetBackup 7.7.1.
-----------------------------------	--

- | | |
|---|--|
| Add deduplication capability | <ul style="list-style-type: none"> ■ Add the appliance to an existing NetBackup environment or replace an existing media server that does not support deduplication. ■ Configure MSDP partition on the Appliance for deduplication capability. |
| Use AdvancedDisk for non-deduplicated backups | <ul style="list-style-type: none"> ■ AdvancedDisk can provide faster restore operation but is not space-optimized like MSDP. This is a good solution for backups that include strict tape out schedules. Backups can be expired after duplication to MSDP and space on AdvancedDisk freed up for next day backups. |
| Add more storage capability | <p>Add storage capability to existing NetBackup 7.7.1 and greater environments.</p> <ul style="list-style-type: none"> ■ Built-in appliance disk storage for 52xx appliances
The internal disks can be used for additional backup storage on a 52xx appliance.

 Note: The 5330 appliance does not have internal disk space available for backups or storage. The space available from the Primary Storage Shelf and up to two Expansion Storage Shelves can be used for storage. ■ Additional external storage
The Symantec Storage Shelf is an external unit that provides additional disk storage space. You can add up to four of these units to a NetBackup 5220 or 5230 appliance.
For a NetBackup 5220 appliance, a factory matched Symantec Storage Shelf must be connected to the appliance. The NetBackup 5230 or 5330 appliances do not require a matched Symantec Storage Shelf.
When you purchase a 5220 appliance and a Symantec Storage Shelf together, the units are matched at the factory for optimum performance. For example, if you purchase a 5220 appliance with two Symantec Storage Shelf units, the factory-matched unit must be physically connected to the appliance. The second (unmatched) unit must be connected to the first unit, not to the 5220 appliance.
If you need or want to add a Symantec Storage Shelf to an existing or an operational NetBackup appliance, your appliance may first require a hardware and/or a memory upgrade. For more information, please contact your NetBackup appliance representative about your expansion needs. |

Tape backup

The appliance includes a Fibre Channel host bus adapter card for a TLD tape storage device for archive support.

About the Master Server role

A NetBackup 52xx series appliance can be configured as a master server with its own internal disk storage. You configure and use this appliance much like you would use a regular NetBackup master server. You can schedule backups or start a backup manually. Users with the appropriate privileges can perform restores.

Note: The NetBackup 5330 appliance is a media server by default and is not supported for the master server role configuration.

This appliance role provides a simplified administrative interface for the local network, disk, and storage unit 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*.

About the Media Server role

In this role, a NetBackup 52xx series appliance operates as a media server with its own internal disk storage.

A NetBackup 5330 appliance is a media server by default. The internal storage in a 5330 appliance cannot be used for storing any data or taking any backups. The internal storage is used for storing the operating system, checkpoints, and logs.

Media server appliances use 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 master server.

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

- **For use with a traditional NetBackup master server**
- **Specify master server**

About accessing the NetBackup Appliance Web Console

On a system that has a network connection to the Appliance, start a Web browser.

In the Web browser address bar, enter the following: **https://host.domain**

`host.domain` is the fully qualified domain name (FQDN) of the Appliance and can also be an IP address.

Note: The NetBackup Appliance Web Console is available only over HTTPS on the default port 443; port 80 over HTTP has been disabled.

You must supply login credentials on the Appliance login page. For an administrator initial login, the user name is `admin` and the password is `P@ssw0rd` or any custom password that you chose during the initial configuration.

Web browsers supported by Appliance

You can use a Web browser to access the NetBackup Appliance Web Console or the IPMI console. The following requirements and recommendations should be considered for the Web browser:

- The NetBackup Appliance Web Console and the IPMI console use pop-up menus. If you use pop-up blockers with your Web browser, some of these menus may not display properly. You must disable pop-up blocking or add the Appliance Web address to the list of acceptable sites in your browser.
- The Web browser should have active scripting (ActiveX and JavaScript) enabled.
- On some server-class systems, an enhanced security configuration can cause some pages to not display properly in Internet Explorer. If you encounter this issue, add the Appliance Web Console to the Trusted-sites list and lower the security setting. To resolve this issue, open Internet Explorer and select **Tools > Internet Options > Security** to configure the Trusted-sites list and lower the security level.
- If you use Internet Explorer 10.0 or above to access the Appliance Web console, security certificate warnings appear when you access a pop-up menu. Select **Continue to this web site (not recommended)** to log on to the appliance. Once you select this option, the security certificate warnings do not appear on the pop-up menus.
- The NetBackup Appliance Web Console is best viewed with 1280 * 1024 or a higher screen resolution.

Table 1-1 lists the Web browsers that Appliance supports.

Table 1-1 Web browsers supported by Appliance

Web browser	Supported Versions	Notes
Microsoft Internet Explorer	10.0 and higher Note: IE 8.x and 9.x are not supported. If you are using IE 8.x or 9.x to access NetBackup, you must upgrade to IE 10.0 or higher.	IE 10.0 and later versions may display a security certificate warning page when you access the NetBackup Appliance Web Console. Select Continue to this website (not recommended) to access the console. The Appliance Web Console cannot be viewed on Internet Explorer 10 or later in a compatible mode. From your browser, use the Tools > Compatibility View Settings menu and uncheck Display all websites in Compatibility view to see the Appliance Web Console.
Mozilla Firefox	21.0 and higher Note: If you try to access the NetBackup Appliance using earlier versions of Firefox and reset the password using Settings > Password, the page may hang.	Mozilla Firefox may display an Untrusted Connection page when you access the NetBackup Appliance Web Console. See “Disabling the Untrusted Connection page in Mozilla Firefox” on page 19.

Disabling the Untrusted Connection page in Mozilla Firefox

When you access the NetBackup Appliance Web Console in Mozilla Firefox, you may see the following Untrusted Connection page.



This Connection is Untrusted

You have asked Firefox to connect securely to **nbapptitan1a.engba.symantec.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

- **Technical Details**
- **I Understand the Risks**

Your choice is either to click **Get me out of here**, which takes you to the Mozilla Firefox start page, or click **Add Exception** (when you expand the **I Understand the Risks** section) and permanently disable the page.

Note: If these options do not appear, consult the browser help on how to view secure websites.

To disable the Untrusted Connection page in Mozilla Firefox

- 1 On the Untrusted Connection page, expand **I Understand the Risks** section and click **Add Exception**.
- 2 In the **Add Security Exception** dialog box, click **Get Certificate**.
- 3 To make this exception permanent, make sure that the **Permanently store this exception** option is checked. This option is checked by default.
- 4 Click **Confirm Security Exception**.
- 5 Restart your browser for the changes to take effect.

About the NetBackup Appliance Shell Menu

Note the following about the NetBackup Appliance Shell Menu interface:

- The NetBackup Appliance Shell Menu user interface cannot input or modify multi-byte characters, and they are not localized to any language for this release.
- Non-English characters are not shown on the NetBackup Appliance Shell Menu user interface after you finish appliance configuration. This issue occurs when you use the NetBackup Appliance Web Console during the initial configuration

of a NetBackup appliance. When you input non-English characters to register your appliance on the Registration page, the non-English characters cannot be shown on the shell menu interface.

About Appliance console components

This section provides information on the panes and navigation features available in the Appliance console. You can view the console by using a Web browser.

About using the links on the title bar

On the title bar of the NetBackup Appliance Web Console, the **Connected To** value shows the name of the appliance, the platform like 5200, 5220, or 5230 and the role in which it has been configured. In case the appliance is configured as a media server, the master server that it is connected to is also displayed.

Example: Connected To: Master 5220: nb-appliance

Here the hostname of the appliance is nb-appliance and it is a 5220 appliance that has been configured as a master server.

Example: Connected To: Media 5230: nb-appliance | Master: app-master

Here the hostname of the appliance is nb-appliance and it is a 5230 appliance that has been configured as a media server. It is connected to a master server named app-master.

On the right-side of the title bar, you may see text like Welcome [admin]. Here **admin** is the user name that is logged on to the NetBackup Appliance Web Console.

Use the links available in the title bar at the top of the console for the following tasks:

- To access online help, click **?**. An enhanced context-sensitive help system named Symantec Help Center is available with the Appliance. Symantec Help Center is a browser-based Help delivery system with advanced search, autosuggest, and filtering capabilities. Symantec Help Center lets you search from a much larger Appliance content set. Additionally you can search from the NetBackup documentation from the same Help window.
More information about online Help is available.
See [“Accessing and using help”](#) on page 22.
- To disconnect from the NetBackup Appliance Web Console and to end your session, click **Logout**.
- To see Appliance product version and copyright information, click **About**.

Accessing and using help

An enhanced context-sensitive help system named Symantec Help Center is shipped with the NetBackup Appliance. Symantec Help Center is a browser-based Help delivery system with advanced search, autosuggest, and filtering capabilities.

Symantec Help Center offers the following advantages over traditional Help systems:

- Symantec Help Center lets you search from a much larger Appliance content set. Symantec Help Center includes content from the *NetBackup Appliance Administrator's Guide*, the *Troubleshooting Guide*, and the *Commands Guide*. This means that you can search content from the *NetBackup Appliance Administrator's Guide*, the *Troubleshooting Guide*, and the *Commands Guide* content from one SymHelp Search window.
- In addition to the Appliance content, Symantec Help Center lets you search content from the *NetBackup Administration Console Help*. By default, you can view and search the Appliance content.

Figure 1-1 shows a sample view of Symantec Help Center and how you can search Appliance and NetBackup content from Symantec Help Center.

Figure 1-1 Sample view of Symantec Help Center

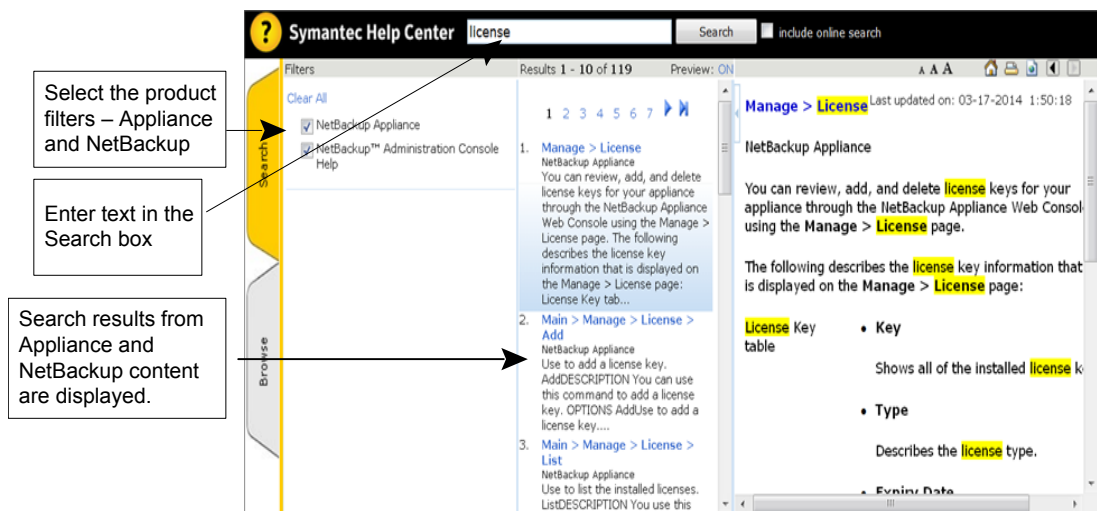
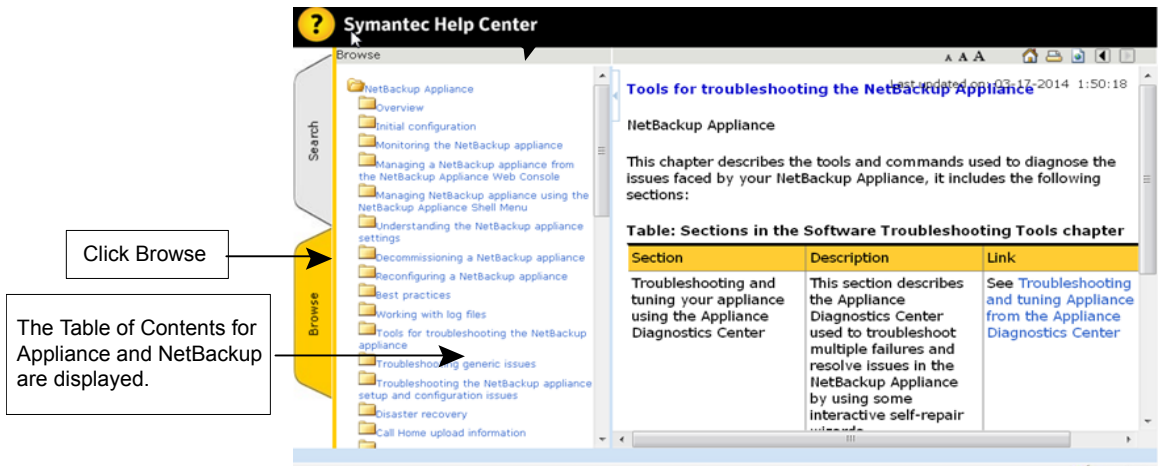


Figure 1-2 Browse functionality in Symantec Help Center



To access and use Symantec Help Center

- 1 Click ? on the upper-right corner of the NetBackup Appliance Web Console. This opens a new browser window that displays context-sensitive help for the specific page.
- 2 You can type the text or phrase that you want to search for, in the text box. You can also type in a query like 'About Appliance', 'configuring NetBackup Appliance' etc.
- 3 To view the updated documentation content that is posted online, you must be connected to the Internet and check **Include online search**.
- 4 You can view and search the Appliance content by default. To be able to search NetBackup content, select *NetBackup Administration Console Help* from the **Product Filters** section. You can then type in your NetBackup related search query in the search toolbar.

You can also click **Browse** on the left-hand side to see the table of contents for Appliance and NetBackup.

About using Web browser bookmarks

Use your Web browser to add a bookmark for any view in the Appliance console and return to it as needed.

You can use the bookmark to return to the same view when you log onto the console again.

Avoiding CSRF (Cross Site Request Forgery)

Symantec NetBackup Appliance is introducing various features to improve the security of your appliance. One such feature implemented from version 2.6.0.2 is to prevent CSRF (Cross Site Request Forgery) in NetBackup Appliance Web Console by using Synchronizer Token Patterns. Each request made to display a webpage in the NetBackup Appliance Web Console is protected by a unique CSRF Security token.

Which means that each time you logon to the NetBackup Appliance Web Console, a new session is created and correspondingly a new security token gets associated with that session. If there is any discrepancy with the security token, the following CSRF error page is displayed:

```
For security reasons, access to the appliance page destination
is denied.
Access is not allowed from an external link or from a bookmarked URL.
To access the appliance page, you must first log out of the appliance and
then log in again.
Click ? for more information.
```

- If you are currently logged on to the NetBackup Appliance Web Console and try to start a new session from a new tab, only the new session is considered as current and active. Any task you perform in the older session may display the CSRF error page.
- If you try to access any page with an incorrect security token, a bookmarked old token, or a modified token that does not match the server-side token for the same session, the CSRF error page is displayed.

See [“About the NetBackup Appliance Web Console login page”](#) on page 24.

About the NetBackup Appliance Web Console login page

The login page provides the fields to enter your login credentials and also includes the following links and information:

Section	Description
Product Information	<p>This section provides the following links where you can access NetBackup appliance information and documentation:</p> <ul style="list-style-type: none"> ■ What is new in Version 2.7.1? ■ Release Notes ■ Administrator's Guide ■ Hardware Installation and Initial Configuration Guide ■ View Compatibility Lists ■ View Symantec Operational Readiness Tools (SORT)
Download Packages	<p>This section indicates whether there are NetBackup client packages stored on the appliance that can be installed on clients. Client packages also include the NetBackup Administration Console. You can select to install all listed client packages or select a specific package to install.</p> <p>Note the following important points about downloading client packages:</p> <ul style="list-style-type: none"> ■ Starting with appliance version 2.6.0.2, NetBackup clients are no longer included with NetBackup appliance release updates. If you want to store clients on the appliance, a separate client package is available to download. The client packages are posted on the same Symantec Support site where the appliance update releases are also posted. Client versions that are stored on the appliance do not have to match the NetBackup version that is currently installed on the appliance. <p>If a client package does not exist on the appliance, the following message appears when you select to download it:</p> <p><code>No packages found.</code></p> <p>To download the client packages and store them on the appliance, see the <i>Symantec NetBackup Appliance Administrator's Guide</i>. Refer to the topic "Downloading client packages to a NetBackup appliance:</p> <ul style="list-style-type: none"> ■ To install the NetBackup Administration Console client, you must first download the Windows client package. This client is required to access the NetBackup Administration Console. ■ You can install the vCentre Plug-in to use vSphere Client to monitor virtual machine backups and recover a virtual machine from a backup.

Section	Description
Browser Recommendation	<p>This section verifies and displays a confirmation if the Symantec NetBackup Appliance Web Console supports your browser.</p> <p>The NetBackup Appliance Web Console supports Internet Explorer versions 10.0 and later, and Mozilla Firefox versions 21.0 and later.</p> <p>Note: Even though IE 9.x is not a supported browser, the NetBackup Appliance Web Console may flag IE 9.x as a supported browser. If you are using IE 8.x or 9.x to access the NetBackup Appliance Web Console, you must upgrade to IE 10.0 or higher.</p> <p>Note: The Symantec NetBackup Appliance Web Console cannot be viewed on Microsoft Internet Explorer 10 or later in a compatible mode. From your browser, use the Tools > Compatibility View Settings menu to clear Display all websites in Compatibility view selection and view the NetBackup Appliance Web Console.</p>

To log on to the Symantec NetBackup Appliance Web Console

- 1 Enter the following URL in the web browser:

`https://ip|hostname/appliance`

In the URL use the *IP* or *hostname* of your appliance. The *hostname* is the label that is assigned to your appliance to identify the device in your network.

Note: If you use Internet Explorer 10.0 or higher to access the NetBackup Appliance Web Console, security certificate warnings appear when you access a pop-up menu. Select **Continue to this website (not recommended)** to log into the appliance. Once you select this option, the security certificate warnings do not appear on the pop-up menus.

The browser displays the Symantec NetBackup Appliance Web Console login page.

Note: If the initial configuration for an appliance is in progress, do not try to run a new instance of the NetBackup Appliance Web Console. You cannot log on to the appliance thus causing an unsuccessful login.

- 2 Enter your user name in the **Username** field. The default user name is **admin**.

- Enter your password in the **Password** field. The default user password is **P@ssw0rd**, where 0 is the number zero.

Note: After the new appliance is configured and you have been registered as a user, the user name and password are sent to your registered email ID.

- Select your preferred language from the **Language** drop-down list. Based on the language you select, the labels on the NetBackup Appliance Web Console are displayed in that language.

English, Japanese, and Simplified Chinese web user interfaces are available for this release. Symantec recommends that the language that you select in the NetBackup Appliance Web Console is the same as your system locale. If the language that you want to select in the NetBackup Appliance Web Console is not the same as your system locale, you should first change the locale in the following manner:

To change the system locale	Details
1. Browse the locales on your system	<p>Log on to the shell menu and run <code>Settings> SystemLocale List language_code</code>.</p> <p>Example: Run <code>Settings> SystemLocale List ja</code> to browse the available locales in Japanese language.</p> <p>The following locales can be displayed:</p> <ul style="list-style-type: none"> ■ <code>ja_JP.UTF-8</code> ■ <code>ja_JP.eucJP</code> ■ <code>ja_JP.eucjp</code> ■ <code>ja_JP.shiftjisx0213</code> ■ <code>ja_JP.sjis</code> ■ <code>ja_JP.utf8</code>
2. Set the preferred locale along with its format	<p>Run <code>Settings > SystemLocale Set language_code</code> command.</p> <p>Example: Run <code>Settings> SystemLocale Set ja_JP.UTF-8</code> to set the <code>ja_JP.UTF-8</code> locale to the Appliance.</p>

Note: Selecting a language in the NetBackup Appliance Web Console that is different from the language of system locale may result in a mixing up of the two languages in the NetBackup Appliance Web Console.

5 Click **Login**.

The appliance displays either of the following:

- Initial Configuration Setup - When you log into the appliance for the first time you are asked to perform the initial configuration and set up your appliance. For more information, refer to the *Symantec NetBackup Initial Configuration Guide*.

Note: If the NetBackup license key on the appliance has expired after an ISO install, continue with the initial configuration. A temporary license key is generated which is valid for 30 days. Symantec recommends that you add a permanent license key before the temporary license key has expired.

- NetBackup Appliance home page - After you have successfully configured your appliance, the **Home** page is displayed. More information about the **Home** page is available.
See “[NetBackup Appliance home page](#)” on page 29.

Note: On some server-class systems, an enhanced security configuration can cause some pages to not display properly in Internet Explorer. If you encounter this issue, add to the NetBackup Appliance Web Console Trusted-sites list and lower the security setting. To resolve this issue, open Internet Explorer and select **Tools > Internet Options > Security** to configure the Trusted-sites list and lower the security level.

[Table 1-2](#) lists the reasons due to which login failure can occur.

Table 1-2 Troubleshooting login failures

Error message	Reasons	Troubleshooting
User authentication failed. Please enter valid user name and password. If problem persists contact your System Administrator.	<ul style="list-style-type: none"> ■ If the provided user name and password are incorrect. ■ If the authentication server is not responsive. 	<ul style="list-style-type: none"> ■ Verify that you have entered the correct user name and password. ■ Contact your System Administrator in case the error appears again.

Table 1-2 Troubleshooting login failures (*continued*)

Error message	Reasons	Troubleshooting
Login was unsuccessful, click ? for details.	<ul style="list-style-type: none"> ■ If you try to log onto a new instance of the NetBackup Appliance Web Console, while the initial configuration is in progress on that appliance. ■ If an unexpected error has occurred. 	<ul style="list-style-type: none"> ■ Ensure that you do not log onto a single appliance using multiple instances of the NetBackup Appliance Web Console. ■ View the UI logs to view the exceptions stack and trace all programmatic statements. You can find the UI logs at the following location: <code>/opt/SYMCnbappws/webserver/logs</code>
The connection has timed out	If the web server is not responsive the login page is not displayed.	Contact your system administrator for more assistance.
Unable to connect	If the web server has been shut down.	Contact your system administrator for more assistance.

NetBackup Appliance home page

When you log into the appliance it displays the **Welcome to Symantec NetBackup Appliance Web Console** home page. This page is displayed after you have configured the appliance role as a media server or a master server. It displays the status of all the vital components that determine the successful functioning of your appliance, using a pictorial representation.

You can click on the elements to view additional information and monitor the status further. The following table elaborates the elements on the home page:

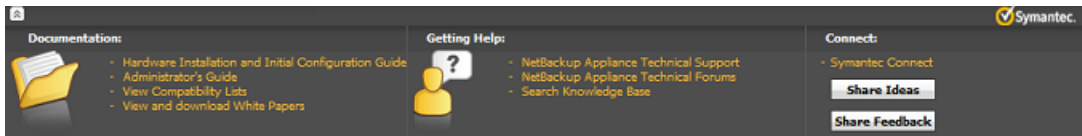
Table 1-3 Home page description

Element	Displays	Helps to	Links to the page
Storage	<p>Displays the used storage space across the appliance. The information is dynamically updated to display the current storage utilization.</p> <p>It displays the Used and Available space within your storage system and is calculated as follows:</p> <ul style="list-style-type: none"> ■ Available = Sum of available space on all configured partitions. ■ Used = Sum of used space on all configured partitions. <p>When you log into the appliance the home page displays the status of the Used and Available storage space.</p>	<p>Determine the available storage space. It enables you to take the required steps if the storage space has been used to the maximum.</p>	<p>Manage > Storage</p> <p>For more information See “Manage > Storage” on page 67.</p>
Deduplication Summary	<p>Displays the current deduplication ratio pertaining to all the backups taken so far across all the media servers.</p>	<p>Determine the quality of the data backed-up using deduplication. Lower the ratio, lower is the amount of data being stored using Deduplication.</p> <p>Deduplication ratio = total number of bytes backed up (without Deduplication) / number of bytes changed and backed up (with Deduplication)</p>	<p>This element is not linked to any specific page. For information on how to set the deduplication parameters See “About configuring deduplication solutions” on page 122.</p>
Hardware	<p>Displays the performance of all the monitored hardware devices.</p>	<p>Determine if the hardware is running and a failure has been detected.</p> <p>An error message is displayed, in case a hardware component malfunctions.</p>	<p>Monitor > Hardware</p> <p>For more information See “Monitor > Hardware options” on page 36.</p>

Table 1-3 Home page description (*continued*)

Element	Displays	Helps to	Links to the page
Notifications	<p>Displays the latest notifications for your appliance. These notifications include:</p> <ul style="list-style-type: none"> ■ Latest software updates available for your appliance. It displays the new software updates available on the support site. ■ Connectivity status for the Call Home server 	<p>Identify the following:</p> <ul style="list-style-type: none"> ■ Latest software upgrades available from the Symantec Support site. ■ Whether Call Home is functional. 	<p>Manage > Software Updates</p> <p>For more information See “Software release updates for NetBackup Appliances” on page 170.</p>

The Symantec NetBackup Appliance Web Console home page displays an expandable footer with links to documentation set, Technical Support, and Symantec Connect. This footer is displayed for all the pages on the NetBackup Appliance Web Console. To view the contents of the footer all you need to do click on the downward arrows displayed on the footer.



Common tasks in Appliance

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

Table 1-4 Quick links for common Appliance tasks

Appliance functions	Tasks	Go to this topic
Monitoring	Monitor hardware, services, and Symantec Data Center Security (SDCS)	<p>See “Monitor > Hardware options” on page 36.</p> <p>See “About hardware monitoring and alerts” on page 36.</p>

Table 1-4 Quick links for common Appliance tasks (*continued*)

Appliance functions	Tasks	Go to this topic
Managing the Appliance	Configure data buffer and deduplication settings of the Appliance Add or remove license keys Run migration utility Manage software updates	See “About configuring deduplication solutions” on page 122. See “Configuring data buffer parameters” on page 118. See “About the Migration Utility” on page 157. See “Manage > Software Updates” on page 173.
Storage management	Resize or move partitions View disk status and add or remove disks View the partition distribution on a disk	See “About storage configuration” on page 63. See “Manage > Storage” on page 67.
Restoring an Appliance	Create a checkpoint Rollback to a checkpoint Perform Factory Reset	See “Manage > Appliance Restore” on page 127.
Configuring Appliance settings	Alert and Call Home Network Date and Time User authentication and management User management Password management	See “About modifying the appliance settings” on page 225.
Troubleshooting	Troubleshoot Appliance issues	See “Troubleshooting and tuning appliance from the Appliance Diagnostics Center” on page 295.

About the NetBackup Appliance documentation

The following documents help to ensure that you can successfully install, configure, and use your appliance. All these documents are posted on the Support website at the following URL:

<http://www.symantec.com/docs/DOC2792>

Table 1-5 NetBackup Appliance documentation

Guide	Description
<i>Symantec NetBackup™ Appliance Hardware Installation Guide</i>	<p>This guide provides the following information:</p> <ul style="list-style-type: none"> ■ An introduction to the physical layout of the appliance hardware. ■ Install preparation steps, such as unpacking procedures, environmental conditions, and safety precautions. ■ Hardware configuration steps <p>This section guides you through the required steps to install your appliance in a rack and connect your appliance cables.</p>
<i>Symantec NetBackup™ Appliance Initial Configuration Guide</i>	<p>This document guides you through the configuration process from the NetBackup Appliance Web Console or from the NetBackup Appliance Shell Menu.</p>
<i>Symantec NetBackup Appliance Upgrade Guide</i>	<p>This document guides you through the required steps to upgrade a NetBackup appliance.</p>
<i>Symantec NetBackup™ Appliance Administrator's Guide</i>	<p>The <i>Symantec NetBackup™ Appliance Administrator's Guide</i> contains the following types of information:</p> <ul style="list-style-type: none"> ■ Deployment information ■ Administering your appliance ■ Monitoring information
<i>Symantec NetBackup™ Appliance Command Reference Guide</i>	<p>The <i>Symantec NetBackup™ Appliance Command Reference Guide</i> provides a complete list of the commands that are available for you to use through the NetBackup Appliance Shell Menu.</p>
<i>Symantec NetBackup Appliance Release Notes</i>	<p>This document contains information about this version of NetBackup Appliance. It contains brief descriptions of new features within the release, operational notes that apply to the release update, and any known issues.</p>
<i>Symantec NetBackup Appliance Troubleshooting Guide</i>	<p>This document contains the latest troubleshooting information for the NetBackup appliances.</p>
<i>Symantec NetBackup Appliance Capacity Planning and Performance Tuning Guide</i>	<p>This document contains information on how to optimize your backup environment and your NetBackup appliance. It helps you to analyze your backup requirements and design a system that best fits your needs.</p>

Table 1-5 NetBackup Appliance documentation (*continued*)

Guide	Description
<i>Symantec NetBackup Appliance Security Guide</i>	This document describes the security features in NetBackup Appliance and how to use those features to ensure that your appliance environment is secure.
<i>Symantec NetBackup Appliance Fibre Channel Guide</i>	This document describes the supported Fibre Channel (FC) capabilities and configurations for NetBackup appliances.
<i>Symantec NetBackup Appliance Decommissioning and Reconfiguration Guide</i>	This document describes how to decommission and reconfigure a NetBackup appliance.
<i>Symantec NetBackup Appliance SNMP Trap Reference Guide</i>	This document provides a complete list of the NetBackup Appliance SNMP traps. It describes what each trap means and the recommended actions for when an error occurs.
<i>NetBackup Copilot for Oracle Configuration Guide</i>	This document outlines how to configure Copilot using NetBackup and the NetBackup Appliance.
<i>Symantec NetBackup Appliance Third-party Legal Notices</i>	<p>The <i>Symantec NetBackup Appliance Third-party Legal Notices</i> document lists the third-party software that is included in this product, and it contains attributions for the third-party software.</p> <p>This document is available from the following website: http://www.symantec.com/about/profile/policies/eulas/</p>

For additional information about the appliance hardware, refer to the following documents:

- *Symantec NetBackup 5220 Appliance and Symantec Storage Shelf Product Description*
- *Symantec NetBackup 5230 Appliance and Symantec Storage Shelf Product Description*
- *Symantec NetBackup 5330 Appliance and Symantec Storage Shelf Product Description*
- *Symantec NetBackup 52xx and 5330 Appliance and Symantec Storage Shelf Safety and Maintenance Guide*

Monitoring the NetBackup appliance

This chapter includes the following topics:

- [About monitoring the NetBackup Appliance](#)
- [About hardware monitoring and alerts](#)
- [About Symantec Data Center Security on the NetBackup appliance](#)

About monitoring the NetBackup Appliance

After you have successfully configured your appliance, you can use any of the two user interfaces – Symantec NetBackup Appliance Web Console or the appliance shell menu to monitor the NetBackup Appliance. You can use the **Monitor** menu in the NetBackup Appliance Web Console to view and monitor the following components of your appliance.

[Table 2-1](#) describes the components that you can monitor using the **Monitor** menu:

Table 2-1 Monitor tab

Monitor	Lets you...	Topic
Hardware	Monitor the hardware, the storage devices, and all the components that are associated with them.	See “About hardware monitoring and alerts” on page 36.

Table 2-1 Monitor tab (*continued*)

Monitor	Lets you...	Topic
SDCS Events	Monitor the Symantec Data Center Security (SDCS) events that occur on the appliance. The SDCS agent is installed and configured when you initially configure your appliance. This agent operates in unmanaged mode by default, but can be connected to an external SDCS server to validate and verify your appliance's audit logs.	See “About Symantec Data Center Security on the NetBackup appliance” on page 46.

About hardware monitoring and alerts

The appliance has the ability to monitor itself for hardware problems. If it detects a problem that needs attention, it uses the following notification mechanisms:

- Hardware monitoring and alerting from the NetBackup Appliance Web Console. See [“Monitor > Hardware options”](#) on page 36.
- Sending an email to the local administrator. See [“About Email notification from a NetBackup appliance”](#) on page 45.
- Sending an alert to the SNMP manager. See [“About SNMP”](#) on page 232.
- Sending a notification to Symantec using Call Home. See [“About Call Home”](#) on page 233.

Symantec recommends that you enable Call Home so that when a problem occurs, a support case is automatically generated, and the hardware diagnostic data is sent. These actions enable faster problem resolution.

You can also check the hardware health details of the appliance by running the `Monitor > Hardware ShowHealth` command using the NetBackup Appliance Shell Menu.

Monitor > Hardware options

Monitoring the hardware components of your appliance is important for correct functioning of the appliance.

The **Monitor > Hardware** page on the NetBackup Appliance Web Console lets you monitor the hardware, the storage devices, and all of the components that are associated with them. If Call Home is enabled, this information is also automatically sent to Symantec Support in the case of a serviceable event. The hardware

monitoring information allows Symantec to provide proactive service and helps lead to a faster resolution of any hardware issues.

Using hardware monitoring, you can monitor the appliance hardware and storage components that are listed in the following tables:

Table 2-2	Hardware components monitored in 52xx appliances
Appliance	Disk, RAID, Fan, Power Supply, CPU, Temperature, Fibre Channel HBA, PCI, Network Card, Adapter
Storage shelf	Disk, Fan, Power Supply, Temperature

Figure 2-1 Hardware components monitored in 52xx series appliances

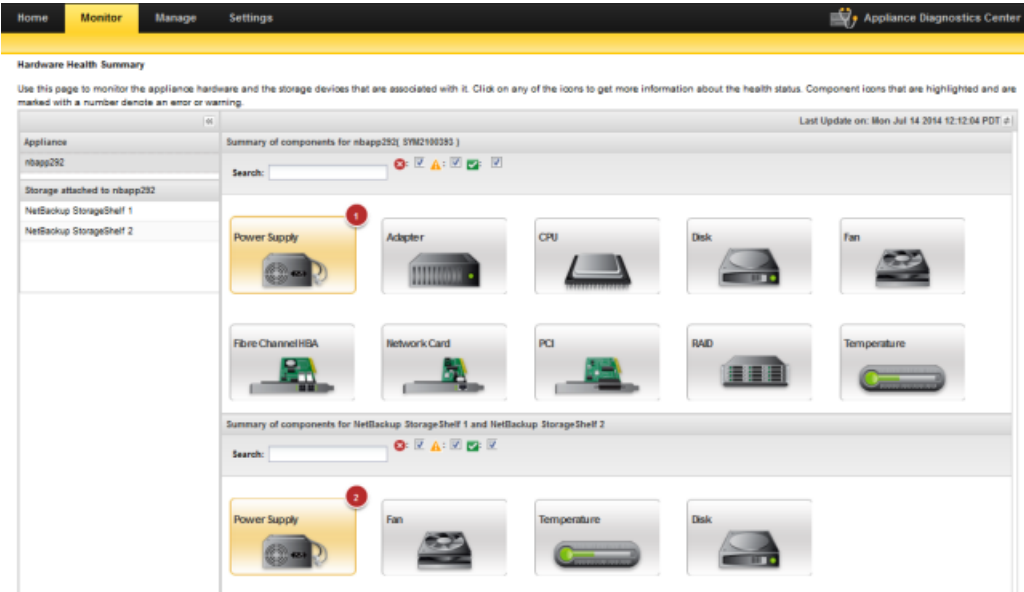
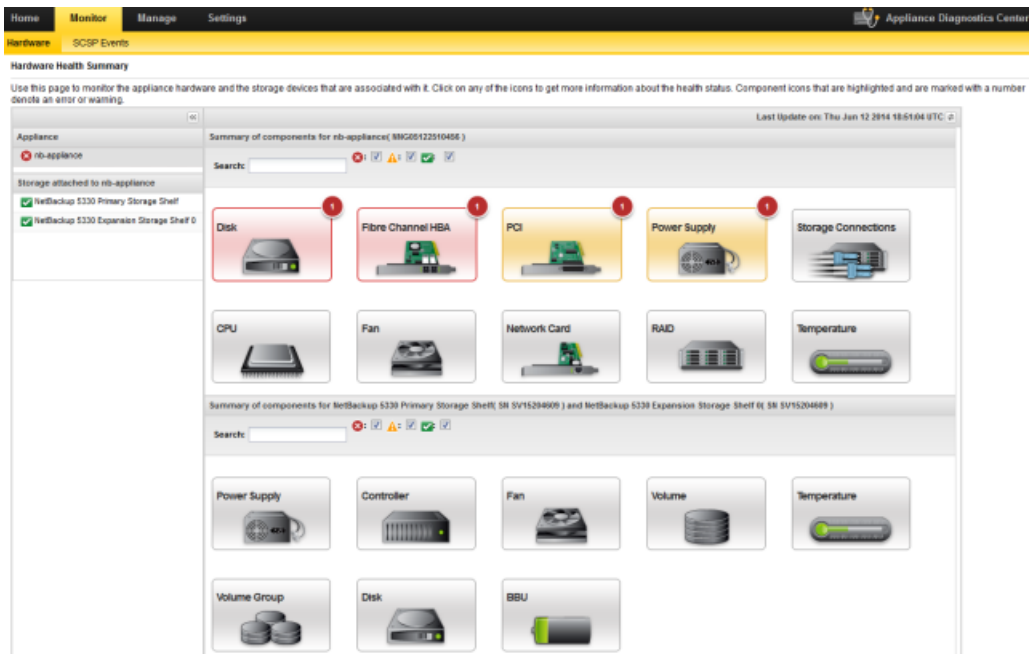


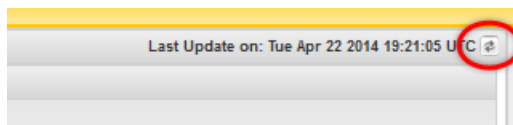
Table 2-3	Hardware components monitored in the 5330 appliance
Appliance	Disk, RAID, Fan, Power Supply, CPU, Temperature, Fibre Channel HBA, PCI, Network Card, Storage Connections
Primary storage shelf	Disk, Fan, Battery Backup Unit (BBU), Controller, Volume, Volume Group, Power Supply, Temperature
Expansion storage shelf	Disk, Fan, Power Supply, Temperature

Figure 2-2 Hardware components monitored in the 5330 appliance



The left pane of the **Monitor > Hardware** page lists **Appliance** and **Storage**. The right pane displays the **Summary of components** for the appliance and for the attached storage. The storage devices can include a 52xx storage shelf, a 5330 primary storage shelf, or a 5330 expansion storage shelf. Click on any of the components for further information, including health status and any errors or warnings.

The information that is displayed is generated from the last Call Home heartbeat. You can click the refresh icon to get the latest hardware information:



Interpreting errors or warnings

When any of the hardware components in the appliance report errors or warnings, the component icon is highlighted and marked with a number. If the hardware icon is highlighted in red, it denotes an error state and if it is highlighted in yellow, it

denotes a warning. The number denotes the number of errors or warnings that the hardware component encounters.

To get more information about the hardware health status, click the hardware component icon. Clicking a hardware component opens a pop-up window that displays information about the health status of the hardware component.

Monitoring storage connections

On a 5330 appliance, you can view the connections between hardware components to check the connection status. Click on **Storage Connections** under **Summary of components for appliance**. The following pop-up window appears:

The screenshot displays the 'Storage Connections' window. On the left, a diagram shows the 'Appliance nb-appliance' connected to the 'NetBackup 5330 Primary Storage Shelf' and the 'NetBackup 5330 Expansion Storage Shelf 0'. The center shows a detailed view of the 'NetBackup 5330 Primary Storage Shelf' with various components and their status indicators. On the right, there are two tables:

Connections				
State	ID	Appliance Port	Primary Storage Shelf Port	Status
✓	1	Slot1 Port1	A FC Ch1	Connected
✓	2	Slot1 Port2	B FC Ch1	Connected
✓	3	Slot4 Port1	A FC Ch2	Connected
✓	4	Slot4 Port2	B FC Ch2	Connected

Power Supply for NetBackup 5330 Primary Storage Shelf		
State	Location	Status
✓	Top	Optimal
✓	Bottom	Optimal

Click on the cables between the hardware components to see an overview of the connections between the appliance, the primary shelf, and the expansion shelf.

You can find more information on cable connections in the *NetBackup Appliance Hardware Installation Guide*.

Flashing a beacon

On a 52xx appliance, the **Disk** component for the appliance and the storage shelf includes an option to flash a beacon. The beacon helps to locate a disk within the appliance or the storage shelf and can be used to identify a disk that requires replacement.

Note: The beacon option is not currently available for the 5330 appliance.

To flash a beacon from the Hardware > Monitor page

- 1 Click on the **Disk** icon under **Summary of components for appliance** or **Summary of components for storage shelf**.
- 2 In the pop-up window that appears, select the disk ID that you want to flash and click **Beacon**.

To flash multiple beacons at once, hold down the **Shift** and the **Ctrl** keys on the keyboard and click on each of the disks that you want to locate. When all of your chosen disks are highlighted, click **Beacon**.

- 3 A pop-up window appears with the following message:

```
Enter the duration (from 1 to 300) for which the disk drive  
light should flash: (in minutes)
```

Provide the duration for which you want the disk to flash the beacon light. After you have entered the duration (in minutes), click **OK**.

The selected beacon flashes for the specified time. When the action is complete, the **Beacon** pop-up window updates with the result.

Hardware components that are monitored

The following tables list the hardware components and their attributes that are monitored in the appliance and in the attached storage.

Table 2-4 NetBackup 52xx and 5330 Appliance hardware that is monitored

Hardware monitored	Data collected
CPU	<ul style="list-style-type: none">■ 52xx: Status, Voltage, Low watermark, High watermark■ 5330: Status, Voltage, Low watermark, High watermark, BIOS firmware version

Table 2-4 NetBackup 52xx and 5330 Appliance hardware that is monitored
(continued)

Hardware monitored	Data collected
Disk	<ul style="list-style-type: none">■ 52xx: Beacon, Slot number, Status, Foreign state, Firmware version, Serial number, Capacity, Type, Enclosure ID■ 5330: Slot number, Status, Foreign state, Firmware version, Serial number, Capacity, Type, Enclosure ID <p>Note: The 5330 appliance includes two hot spares for the OS RAID volumes. When you receive your 5330 appliance, the disks that are located in slot 2 and slot 5 are configured as hot spares. However, if a disk in either RAID volume experiences a hardware error, the appliance uses one of the hot-spare disks to rebuild the RAID volume. When the faulty disk is replaced, the replacement disk becomes the new hot spare. The Disk icon on the Monitor > Hardware page of the NetBackup Appliance Web Console and the <code>Monitor > Hardware ShowHealth Appliance Disk</code> command in the NetBackup Appliance Shell Menu show which of the disks are currently configured as the hot spares. You can also use the RAID icon on the Monitor > Hardware page or the <code>Monitor > Hardware ShowHealth Appliance RAID</code> command to check if all hot spares are available.</p>
Fan	<ul style="list-style-type: none">■ Name, Status, Speed, Low watermark
Power Supply	<ul style="list-style-type: none">■ Status, Wattage, High watermark
RAID	<ul style="list-style-type: none">■ WWID, Name, Status, Capacity, Type, Disks, Write policy, Enclosure ID, Hotspare availability <p>Note: The WWID in the RAID table is a unique device ID of the disk. Clicking a WWID in the RAID table directs you to the Disk tab on the Manage > Storage page of the NetBackup Appliance Web Console. The console highlights the disk that corresponds to the WWID that is clicked. Clicking the highlighted Disk ID (or the WWID) on the Manage > Storage page opens a RAID status details window. The RAID details window provides status information about the RAID and the highlighted storage disk.</p>

Table 2-4 NetBackup 52xx and 5330 Appliance hardware that is monitored
(continued)

Hardware monitored	Data collected
Temperature	<ul style="list-style-type: none"> ■ Type, Temperature, Low watermark, High watermark <p>Note: The temperature readings for the P1 Therm Margin sensor and the P2 Therm Margin sensor are shown as negative values. The negative values indicate how hot (in degrees C) it can get before the CPU reaches the maximum heat tolerance. The low watermark and highwater mark for these sensors is -15 degrees C and -128 degrees C respectively.</p>
Adapter	<ul style="list-style-type: none"> ■ 52xx: Adapter model, Adapter status, BBU status, BBU Learn Cycle active, Charge, Charging status, Voltage, Temperature, Manufacturing date ■ 5330: N/A
PCI	<ul style="list-style-type: none"> ■ 52xx: Slot, Details ■ 5330: Slot, Details, Firmware
Fibre Channel HBA	<ul style="list-style-type: none"> ■ Status, Mode, PCI slot, Port World Wide Name (WWN), Speed, Remote Port <p>Note: Fibre Channel HBA ports that are marked with Initiator* mode indicate that they are configured for target mode when the SAN Client Fibre Transport media server is active. However, these ports are currently running in initiator mode, which implies that the SAN Client is disabled or it is inactive.</p>
Network Card	<ul style="list-style-type: none"> ■ Port name, PCI slot, Card model, Serial number, Port speed, MAC address, Link state <p>Note: On a 5330 appliance, there are two Ethernet ports in each 10-Gb Ethernet network interface card that is installed on the appliance. The number of ports depends on the appliance's PCIe slot configuration.</p> <p>See "NetBackup 5330 compute node Ethernet port configurations" on page 247.</p>
Storage Connections	<ul style="list-style-type: none"> ■ 52xx: N/A ■ 5330: Appliance port, Expansion Storage Shelf port, Status

Table 2-4 NetBackup 52xx and 5330 Appliance hardware that is monitored
(continued)

Hardware monitored	Data collected
Storage Status*	<ul style="list-style-type: none"> ■ 52xx: N/A ■ 5330: Status <p>Note: The Storage Status component monitors the health of the storage array as a whole. If a Storage Status error or warning message appears, the error cannot be acknowledged to suppress notifications. If you have Call Home enabled, Symantec is notified of the error, and a Support ticket is opened on your behalf. Symantec Support contacts you shortly afterward.</p> <p>If you do not have Call Home enabled and you receive a Storage Status error, contact Symantec Support for assistance.</p>
Partition Information*	<ul style="list-style-type: none"> ■ Partition, Total size, Used percentage, Status <p>Note: In the MSDP partition, the value that is displayed for the Used space may be different from the backup space that is available or used on the MSDP partition. The backup space statistics for the MSDP partition can be obtained by checking the MSDP disk pool sizes from the NetBackup Administration Console.</p>
MSDP*	<ul style="list-style-type: none"> ■ Queue size, Oldest tlog creation date

*This option is only available in the NetBackup Appliance Shell Menu, with the `Main > Monitor > Hardware` commands. See the *NetBackup Appliance Command Reference Guide* for more information.

Table 2-5 52xx Symantec Storage Shelf hardware that is monitored

Hardware monitored	Data collected
Disk	<ul style="list-style-type: none"> ■ Beacon, Slot number, Status, Foreign state, Firmware version, Serial number, Capacity, Type, Storage shelf ID
Fan	<ul style="list-style-type: none"> ■ Status, Speed, Low watermark
Power Supply	<ul style="list-style-type: none"> ■ Status

Table 2-5 52xx Symantec Storage Shelf hardware that is monitored
(continued)

Hardware monitored	Data collected
Temperature	<ul style="list-style-type: none"> ■ Type, Temperature, High watermark <p>Temperature monitoring includes the following temperature sensors that are located on the storage shelf:</p> <ul style="list-style-type: none"> ■ I/O Module1 (1) ■ I/O Module1 (2) ■ I/O Module2 (1) ■ I/O Module2 (2) ■ Backplane1 ■ Backplane2 ■ PSU1 (1) ■ PSU1 (2) ■ PSU2 (1) ■ PSU2 (2)

Table 2-6 5330 Primary Storage Shelf hardware that is monitored

Hardware monitored	Data collected
Disk	<ul style="list-style-type: none"> ■ Location, Status, Capacity, Associated Volume Group, Firmware version, Serial number
Fan	<ul style="list-style-type: none"> ■ Location, Status
Power Supply	<ul style="list-style-type: none"> ■ ID, Location, Status
Temperature	<ul style="list-style-type: none"> ■ Location, Status
BBU	<ul style="list-style-type: none"> ■ Location, Status
Controller	<ul style="list-style-type: none"> ■ Location, Status
Volume	<ul style="list-style-type: none"> ■ LUN, Status, Associated Volume Group, WWID, Capacity
Volume Group	<ul style="list-style-type: none"> ■ Volume Group name, Status, Associated Volume Group, RAID level, Capacity, Disks

Table 2-6 5330 Primary Storage Shelf hardware that is monitored
(continued)

Hardware monitored	Data collected
Storage Connections	<ul style="list-style-type: none">■ Primary Storage Shelf port, Expansion Storage Shelf port, Status <p>Note: This option is only displayed under the Primary Storage Shelf from the NetBackup Appliance Shell Menu. On the NetBackup Appliance Web Console, the connections information is included in the Storage Connections icon under the appliance.</p>

Table 2-7 5330 Expansion Storage Shelf hardware that is monitored

Hardware monitored	Data collected
Disk	<ul style="list-style-type: none">■ Location, Status, Capacity, Associated Volume Group, Firmware version, Serial number
Fan	<ul style="list-style-type: none">■ Location, Status
Power Supply	<ul style="list-style-type: none">■ Location, Status
Temperature	<ul style="list-style-type: none">■ Location, Status

About Email notification from a NetBackup appliance

A NetBackup Appliance has the ability to send an email to a local administrator when a hardware failure is detected. You can use the **Settings > Notification > Alert Configuration** page of the NetBackup Appliance Web Console to configure the email address that you want to use for hardware failure notifications. You can also use the command from the NetBackup Appliance Shell Menu. The contents of the email identifies the type of hardware failure that occurred and the status of the failure.

For complete information about how to configure email addresses using the NetBackup Appliance Shell Menu, refer to the *NetBackup™ Appliance Command Reference Guide*.

The following is an example of an email notification that is sent in case of any hardware failures.

Hardware Alerts

Dear customer,

Your appliance **XXXXXXXXXXXX** (**XXXXXXXXXX**) has encountered the following error(s):

- Disk is missing from slot.
 - Time of event: 2015-10-01T16:41:26.78461302-07:00
 - UMI Event code: V-475-100-1005
 - Component Type: Disk
 - Component: Enclosure 51 Disk 16
 - Status: Missing
 - State: ERROR
 - Additional information about this error is available at following link:
[V-475-100-1005](#)

If AutoSupport is enabled on your appliance, this information is automatically transmitted to Veritas for further analysis.

Producing a DataCollect package prior to support engagement may help in expediting resolution. For information on how to gather the logs that are created by the DataCollect utility, refer to the *NetBackup Appliance Administrator's Guide*.

Best Regards,
Veritas Customer Support

About Symantec Data Center Security on the NetBackup appliance

Note: In previous appliance releases, Symantec Data Center Security (SDCS) was known as Symantec Critical System Protection (SCSP). As part of the upgrade to NetBackup Appliance 2.7.1, the appliance SDCS agent is set to unmanaged mode. If an appliance was running in managed mode before upgrade, make sure to reset that appliance back to managed mode after the upgrade completes.

You must also update the appliance IPS and IDS policies on your SDCS management server. You cannot use the older policies to manage an appliance that is running software version 2.7.1 or newer. The new policies can be downloaded from the **Monitor > SDCS Events** page of the NetBackup Appliance Web Console. Also note that any custom rules or support exceptions you might have for the IPS and IDS policies are not available after an upgrade to NetBackup Appliance 2.7.1.

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 appliance intrusion prevention system (IPS) and intrusion detection system (IDS) policies. The overall SDCS solution on the appliance provides the following features:

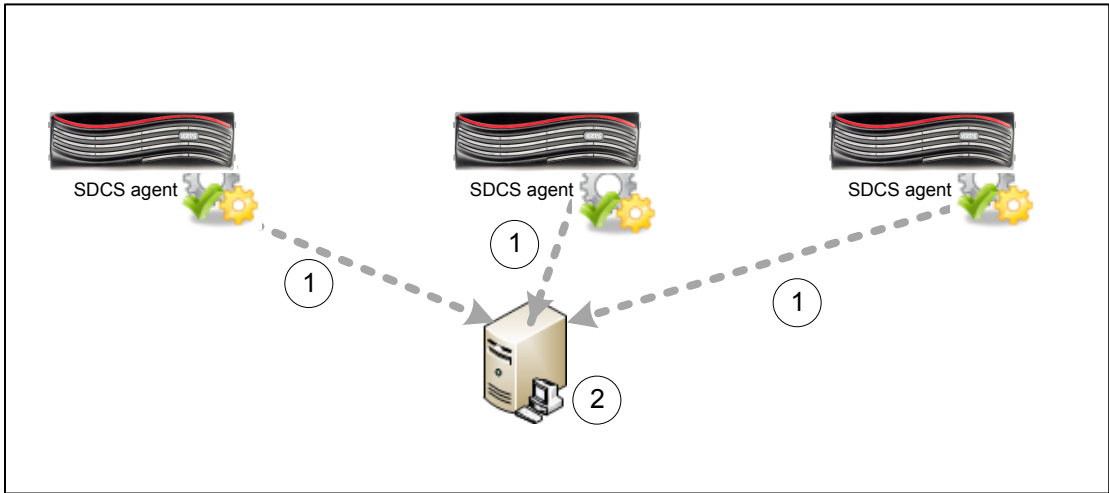
- **Hardened Linux OS components**
Prevents or contains malware from harming the integrity of the underlying host system as a result of OS vulnerabilities.
- **Data protection**
Tightly limits appliance data access to only those programs and activities that need access, regardless of system privileges.
- **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.
- **Centralized managed mode operations**
Lets you use a central SDCS manager for an integrated view of security across multiple appliances as well as any other enterprise systems managed by SDCS.

The SDCS implementation on the appliance can operate in an unmanaged mode or a managed mode. By default, SDCS operates in an unmanaged mode and helps secure the appliance using host-based intrusion prevention and detection technology. The NetBackup appliance is in unmanaged mode, when it is not connected to the SDCS server. In unmanaged mode, you can monitor SDCS events from the NetBackup Appliance Web Console. Use the **Monitor > SDCS Events** page, to monitor the events logged. The events are monitored using the NetBackup appliance IDS and IPS policies. These policies are automatically applied at the time of initial configuration. Click **Filter Logs** to filter and view specific events.

In managed mode, the SDCS agent on the appliance continues to protect the appliance while also connecting to an external SDCS server for centralized management and log analysis. In managed mode, the appliance is connected to the SDCS server and the events are monitored using the SDCS management console. Using this mode multiple appliances can be monitored using a single SDCS server. SDCS agents are configured with each NetBackup appliance that are used to send events to the SDCS server.

[Figure 2-3](#) illustrates SDCS in managed mode.

Figure 2-3 SDCS implementation in managed mode



To set up managed mode, you can install the SDCS server and management console and then connect the appliance to an SDCS server.

Use **Monitor > SDCS Events** page to:

- Download SDCS server and console
- Install the server and console
- Download NetBackup Appliance IPS and IDS policies
- Apply these policies using the SDCS management console
- Connect the NetBackup appliances with the server
- Monitor events for all the NetBackup appliances connected to this server.

Use **Monitor > SDCS Events > Connect to SDCS server** to:

- Add SDCS server details
- Download authentication certificate
- Connect to the SDCS server

For complete information about the SDCS implementation on the appliance, refer to the *NetBackup Appliance Security Guide*.

Monitor > SDCS Events

You can use the **Monitor > SDCS Events** menu to monitor the Symantec Data Center Security (SDCS) agent and event logs.

The SDCS agent is installed and configured when you initially configure your appliance. This agent ensures that your appliance's audit logs are sent to the SDCS server to be validated and verified.

The **Monitor > SDCS Events** page displays the following:

- **Filter Logs** - Filter the SDCS audit logs that get displayed on the **SDCS Events** page.
- **Current Log Retention** - Displays the current log retention level. When the appliance is configured in a managed mode, the status is set to **Not Applicable** as the audit logs are monitored using the SDCS server.
- **Set Log Retention** - Set the SDCS log retention by period days or number of log files.
- **Connect to SDCS server** - Connect to an SDCS server to configure the appliance in managed mode.
- **Symantec Data Center Security Downloads** - Download the SDCS server and console, and the IPS and IDS policies.

Note: You can manually implement third-party certificates on web service support using the Java keystore repository of security certificates. For more information, See [“Implementing third-party SSL certificates”](#) on page 58.

[Table 2-8](#) describes the event attributes for each sortable column of the SDCS event viewer.

Table 2-8 SDCS event attributes

Columns	Description
Event ID	The ID generated for each event log. The event ID can be used to search the event logs.
Date and Time	The date and time for each event log.
Event Type	The event type for each event log. For example, if the event type is Server Error , it denotes that a server error has occurred and is recorded in the event logs.

Table 2-8 SDCS event attributes (*continued*)

Columns	Description
Severity	<p>The severity of each event in the log. For example, an event like the Server Error would be of Critical severity.</p> <p>The following severity types are displayed:</p> <ul style="list-style-type: none">■ 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.
Message	<p>The message that describes the logged event.</p>
Details	<p>Details of each logged event. Click the Log Details pop-up window icon to view the details of the logged event. For a list of all the possible details that can be displayed, refer to the SDCS documentation.</p>

Viewing SDCS audit log details

You can view the detailed information for each Symantec Data Center Security (SDCS) logged event using the **SDCS Events** page. Click the **Log Details** pop-up window icon to view the details of the logged event. [Table 2-9](#) describes the various details that displayed in the **Log Details** pop-up window.

Table 2-9 SDCS log details description

Detail	Description
Event Severity	<p>The severity of the logged event.</p> <p>The following severity types are displayed:</p> <ul style="list-style-type: none"> ■ 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.

Filtering SDCS audit logs

The following procedure describes how to filter the SDCS audit logs displayed on the **Monitor > SDCS Events** page of the NetBackup Appliance Web Console.

To filter SDCS audit logs

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Monitor > SDCS Events**.

The **Monitor > SDCS Events** page contains an event viewer that displays the audit logs for the last 6 hours.

- 3 Click the **Filter Logs** button.

The **Filters** dialog box is displayed.

- 4 Use the following fields to enter the filter criteria:

Field	Description	Example
Search String	Enter a search string to filter audit logs using the parameters mentioned in the string.	Outbound connections
Event Id	Enter the event ID to filter audit logs by ID number.	1375524
Events	Select an event type from the drop-down list to filter the audit logs by event type.	IDS Audit
Severities	Select a severity type for the logs to be filtered and displayed.	Critical
From Date From Time	Select the From and To date and time. The appliance displays the audit logs for the selected time period.	03/10/2011, 14.19.01 to 04/10/2011, 14.19.01
To DateTo Time		

- 5 Click the **Apply** button to apply the filter.

The appliance displays the relevant logs in the audit log viewer.

Setting the SDCS audit log retention specification

When your appliance is not connected to a Symantec Data Center Security (SDCS) server, the SDCS logs are still stored locally on the appliance. The following

procedure describes how to set the audit log retention using the NetBackup Appliance Web Console.

Note: When the appliance is configured in a managed mode, the status is set to **Not Applicable** and the **Set Log Retention** button is disabled. That is because the audit logs are monitored using the connected SDCS server.

To set the audit log retention

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Monitor > SDCS Events**.
- 3 The **Monitor > SDCS Events** page contains an event viewer that displays the audit logs for the last 6 hours.

Note: If the appliance is running in managed mode the SDCS events viewer does not display the audit logs.

- 4 Click on the **Set Log Retention** button, to set the retention period or log file number.

The appliance displays the **Retention Settings** dialog box.

- 5 You can set the retention using the following fields:

Field	Description
Period	<p>Select this radio button to set the log retention in number of days.</p> <p>The retention period setting considers the date on which a log file is modified over the date on which the file is created. For example, if the retention period is set to two days. The files that have been modified in the last two days will not be pruned, even though their creation data is older than two days.</p>
Days	<p>Enter the number of days. The appliance stores the SDCS audit logs for the specified number of days. This field is enabled, when you select the Period radio button.</p>
Number of Logs	<p>Select this radio button to enter the number of log files to be retained.</p>
FileNumber	<p>Set the audit number of files. Size of each file is 10 MB.</p>

- 6 Click **OK** to set the retention specifications.

The appliance applies the retention specifications and stores the logs accordingly.

About Symantec Data Center Security Downloads

By default, SDCS operates in an unmanaged mode and helps secure the appliance using host-based intrusion prevention and detection technology. In managed mode, the SDCS agent on the appliance continues to protect the appliance while also connecting to an external SDCS server for centralized management and log analysis. The unmanaged mode lets you segregate the tasks of a backup administrator and a security administrator, where in a security administrator is provided with the ability to monitor and manage the security options for all of the NetBackup appliances included in a large enterprise.

The following are required to run the appliance in unmanaged mode:

- A management server running the Symantec Data Center Security: Server Advanced 6.5 or later.
- A computer running the Symantec Data Center Security: Server Advanced management console. (The SDCS management console is required to apply the IPS and IDS policies.)

The SDCS server and console software as well as the appliance IPS and IDS policies can be downloaded from the **Monitor > SDCS Events** page of the NetBackup Appliance Web Console.

Warning: You must apply the downloaded IPS and IDS policies as soon as you connect the appliance to the SDCS server. Without applying the policies, there won't be any intrusion prevention and intrusion detection policies on the system to be enforced by the SDCS agent.

Downloading the SDCS server and console software from the NetBackup appliance

The following procedure describes how to download the SDCS server and console software packages from the **SDCS Events** page.

To download the SDCS server and console:

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Monitor > SDCS Events**.
- 3 Under **Symantec Data Center Security Downloads**, click **SDCS Server and Console** to download the installation packages for the SDCS server and console.

The `sdcserver.zip` file is downloaded to your local computer.

- 4 Extract the contents from the `sdcserver.zip` file.

The `SDCSInstall` folder contains the following:

- `server.exe` - used to install the Symantec Data Center Security: Server Advanced management server.
An installation wizard is used to help you install the management server. For more information about installing the SDCS management server, refer to the *Symantec Data Center Security Installation Guide* available at the following location:
https://support.symantec.com/en_US/article.DOC7979.html.
- `console.exe` - used to install the Symantec Data Center Security: Server Advanced management console.
An installation wizard is used to help you install the management console. For more information about installing the SDCS management console, refer to the *Symantec Data Center Security Installation Guide* available at the following location:
https://support.symantec.com/en_US/article.DOC7979.html.

Downloading the IPS and IDS policies from the NetBackup appliance

The following procedure describes how to download the NetBackup appliance IPS and IDS policies for using Symantec Data Center Security (SDCS) in unmanaged mode.

To download NetBackup appliance IPS and IDS policies:

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Monitor > SDCS Events**.
- 3 Under **Symantec Data Center Security Downloads**, click **NetBackup Appliance IPS and IDS Policies** to download the IDS and IPS policies.

The `SDCSSPolicies.zip` file is downloaded to your local folders.

- 4 Extract the contents from the `SDCSSPolicies.zip` file.

The `SDCSSPolicies` folder contains the following:

- `NetBackup Appliance Detection Policy.zip` - contains the IDS policy. This policy is an “after-the-fact” IDS for monitoring important significant events and optionally taking remediation actions on events of interest.
- `NetBackup Appliance Prevention Policy.zip` - contains the IPS policy. This policy is an “in-line” IPS that can proactively block unwanted resource access behaviors before they can be acted upon by the operating system.

Note: These policies help to validate the events that take place on appliance and can be monitored by either using the **Monitor > SDCS Events** page in an unmanaged mode or the SDCS management console.

- 5 After you have set up the SDCS server and connected the appliance to it, use the SDCS management console to apply the IPS and IDS policies.

See “[Connecting to the SDCS server](#)” on page 57.

For instructions on how to apply policies using the SDCS management console, refer to the *Symantec Data Center Security: Server Advanced Administrator's Guide* at the following location:

https://support.symantec.com/en_US/article.DOC7979.html

Warning: You must apply the downloaded IPS and IDS policies as soon as you connect the appliance to the SDCS server. Without applying the policies, there won't be any intrusion prevention and intrusion detection policies on the system to be enforced by the SDCS agent.

Connecting to the SDCS server

The following procedure describes how to connect to the Symantec Data Center Security (SDCS) server from the **SDCS Events** page of the NetBackup Appliance Web Console.

Note: You cannot connect to an SDCS server without providing its authentication certificate. You can either download the certificate from the site or point to a downloaded certificate earlier, from your local folders.

To connect an SDCS server

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **SDCS Events**.
- 3 Under **Connect to SDCS server**, click **Connect**.
The **Connect to SDCS Server** dialog box appears.
- 4 Enter a valid host name or IP address of the SDCS server in the **Host Name / IP** field.
- 5 Enter the port number of the SDCS server in the **Port** field.
- 6 Select either **Download authentication certificate from the SDCS server** or **Provide the location for the existing certificate**.
The appliance displays the certificate details.
- 7 Click on **Accept Certificate** to accept the certificate.
The appliance displays the **Certificate issued** message.
- 8 Click **Connect** to connect to the SDCS server.
The appliance has connected to the SDCS server successfully when the following message appears:
Connected successfully to SDCS server.

Revert SDCS to unmanaged mode on a NetBackup appliance

If you have set up an appliance to operate in managed mode, you can use the following procedure to revert it back to unmanaged mode and disconnect it from the SDCS server:

To revert the NetBackup appliance from managed mode back to unmanaged mode

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Monitor > SDCS Events**.

- 3 Under **Connect to SDCS server**, click **Connect**.
The **Connect to SDCS Server** dialog box appears.
- 4 Enter **127.0.0.1** or **localhost** in the **Host Name / IP** field.
- 5 Enter the port number of the appliance in the **Port** field.
- 6 Click **Connect**.
The appliance reverts to the unmanaged mode.

Implementing third-party SSL certificates

You can manually add and implement third-party certificates for the web service support. The appliance uses the Java KeyStore as the repository of security certificates. A Java KeyStore (JKS) is a repository of security certificates, like the authorization certificates or the public key certificates that are used for instance in SSL encryption. If you want to implement third-party certificates, use the following procedure:

To implement third-party SSL certificates:

- 1 Prepare keystore file for web services. The procedure varies with the type of PKCS (Public-key Cryptography Standards) you use, the following table describes the steps to use PKCS# 7 and PKCS# 12 standard formats

PKCS format	Preparing keystore files
-------------	--------------------------

PKCS#7 or X.509 format	You can use the following link:
------------------------	---------------------------------

	https://knowledge.verisign.com/support/ssl-certificates-support/index.html
--	---

PKCS format Preparing keystore files

- PKCS#12 format 1 Convert PEM formatted x509 Cert and Key to a PKCS# 12, using the following commands:

```
openssl pkcs12 export -in server.crt -inkey
server.key -out server.p12 -name some-alias
-CAfile ca.crt -caname root
```

For more information on `openssl` usage, refer to <http://www.openssl.org/>.

Note: Ensure that you put a password on the PKCS #12 file. When the password is not applied to the file, you may get a null reference exception when you try to import the file

- 2 Convert the pkcs12 file to a Java Keystore using the following commands:

```
keytool -importkeystore -deststorepass
changeit -destkeypass changeit -destkeystore
server.keystore -srckeystore server.p12
-srcstoretype PKCS12 -srcstorepass some-
password -alias some-alias
```

For more information on `keytool` usage, refer to <http://docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html>

- 2 Shutdown web service using the following command:

```
/etc/init.d/nbappws stop
```

- 3 Replace the existing keystore file with your new keystore file. The default file name is `/opt/SYMCnbappws/Security/keystore`.

- 4 Correct the following information in the configuration files:

- Change the `keystoreFile` and `keystorePass` settings in the `/opt/SYMCnbappws/config/server.xml`.
- Change the `keystoreFile` and `keystorePass` settings in the `/opt/SYMCnbappws/webserver/conf/server.xml`.
- Change the `javax.net.ssl.trustStore` and `javax.net.ssl.trustStorePassword` settings in the `/opt/SYMCnbappws/bin/startgui.sh`.

- 5 Startup web service using the following command:

```
/etc/init.d/nbappws start
```

Managing a NetBackup appliance from the NetBackup Appliance Web Console

This chapter includes the following topics:

- [About the Manage views](#)
- [About storage configuration](#)
- [About appliance supported tape devices](#)
- [About configuring Host parameters for your appliance](#)
- [Manage > Appliance Restore](#)
- [Manage > License](#)
- [About the Migration Utility](#)
- [Software release updates for NetBackup Appliances](#)
- [Manage > Additional Servers](#)
- [Manage > Certificates](#)

About the Manage views

The NetBackup Appliance enables you to use the NetBackup Administration Console to manage your clients, create policies, run backups, and perform other

administration functions. For information on how to perform these functions from the NetBackup Administration Console, you must refer to your NetBackup core documentation set. If you want to download the latest versions of this documentation set, you can do so from the Symantec Support Web site. For help using the NetBackup Administration Console, refer to the *Symantec NetBackup Administrator's Guide, Volume I* on the Symantec Support Web site.

You can use the **Manage** tab in the NetBackup appliance user interface to view and configure the following settings.

[Table 3-1](#) describes the tabs included in the **Manage > Host** menu:

Table 3-1 Manage > Host

Manage	Lets you...	Topic
Data Buffer	Configure the data buffer parameters using Data Buffer tab in the NetBackup Appliance Web Console.	See "Manage > Host > Data Buffer options" on page 116.
Lifecycle	View and change the lifecycle parameters using this tab when the appliance is configured as a master server.	See "Manage > Host > Lifecycle options" on page 118.
Deduplication	View and change the deduplication parameters using this tab.	See "About configuring deduplication solutions" on page 122.
Advanced	Enable Bare Metal Restore (BMR) from this tab when the appliance is configured as a master server.	See "About BMR integration" on page 125.
IPMI	Reset the IPMI. The reset operation involves restarting the IPMI.	See "Manage > Host > IPMI options" on page 126.

[Table 3-2](#) describes the **Manage > Storage** menu:

Table 3-2 Manage > Storage

Manage	Lets you...	Topic
Capacity Distribution section	View a graphical representation of the storage partitions within your appliance. The donut chart shows the storage partitions that are configured.	See “Manage > Storage” on page 67.
Capacity Chart section	View an overview of storage capacity usage ranges for specific periods of time.	
Partitions section	View details about all the partitions that are configured on the Appliance.	
Disks section	View a tabular representation of the storage disks that comprise your appliance and the storage shelves that are attached to it.	

[Table 3-3](#) describes the tabs included in the **Manage > Migration Utility** menu:

Table 3-3 Manage > Migration Utility

Manage	Lets you...	Topic
Policy Conversion	Select the start time, the migration window (duration), the source disk pool where the current backup images reside, and the destination (target) disk pool where you want the images migrated.	See “Policy Conversion” on page 166.
Selection Criteria	Change the policy that you want to use for the backups that are now targeted for the destination disk pool.	See “Selection Criteria” on page 159.
Migration Job Status	View the status and the result of all the scheduled migration jobs.	See “Migration Job Status” on page 163.

[Table 3-4](#) describes the individual following sub-menus under the **Manage** menu:

Table 3-4 Manage > Appliance Restore, License, Software Updates, Additional Servers

Manage	Lets you...	Topic
Appliance Restore	Reset 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.	See “ Manage > Appliance Restore ” on page 127.
NetBackup License	Review, add, and delete license keys through the administrative Web UI.	See “ Manage > License ” on page 153.
Software Updates	View, install, or delete a software update on your appliance. This screen contains two tables that show the software updates that are available for you to download for your appliance and the software updates that you can choose to install or delete. This screen also displays the NetBackup Appliance software version that is currently installed on your appliance.	See “ Software release updates for NetBackup Appliances ” on page 170.
Additional Servers	Add or delete additional servers. This tab lets you add an entry to the NetBackup bp.conf file. The bp.conf file allows communication to occur between the appliance and the Windows NetBackup Administration Console, so you can manage your appliance through that console. Note: This tab is only displayed for an appliance configured as a master server.	See “ Manage > Additional Servers ” on page 196.

About storage configuration

The NetBackup Appliance Web Console enables you to manage the storage configuration. You can use the **Manage > Storage** pane to manage the storage space.

The Symantec NetBackup 5220 and 5230 appliance is available for use with up to four Symantec storage shelves. The storage shelves provide you with additional disk storage space. After you have physically connected the storage shelves, use the NetBackup Appliance Web Console to manage the storage space.

The Symantec NetBackup 5330 appliance must be connected to one Primary Storage Shelf. The storage space can be expanded by using up to two Expansion Storage Shelves. After you have physically connected the Expansion Storage Shelf, use the NetBackup Appliance Web Console to manage the storage space.

Note: The 5330 appliance (base unit) does not have internal disk space available for backups or storage. It only stores the OS, logs, checkpoints etc. The space available from the Primary Storage Shelf and the Expansion Storage Shelf can be used for backups.

- If you have a NetBackup 5330 Appliance with an Expansion Storage Shelf, the following restrictions apply:
- Moving an Expansion Storage Shelf from one 5330 appliance to another 5330 appliance is not supported.
 - Moving disk drives within an Expansion Storage Shelf is not supported.

Figure 3-1 provides a bird's-eye view of how storage space is configured within your 52xx appliance.

Figure 3-2 provides a bird's-eye view of how storage space is configured within your 5330 appliance.

Figure 3-1 NetBackup 52xx Appliance storage space

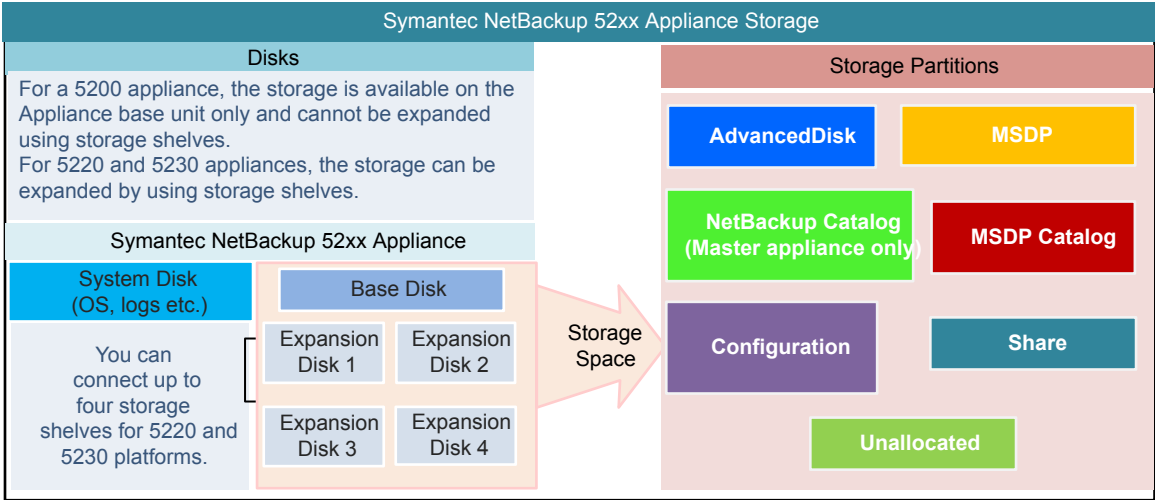


Figure 3-2 NetBackup 5330 Appliance storage space

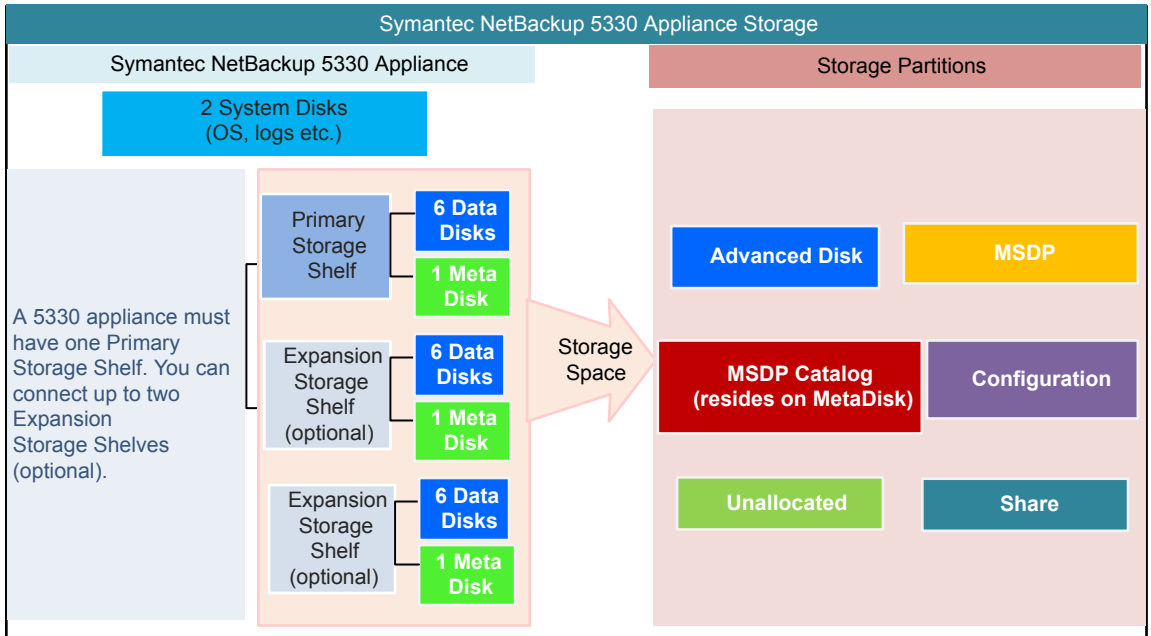


Figure 3-3 lists the tasks that you can perform on the appliance storage space.

Figure 3-3 Storage operations

Storage Operations	
<p>Tasks performed on Storage Disks</p> <p>To perform the tasks listed below:</p> <ul style="list-style-type: none"> - Go to Manage > Storage > Disks in the Appliance console. - Use the Manage > Storage shell menu <p>Add</p> <p>Adds a disk in the New Available state. Adds disk space to the unallocated storage.</p> <p>Command - Add <Disk ID></p> <p>Remove</p> <p>Removes disk space from the unallocated space.</p> <p>Command - Remove <Disk ID></p> <p>Scan</p> <p>Refreshes the storage disks and devices information.</p> <p>Command - Scan</p> <p>Show Disk</p> <p>Shows the disk's total and unallocated storage capacity and status.</p> <p>Command - Show Disk</p> <p>Tasks Common to Disks and partitions</p> <p>Monitor</p> <p>Displays progress of storage management tasks like Add, Remove, and so on.</p> <p>Command - Monitor</p> <p>Show Distribution</p> <p>Shows the distribution of partitions on a disk.</p> <p>Command - Show Distribution</p>	<p>Tasks performed on Storage Partitions</p> <p>To perform the tasks listed below:</p> <ul style="list-style-type: none"> - Go to Manage > Storage > Partitions in the Appliance console. - Use the Manage > Storage shell menu <p>Create</p> <p>Creates a share partition only.</p> <p>Command - Create Share</p> <p>Delete</p> <p>Deletes a share partition only.</p> <p>Command - Delete Share <ShareName></p> <p>Edit</p> <p>Edits the description and client details of a share.</p> <p>Command - Edit Share <Details> <ShareName></p> <p>Move</p> <p>Moves the partition from one disk to another.</p> <p>Command - Move <Partition> <SourceDisk> <TargetDisk> [Size] [Unit]</p> <p>Resize</p> <p>Create, resize, or delete a partition. You can delete a partition if Appliance is in a factory state (not configured as a master or media server).</p> <p>Command - Resize <Partition> <Size> <Unit></p> <p>Show Partition</p> <p>Shows the partition's total, available, and used storage capacity. You can also view configuration and usage information for all partitions or specific partitions.</p> <p>Command - Show Partition <All/Configuration/Usage> [PartitionType]</p>

All the tasks that can be performed on the NetBackup Appliance Web Console can also be performed by using the `Manage > Storage` shell menu.

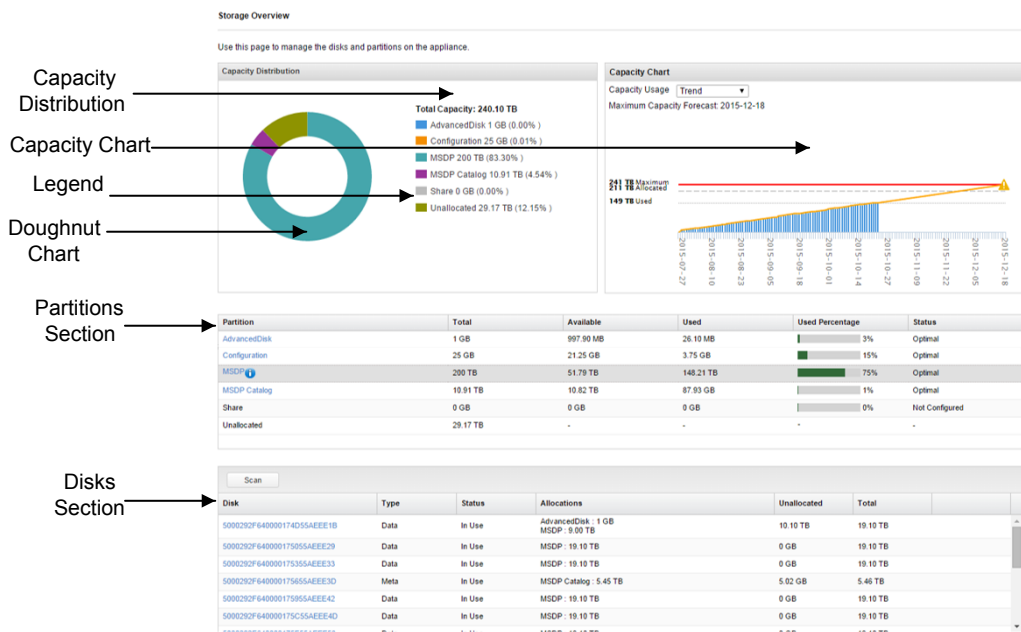
For more information about `Main > Manage > Storage` commands, refer to *NetBackup™ Appliance Command Reference Guide*.

Manage > Storage

The `Manage > Storage` menu enables you to manage the storage configuration. Use the **Capacity Distribution** section to quickly view the storage configuration. From the **Partitions** and **Disks** sections, you can manage this storage space.

Figure 3-4 shows a sample view of `Manage > Storage` page for a 5330 appliance.

Figure 3-4 `Manage > Storage` page for a 5330 appliance



The **Capacity Distribution** section provides a graphical representation of the storage partitions within your appliance. The doughnut chart shows the storage partitions that are configured. It also shows how each partition is sized. The legend that adjacent to the doughnut chart displays the color and size of each partition. Only the configured partitions display as links in the legend and can be clicked.

The **Capacity Chart** section provides an overview of storage capacity usage ranges for specific periods of time. You can select one week to one year from the drop-down list. When you select **Trend** from the drop-down list, Netbackup Appliance analyzes the past storage capacity usage, and calculates when the available storage is fully used.

Appliance collects the capacity usage data at 1:00 AM (server time) everyday and updates the capacity chart several minutes later. It indicates that the display of the capacity chart is not real time but has one-day delay. For example, to check the capacity usage by 2015-10-10, you need to wait until 1:05 AM on 2015-10-11.

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

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 master server.
The NetBackup Catalog is always located on a Base disk on a 52xx appliance.

Configuration A storage partition that stores configuration information.

MSDP The allocated space for Media Server Deduplication (or MSDP) on your appliance.

On a 5220 or 5230 appliance, the MSDP partition should reside on an expansion disk for optimum performance.

See ["Moving the MSDP partition from a base disk to an expansion disk for optimum performance"](#) on page 81.

MSDP Catalog This partition contains metadata for MSDP which includes information regarding MSDP backups.

On the 52xx appliances, the MSDP Catalog partition can either exist on the Base or the Expansion disk. On a 5330 appliance, the MSDP Catalog partition is located on a dedicated disk that called the Metadisk. The Metadisk contains the MSDP Catalog partition only.

Share This partition contains all of the shares that have been allocated for database backups.

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.

See the NetBackup documentation for more information on partitions.

[Table 3-5](#) lists the supported sizes and platforms for each partition.

Table 3-5 Appliance storage partitions

Partition Name	Minimum supported size	Maximum supported size	Supported Platforms
AdvancedDisk	1 GB	Maximum available capacity	5200, 5220, 5230 5330
NetBackup Catalog	250 GB (Master server)	4 TB (Master server)	5200, 5220, 5230 (master server only)
Configuration	25 GB	500 GB	5200, 5220, 5230 5330
MSDP	5 GB	Maximum available capacity	5200, 5220, 5230 5330
MSDP Catalog	5 GB	25 TB	5200, 5220, 5230, 5330
Share (Copilot)	5 GB	Maximum available capacity The limit for each individual share is 250 TB	5230, 5330

The **Partitions** section displays details about all the partitions that are configured on the Appliance. The following columns are displayed in the Partitions table:

Column Name	Description
Partition	<p>Displays the name of the partition.Example: AdvancedDisk</p> <p>Clicking the partition name opens another page that shows details about the specific partition and also lets you resize and move the partition.</p> <p>Checking partition details lists details about the partition.</p>
Status	<p>Displays the status of the partition.</p> <p>Example: Optimal</p> <p>Table 3-6 describes each partition status.</p>
Used	<p>Displays the used space within a partition.</p> <p>Example: 13.70 GB</p>
Available	<p>Displays the free space within a partition.</p> <p>Example: 1.62 TB</p>
Total	<p>Displays the total space within the partition.</p> <p>Example: 1.63 TB</p>
Used Percentage	<p>Displays the percentage of used space in the partition.</p> <p>Example: 2%</p>

Note: The sizes that are displayed for the MSDP partition on the **Manage > Storage** page or by using the **Manage > Storage > Show** command on the NetBackup Appliance Shell Menu 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 it's 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.

[Table 3-6](#) describes the various partition status that is displayed next to the partition type.

Table 3-6 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.

Click any partition from the **Partition** section to go to the partition detail page. For more information about partition details page, see [Checking partition details](#)

[Table 3-7](#) describes the various partition states.

Table 3-7 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 3-6 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 3-6 for more information.

The **Disks** section provides a tabular representation of the storage disks that comprise your appliance and the storage shelves that are attached to it.

You must scan for new disks when you connect new storage. You must also scan to refresh the storage information when you disconnect and reconnect storage to the Appliance.

Click **Scan** to scan for new disks and then click **OK** to confirm the prompt.

Note: If you are scanning the 5330 appliance for the first time, disk initialization may take some time. The disk initialization happens in the background and may take up to 56 hours depending on the system load. The estimated time is up to 28 hours for a Primary Storage Shelf and up to 28 hours for an Expansion Storage Shelf. You can continue to use the appliance during this time. However, if one or more of the new disks are used by partitions during the disk initialization process, the performance of backup and restore operations on the specific disks degrades by up to 30%.

If you want to expand storage and attach a Storage Shelf or an expansion system to an appliance, see the *Symantec NetBackup Appliance Hardware Installation Guide* for the appropriate platform. Once these Storage Shelves or expansion systems are properly connected to the Appliance, you must scan for the newly available disks from the **Disks** section. The new disks have the **New Available** status. Once the newly available disks are displayed, these disks must be added so the additional space can be used.

See [“Adding the storage space from a newly available disk”](#) on page 85.

The following columns are displayed in the table:

Column names	Description
Disk	Displays the ID that is associated with the disk. Example: 50001FAFA000000F5B0519CB4
Type	Displays the type of disk. Example: Base Table 3-8 describes each disk type.
Status	Displays the status of the disk. Example: In Use Table 3-9 describes each status.
Allocations	Lists the partitions that exist on each disk. Also lists the size of each partition. Example: AdvancedDisk: 18 TB
Unallocated	Displays the available space within the disks that has not been allocated. Example: 1.9172 GB

Column names	Description
Total	Displays the total storage space within the disk. Example: 4.5429 TB

[Table 3-8](#) lists the disk types that can appear depending on your Appliance platform.

Table 3-8 Disk Types

Type	Description	Supported Platforms
System	This category tells you the storage that is occupied by the appliance operating system, logs etc.	5200, 5220, 5230 5330
Base	This category tells you the storage that is available with the appliance base unit.	5200, 5220, 5230
Expansion	A storage shelf that is connected to a 5220 or 5230 appliance.	5220, 5230
Data	All partitions, except MSDP Catalog, exist on the Data disk. Examples of partitions that exist on the data disks are MSDP, AdvancedDisk, Configuration etc. There can be six data disks for a Primary Storage Shelf and six for an Expansion Storage Shelf.	5330
Meta	The MSDP Catalog partition exists only on the Meta disk. There can be one Meta disk for a Primary Storage Shelf and one for an Expansion Storage Shelf.	5330
Unknown	This category appears when appliance cannot determine the disk type like when the disk is not accessible.	Not Applicable

[Table 3-9](#) describes the various status that is displayed in the **Status** field.

Table 3-9 Disk Status

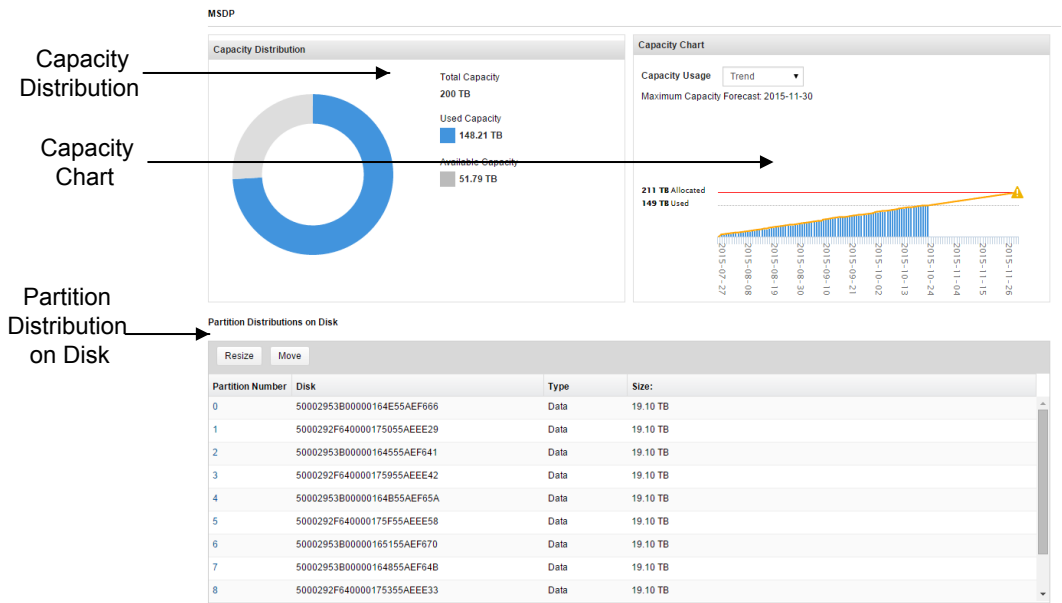
Status	Description
Foreign	<p>Denotes that the disk has storage configuration information, and may contain data.</p> <p>The Remove link is displayed next to all Foreign disks. You can remove any pre-existing data from a Foreign disk. After you remove a Foreign disk, the status of the disk is New Available.</p> <p>Disk status is displayed as Foreign, when:</p> <ul style="list-style-type: none"> ■ A disk that was In Use was physically disconnected, later reconnected. In this case, restarting the appliance would bring the disk status back to its previous state. ■ A disk that was In Use was physically disconnected. The Appliance was reimaged and reconfigured and the disk is connected back. <p>Or</p> <ul style="list-style-type: none"> ■ A disk that was connected to another system still has configuration information of the old system
In Use	<p>Denotes that the disk is currently in use.</p> <p>The Remove link is displayed if the disk does not have any partition.</p>
n/a	<p>Denotes that no commands or operations can be performed on disks with this status.</p> <p>An example of a disk that has n/a status is System.</p> <p>An example of a disk that has n/a status is Operating System.</p>
New Available	<p>Denotes that the disk is available to be added to the storage space. The Add link is displayed to add the storage disk to the storage space.</p>
Not Accessible	<p>Storage disk that was In Use is not accessible any more.</p>

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 Symantec Support team to resolve disk-related issues. More information about the `Main > Support > Datacollect` menu is available.

Checking partition details

Figure 3-5 shows a sample view of partition details page for a 5330 appliance.

Figure 3-5 Partition details page for a 5330 appliance



The **Capacity Distribution** section provides a graphical representation of a specific storage partition within your appliance. The doughnut chart shows the storage partition that is configured. It also shows how the specific partition is sized. The legend that adjacent to the doughnut chart displays the color and size of the partition. Only the configured partitions display as links in the legend and can be clicked.

The **Capacity Chart** section provides an overview of storage capacity usage ranges for specific periods of time. You can select one week to one year from the drop-down list. When you select **Trend** from the drop-down list, Netbackup Appliance analyzes the past storage capacity usage, and calculates when the available storage is fully used.

The **Partition Distributions on Disk** section shows where a specific partition resides. It also shows the disk type and size.

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

[Table 3-10](#) lists the operations that can be performed, on a partition, using the NetBackup Appliance Shell Menu and the NetBackup Appliance Web Console.

Table 3-10 Operations to manage the appliance storage partitions

Operation	Description	Partition
Resize	<p>Creates, resizes, or deletes a selected partition. Review the following considerations:</p> <ul style="list-style-type: none"> You can create a partition using Resize only if the Appliance is configured as a master or a media server. You can resize a partition to a higher or lower value depending on the type of partition. The size is expanded by using the unallocated space. You can delete a partition using Resize only if the Appliance is in a factory state (when it is not configured as a master server or a media server). <p>See "Resizing a partition" on page 76.</p> <p>See "Resize dialog" on page 78.</p>	<ul style="list-style-type: none"> AdvancedDisk Configuration MSDP Share (NetBackup Appliance Shell Menu only) MSDP Catalog NetBackup Catalog
Move	<p>Moves the selected partition from a source disk to the destination disk.</p> <p>See "Moving a partition" on page 80.</p>	<ul style="list-style-type: none"> AdvancedDisk Configuration MSDP Share (NetBackup Appliance Shell Menu only) MSDP Catalog <p>Note: The NetBackup Catalog partition cannot be moved.</p> <p>Note: On a 5330 appliance, the MSDP Catalog partition exists on its own metadisk and can only be moved between metadisks (if applicable).</p>

Resizing a partition

A partition can be resized to a higher or lower value. You can also create or delete a partition by resizing a partition.

You can create data partitions like AdvancedDisk or MSDP using Resize only if the Appliance is configured as a master server or a media server.

When you create an MSDP partition, a backup policy to protect the MSDP Catalog is automatically created.

You can delete a partition using Resize only if the Appliance is in a factory state (when it is not configured as a master server or a media server).

Note: You cannot delete Configuration or NetBackup Catalog partitions even if the Appliance is in a factory state.

Note: A share partition cannot be created or deleted using the Resize command.

Review the following points before you resize a storage partition:

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

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Manage > Storage** .
- 3 In the **Partitions** section, click the partition that you want to resize. The partition details page opens.
- 4 In the **Partition Distributions on Disk** section, click **Resize**.

- 5 Enter appropriate values for the parameters on the **Resize <partition>** dialog. Click **Resize** to resize the partition.
See “[Resize dialog](#)” on page 78.
- 6 The progress details are displayed when you resize a partition.
Click **OK** once the operation is complete. The partition details page is automatically refreshed.

Resize dialog

Review the following points before you resize a storage partition:

- The AdvancedDisk, Configuration, NetBackup Catalog, MSDP, and the MSDP Catalog partitions can be resized to a higher or a lower value. To resize, enter values in increments of 1 GB.
- Each partition has a minimum and maximum supported size. Ensure that you resize a partition within these values.

The following parameters are displayed on the **Resize** dialog:

Parameter	Description
Used Size	The Used Size is displayed when you resize AdvancedDisk, Configuration, MSDP, MSDP Catalog, and the NetBackup Catalog partitions. For these partitions, you cannot enter a value that is lower than the Used Size of the partition.
Unallocated Size	Displays the available space on the appliance.
Current Size	Displays the total size of the partition.
Storage Unit Name	<p>The storage unit name appears only if you create AdvancedDisk or MSDP partition (Current Size is 0). You can assign a different storage unit name, other than the default.</p> <p>The storage unit name can contain any letters, numbers, or special characters. The name can include up to 256 characters.</p> <p>Note: The name should not start with the minus (-) character and spaces should not be used anywhere in the name.</p>

Parameter	Description
Disk Pool Name	<p>The Disk Pool Name appears only if you create AdvancedDisk or MSDP partition (Current Size is 0). You can assign a different disk pool name, other than the default.</p> <p>The disk pool name can contain any letters, numbers, or special characters. The name can include up to 256 characters.</p> <p>Note: The name should not start with the minus (-) character and spaces should not be used anywhere in the name.</p>
New Size	<p>Enter a value in the text box and select the appropriate unit. You can also drag the slider to the new size. (in GB, TB, or PB). You can also click on the bar up to the new size.</p> <p>Only an absolute value is supported if the unit is GB. Absolute and decimal values are supported if the units are TB or PB.</p> <p>The maximum value on the slider displays the partition size that you can scale up to. For AdvancedDisk and MSDP partitions, the maximum value is the sum of Current Size and Unallocated Size.</p> <p>For other partitions like Configuration and NetBackup Catalog, the maximum value on the slider is the lower value when you compare the following values:</p> <ul style="list-style-type: none"> ■ Sum of Current Size and Unallocated Size ■ Maximum supported size of the partition <p>For example, consider a NetBackup Catalog partition with a Current size of 300 GB and an Unallocated Size of 6 GB. The maximum supported size for a NetBackup Catalog partition is 4 TB. Since the maximum supported size for NetBackup Catalog (4 TB) is greater than 306 GB (Current Size (300 GB) + Unallocated Size (6 GB)), the Maximum Size is displayed as 306 GB.</p>

Troubleshooting resize-related issues

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

[Error] Failed to resize the 'MSDP' partition '2' because the partition is either fragmented or busy. Retrying the operation after sometime may resolve the issue. Contact Symantec Technical Support if the issue persists.

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 Symantec Technical Support for further assistance.

Moving a partition

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

Note: The NetBackup Catalog partition cannot be moved. The NetBackup Catalog partition must always be present on the base unit of a 52xx appliance.

On a 5330 appliance, the MSDP Catalog partition must always be present on the Metadisk and can only be moved between Metadisks (wherever applicable).

To move a partition

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Manage > Storage**.
- 3 In the **Partitions** section, click the partition that you want to move. The partition details page opens.
- 4 In the **Partition Distributions on Disk** section, click **Move**.
See [“Move <partition> dialog”](#) on page 80.
- 5 Click **Move** to move the partition.

Note: The partition size and the workload on the system determines the time taken to move a partition.

- 6 The Move dialog displays the progress details and status of the move operation.
Click **OK** once the operation is complete. The partition details page is automatically refreshed.

Move <partition> dialog

The Move <Partition Name> window displays the following parameters:

Parameter	Description	Example
Source Disk	Displays the name of disk that currently holds the selected partition.	76YTG2BA7CBACB4F416D631CE (Base)
Partition Size	Displays the selected partition's size on the source disk.	300 GB

Parameter	Description	Example
Target Disk	Click the drop-down list and select the target disk to which you want to move the partition. Note: The Target disk must be different from the Source disk.	9DB0FD2BA7CBACB4F416D631CE (Expansion)
Unallocated Size	Displays the unallocated size on the target device.	100 GB
Size	Type the storage size in GB, TB, or PB that you want to move from the current disk to the new disk. Note: It is an optional field. If the size is not specified, the appliance moves the entire partition. Note: The size to be moved cannot be greater than the Unallocated Size on the target disk.	35 GB

Moving the MSDP partition from a base disk to an expansion disk for optimum performance

If all or a part of your Media Server Deduplication Pool (MSDP) partition resides on the appliance base unit (base disk), it is recommended that you move the MSDP partition to an expansion disk. This recommendation applies to 5220 and 5230 appliances and is needed for optimum performance.

The following procedures explain how to move the MSDP partition from a base disk to an expansion disk. The base disk resides on the appliance base unit. The expansion disk resides on a storage shelf that is attached to the appliance. A 5220 or a 5230 appliance can have up to two expansion disks.

Consider the following scenarios:

- Scenario 1 - The MSDP and AdvancedDisk partitions are configured on the base disk. The expansion units are physically attached to the appliance but have not been added yet.
- Scenario 2 - The MSDP partition exists on the base disk. The expansion units are configured and partitions exist on them.

Select the scenario that applies to you and follow the appropriate procedure outlined below.

Scenario 1 - To move the MSDP partition from a base disk to an expansion disk

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Manage > Storage** and go to **Disks** section. Check the partitions that are on the Base disk. Suppose that you have MSDP, AdvancedDisk, Catalog, and Configuration partitions on the base disk as shown below.
- 3 Ensure that the base disk is fully allocated by resizing the non-MSDP partitions (like AdvancedDisk). To ensure that the base disk is full, resize the AdvancedDisk partition to a value that is just below the maximum value displayed in the slider.

In the **Partitions** section, click **AdvancedDisk** partition to open the partition details page. On the partition details page, click **Resize** in the **Partition Distributions on Disk** section. Enter a size in the **New Size** field that is slightly below the maximum value.

Click **Resize** to resize.

Click **OK** after the resize operation is complete. The page is refreshed automatically and reflects the updated size.

- 4 In the **Disks** section, click the **Add** link next to the expansion unit. Click **Yes** to confirm the addition and **OK** when it finishes. Repeat this process for the second expansion unit.

Note that the Unallocated space increases.

- 5 Check the space occupied by MSDP partition.

In the **Partitions** section, click the **MSDP** link to open the MSDP partition details page. Check the **Partition Distributions on Disk** section.

Note that the expansion disk must have at least 260 GB of unallocated space when you move the MSDP partition to the expansion disk at a later point.

- 6 On the MSDP partition details page, click **Resize** in the **Partition Distributions on Disk** section. Enter a value that is slightly below the Unallocated Size. Ensure that the Unallocated size that remains must be more than the MSDP size on the base disk.

Click **Resize** to resize.

Click **OK** after the resize operation is complete. The page is refreshed automatically and reflects the updated size.

- 7 Check how the MSDP partition is distributed across disks.

On the MSDP partition details page, check the **Partition Distributions on Disk** section. In this example, a part of the MSDP partition resides on the base disk.

- 8 Click **Move** in the **Partition Distributions on Disk** section.
- 9 Move the MSDP partition from the base disk to the expansion disk.
In the **Move <MSDP>** window, select the expansion disk that has enough Unallocated size as the Target disk.
- 10 Click **Move** to move the partition.

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

- 11 The **Move** dialog displays the progress details and status of the move operation. Click **OK** once the operation is complete. The MSDP partition details page is automatically refreshed.
- 12 On the MSDP partition details page, check the **Partition Distributions on Disk** section. The MSDP partition resides on the expansion disks.

The following procedure explains how to move the MSDP partition from a base disk to an expansion disk when the expansion disk has partitions configured on it.

Scenario 2 - To move the MSDP partition from a base disk to an expansion disk

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Manage > Storage** and go to **Partitions** section.
- 3 Check if the MSDP partition is located on the base disk.
In the **Partitions** section, click **MSDP** partition to open the MSDP partition details page.

- 4 On the MSDP partition details page, check the **Partition Distributions on Disk** section.

If the **Type** is Base for any of the disks, all or a part of the MSDP partition resides on the base disk. In this example, the MSDP partition is located on the base disk as well as the Expansion disk.

If the **type** is Expansion for all the disks, the MSDP partition doesn't exist on the base disk. In this case, you do not need to move the MSDP partition. You can ignore the rest of the procedure.

- 5 Click **Move** in the **Partition Distributions on Disk** section.
- 6 On the **Move <MSDP>** window, click the drop-down list and select the target disk to which you want to move the partition. The target disk must be an expansion disk.

- 7 Click **Move** to move the partition.

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

- 8 The **Move** dialog displays the progress details and status of the move operation. Click **OK** once the operation is complete. The MSDP partition details page is automatically refreshed.

Scanning storage devices from the NetBackup Appliance Web Console

The following procedure describes how to scan the connected storage devices from **Manage > Storage > Disks**. Whenever a storage device is connected, use **Scan** to detect the storage device or refresh its status. If the `Scan` does not display the updated storage device information, then restart the appliance to refresh the storage device information.

Note: If you want to expand storage and attach a Storage Shelf or an expansion system to an appliance, see the *Symantec NetBackup Appliance Hardware Installation Guide* for the appropriate platform. Once these Storage Shelves or expansion systems are properly connected to the Appliance, you must scan the devices from the **Disks** section. Once the newly available disks are displayed, these disks must be added so the additional space can be used. The new disks have the **New Available** status.

To scan storage devices from the NetBackup Appliance Web Console

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Manage > Storage > Disks**.
- 3 Click **Scan**.

- 4 You are prompted for confirmation. Click **Yes** to confirm. The scan starts.

Note: If you are scanning the 5330 appliance for the first time, disk initialization may take some time. The disk initialization happens in the background and may take up to 56 hours depending on the system load. The estimated time is up to 28 hours for a Primary Storage Shelf and up to 28 hours for an Expansion Storage Shelf. You can continue to use the appliance during this time. However, if one or more of the new disks are used by partitions during the disk initialization process, the performance of backup and restore operations on the specific disks degrades by up to 30%

- 5 When the scan is complete, click **OK**. The **Disks** section refreshes automatically. If a new storage shelf is detected on a 52xx appliance, a new disk ID appears in the **Disks** section.

For 52xx appliances, the new entry should have the following attributes:

- Type = Expansion
- Status = New Available

For 5330 appliances, 6 Data disks and 1 Meta disk are displayed for a Primary Storage Shelf or an Expansion Storage Shelf. For a 5330 appliance that has a Primary Storage Shelf and an Expansion Storage Shelf, 12 Data disks and 2 Metadisks appear in the **Disks** section. The status for these disks is New Available.

You can now add this disk to the Unallocated space.

See [“Adding the storage space from a newly available disk”](#) on page 85.

Adding the storage space from a newly available disk

The following procedure describes how to add space from a newly available disk into the unallocated space.

If you want to attach a Storage Shelf or an expansion system to an appliance, see the *Symantec NetBackup Appliance Hardware Installation Guide* for the appropriate platform. Once these Storage Shelves are properly connected to the Appliance, you must scan for the newly available disks from the **Disks** section. The new disks have the **New Available** status. Once the newly available disks are displayed, these disks must be added so the additional space can be used.

To add the storage space from a newly available disk

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Manage > Storage** and go to the **Disks** section

- 3 The **Disks** section displays all the disks. Only disks that have the **Status** as **New Available** can be added. The **Add** link is displayed next to such disks.

Note: If the disk status is **Foreign**, click **Remove** so that data is removed and the disk status becomes **New Available**. Contact Symantec Support if you want to recover this data.

- 4 Click **Add** to add the disk.

A dialog box displays the following message:

This operation will add the disk to the Unallocated storage. Do you want to continue?

Click **Yes**.

- 5 The system displays the following message:

```
Adding disk <disk ID>
Succeeded.
```

Click **OK** to exit. The Manage > Storage > Disks page is automatically refreshed.

When you add the disk, the appliance updates its **Status** to **In Use**. This change is also reflected in the **Partitions** section. The **Unallocated** space is increased and the additional storage space is displayed in the **Partitions** graph and table.

Removing an existing storage disk

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

Note: Ensure that you move all the partitions from the disk to other disks, before removing a disk with status **In Use**. You can view the partitions on each disk from the **Allocations** column in **Manage > Storage > Disks**.

Note: You can use the beacon feature to identify the expansion disk, while disconnecting it. You can also use the beacon feature to identify the base disk.

To remove an existing disk

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Go to **Manage > Storage > Disks**.

- 3 The **Status** column in the **Disks** table displays the **Remove** link. It appears for disks with status **In Use** that do not contain any partitions. It also appears for disks with status **Foreign**.

Note: If a disk with status **In Use** has partitions and you want to remove it, you must first move the partition to other disks. You can view the partitions on each disk from the **Allocations** column in **Manage > Storage > Disks**.

- 4 Click the **Remove** link, to remove the disk.

A dialog box displays the following message:

This operation will remove the disk <disk ID>. Do you want to continue?

Click **Yes** to continue.

If you remove a disk with status **Foreign** that has data, the following message is displayed:

This operation will remove the disk <disk ID>. Any backup data present in the <disk ID> disk will be deleted. Do you want to continue?

Click **Yes** to continue.

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

- 5 The system displays the following message:

```
Removing disk <disk ID>  
Succeeded.
```

Click **OK** to exit. The **Manage > Storage > Disks** page is automatically refreshed.

When you remove the disk, the appliance updates the **Status** of this disk to **New Available**. This change is also reflected in the **Partitions** section. The **Unallocated** space is decreased and displayed accordingly in the **Partitions** graph and table.

Note: When you physically attach or disconnect a storage shelf from the 5220 appliance, you must update the boot order, reboot the storage shelf, and finally reboot your appliance. Also, if you disconnect one of the two connected storage shelves, you need to reboot the appliance.

Warning: After physically disconnecting a storage shelf, if the 5220 appliance reboots it can hang and display the Symantec **Boot splash** screen. Press the `ESC` key to proceed. The RAID controller firmware provides step-by-step instructions to help you boot the appliance.

Monitoring the progress of storage manipulation tasks

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

To monitor storage tasks

- 1 Log on to the NetBackup Appliance Shell Menu.
- 2 Go to the `Manage > Storage` menu by using the following command:

```
Main > Manage > Storage
```

- 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)
```

Scanning storage devices using the NetBackup Appliance Shell Menu

The following procedure describes how to scan the connected storage devices to your appliance, through the NetBackup Appliance Shell Menu. You can also scan storage devices from **Manage > Storage > Disks**.

Note: Whenever a storage device is connected or disconnected, use this command to detect the storage device or refresh its status. If the `scan` command does not display the updated storage device information, then restart the appliance to refresh the storage device information.

To scan the storage devices connected to your appliance

- 1 Log on to the NetBackup Appliance Shell Menu.
- 2 Go to the `Manage > Storage` menu by using the following command:

```
Main > Manage > Storage
```

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

- 3 Enter the `Scan` command to scan the storage devices.

For 52xx appliances, the connected devices are scanned and the following output is displayed:

```
Storage> Scan
- [Info] Refreshing the storage devices...
- [Info] Succeeded.
```

NOTE: If you run the 'Manage->Storage->Show Disk' command and the device run the 'Manage->Storage->Scan' command to import and refresh the device appear, restart the appliance to refresh the device information.

For 5330 appliances, the connected devices are scanned and the following output may be displayed:

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

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

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

About Copilot functionality and share management

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.

To configure Copilot functionality, the following steps need to be completed:

- Create a share on the appliance using the NetBackup Appliance Shell Menu.
- Mount the appliance share on the Oracle server.
- Configure a Storage Lifecycle Policy (SLP) and Oracle Intelligent Policy (OIP) using NetBackup.

Refer to the *NetBackup Copilot for Oracle Configuration Guide* for the entire configuration process.

Share partitions can be created, modified, viewed, and deleted through the use of the NetBackup Appliance Shell Menu. Use the following topics as a guide to managing your share partitions.

- See [“Creating a share from the NetBackup Appliance Shell Menu”](#) on page 92.
- See [“Viewing share information from the NetBackup Appliance Shell Menu”](#) on page 94.
- See [“Editing a share from the NetBackup Appliance Shell Menu”](#) on page 96.
- See [“Resizing a share from the NetBackup Appliance Shell Menu”](#) on page 99.
- See [“Moving a share from the NetBackup Appliance Shell Menu”](#) on page 100.
- See [“Deleting a share from the NetBackup Appliance Shell Menu”](#) on page 101.

Refer to the *NetBackup Appliance Commands Reference Guide* for more specific details about each command.

Refer to the *NetBackup™ for Oracle Administrator's Guide* for more information on Copilot in NetBackup software.

Creating a share from the NetBackup Appliance Shell Menu

The following procedure explains how to create a share from the NetBackup Appliance Shell Menu.

To create a new share from the NetBackup Appliance Shell Menu:

- 1 Open an SSH session to log on to the appliance as an administrator.
- 2 Enter `Main_Menu > Manage > Storage > Create Share`. 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`.
- 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 102.

8 Once you have entered the NFS export options, the following information is displayed:

```
- [Info] Summary:
      Name : share_1
      Description : Testing share_1
      Allocated Capacity : 5GB
      Clients :
                10.100.0.2(rw,no_root_squash)

>> Continue? ['yes', 'no']
```

9 Enter `yes` to continue.

The following information is displayed:

```
- [Info] Creating Share share_1
- [Info] 'Share' storage partition does not exist. Creating it now...
- [Info] The estimated time to create the 'Share' 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.
- [Info] Creating the 'Share' partition 'share_1'...
- [Info] Mounting the 'Share' partition 'share_1'...
- [Info] Exporting Share 'share_1' at mount point '/shares/share_1'
- [Info] Share share_1 created successfully
- [Info] NOTES:
```

Share exported at '10.132.1.237:/shares/share_1'.
Please create a mount point with this export path for all Database
Servers that need access to this Share.

See the NetBackup Appliance Administrator's guide for more detailed
mount instructions.

See [“About Copilot functionality and share management”](#) on page 91.

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.

Viewing share information from the NetBackup Appliance Shell Menu

The following procedure explains how to view share partition information using the NetBackup Appliance Shell Menu.

To view share partition information using the NetBackup Appliance 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`.

The following is an example output displaying share information:

```
Storage> Show Partition ALL share
```

Partition	Total	Available	Used	%Used	Status
Share	10 GB	9.89 GB	116.45 MB	2	Optimal

Share

Partition	Total	Available	Used	%Used	Status
share1	5 GB	4.94 GB	58.23 MB	2	Mounted
share2	5 GB	4.94 GB	58.23 MB	2	Mounted

Share - share1

Description:

test share

Clients | Options

10.80.100.12 | no_root_squash, rw, secure

Share - share2

Description:

test share 2

Clients | Options

10.80.112.14 | no_root_squash, rw, secure

Instructions to use a share:

On UNIX systems, a share can be mounted using `nb-appliance:/shares/<Name>`.

Refer to the *NetBackup Appliance Commands Reference Guide* for more specific details about the command.

See “[About Copilot functionality and share management](#)” on page 91.

See “[About viewing storage space information using the `show` command](#)” on page 102.

Editing a share from the NetBackup Appliance Shell Menu

Shares can be edited using the `Manage > Storage > Edit Share` command. You can edit the following details of the share:

- Share description
- Add, update, or delete clients.

The following procedure explains how to edit a share description from the NetBackup Appliance Shell Menu.

To edit a share description

- 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.

The following is an example output:

```
Manage > Storage > Edit Share Description share_1
- [Info] Old Description :
    test share
>> Enter a new short description: (None) new test share
- [Info] Summary:
    Name : share_1
    Description : new test share

>> Continue? ['yes', 'no'] yes
- [Info] Updating Share share_1
- [Info] Updating Share partition 'share_1'
- [Info] Share share_1 updated successfully
```

The following procedure explains how to add a client to a share from the NetBackup Appliance Shell Menu.

To add a client to a share

- 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.

The following is an example output:

```
Manage > Storage > Edit Share Clients Add share_1
- [Info] List of Oracle server clients that can access this share :
      10.80.40.110(rw,no_root_squash,secure)
>> Enter comma-separated list of Oracle server clients you would like to add: 10.80.40.111,10.80.40.112
- [Info] Enter the NFS export options for each of the Oracle clients
      The following options are supported:
      ro, rw, root_squash, no_root_squash, all_squash,
      anonuid=<uid-value>, anongid=<gid-value>, secure, insecure.
      For detailed information about the NFS export command options, refer to the
      NetBackup Appliance Administrator's guide.
>> Enter the export options for '10.80.40.111': (rw,no_root_squash,secure)
>> Enter the export options for '10.80.40.112': (rw,no_root_squash,secure)
- [Info] Summary:
      Name : share_1
      Clients :
      10.80.40.112(rw,no_root_squash,secure)
      10.80.40.111(rw,no_root_squash,secure)
      10.80.40.110(rw,no_root_squash,secure)

>> Continue? ['yes', 'no'] yes
- [Info] Updating Share share_1
- [Info] Updating Share partition 'share_1'
- [Info] Re-exporting Share 'share_1' at mount point '/shares/share_1'
- [Info] Share share_1 updated successfully
```

The following procedure explains how to update the clients of a share from the NetBackup Appliance Shell Menu.

To update the clients of a share

- 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.

The following is an example output:

```
Manage > Storage > Edit Share Clients Update share_1
- [Info] List of Oracle server clients that can access this share :
      10.80.40.112(rw,no_root_squash,secure)
      10.80.40.111(rw,no_root_squash,secure)
      10.80.40.110(rw,no_root_squash,secure)
>> Enter comma-separated list of Oracle server clients you would like to update: 10.80.40.112
- [Info] Enter the NFS export options for each of the Oracle clients
      The following options are supported:
      ro, rw, root_squash, no_root_squash, all_squash,
      anonuid=<uid-value>, anongid=<gid-value>, secure, insecure.
      For detailed information about the NFS export command options, refer to the
      NetBackup Appliance Administrator's guide.
>> Enter the export options for '10.80.40.112': (rw,no_root_squash,secure) rw
- [Info] Summary:
      Name : share_1
      Clients :
      10.80.40.112(rw)
      10.80.40.111(rw,no_root_squash,secure)
      10.80.40.110(rw,no_root_squash,secure)

>> Continue? ['yes', 'no'] yes
- [Info] Updating Share share_1
- [Info] Updating Share partition 'share_1'
- [Info] Re-exporting Share 'share_1' at mount point '/shares/share_1'
- [Info] Share share_1 updated successfully
```

The following procedure explains how to delete clients from a share from the NetBackup Appliance Shell Menu.

To delete clients from a share

- 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.

The following is an example output:

```
Manage > Storage > Edit Share Clients Delete share_1
- [Info] List of Oracle server clients that can access this share :
    10.80.40.112(rw)
    10.80.40.111(rw,no_root_squash,secure)
    10.80.40.110(rw,no_root_squash,secure)
>> Enter comma-separated list of Oracle server clients you would like to delete: 10.80.40.111
- [Info] Summary:
    Name : share_1
    Clients :
        10.80.40.112(rw)
        10.80.40.110(rw,no_root_squash,secure)

>> Continue? ['yes', 'no'] yes
- [Info] Updating Share share_1
- [Info] Updating Share partition 'share_1'
- [Info] Re-exporting Share 'share_1' at mount point '/shares/share_1'
- [Info] Share share_1 updated successfully
```

Refer to the *NetBackup Appliance Commands Reference Guide* for more specific details about the command.

See [“About Copilot functionality and share management”](#) on page 91.

Resizing a share from the NetBackup Appliance Shell Menu

Shares can be resized using the `Manage > Storage > Resize` command.

Note: Resizing a partition may take a significant amount of time depending on the load on the system and the amount of data present on the partition. In some cases, the operation may take up to a day depending on the fragmentation of the partition.

The following procedure explains how to resize a share from the NetBackup Appliance Shell Menu.

To resize a share

- 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.

The following is an example output:

```
Storage > Resize Share 1 TB share1
- [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 'Share' 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.
```

Refer to the *NetBackup Appliance Commands Reference Guide* for more specific details about the command.

See [“About Copilot functionality and share management”](#) on page 91.

Moving a share from the NetBackup Appliance Shell Menu

The following procedure explains how to move a share using the NetBackup Appliance Shell Menu.

To move a share using the NetBackup Appliance 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.

The following is an example output:

```
Storage > Move Share share_1 unit_1 unit_2 5 GB
- Moving the partition would approximately take 0 hours, 2 minutes.
  Do you want to continue? (yes/no)
Moving part '1/1' disk... Done
- Succeeded
```

Refer to the *NetBackup Appliance Commands Reference Guide* for more specific details about the command.

See [“About Copilot functionality and share management”](#) on page 91.

Deleting a share from the NetBackup Appliance Shell Menu

The following procedure explains how to delete a share using the NetBackup Appliance Shell Menu.

To delete a share using the NetBackup Appliance 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.

The following is an example output:

```
Manage > Storage > Delete Share share_2
>> Caution: Make sure all data has been backed up before deleting the Share.
Are you sure you want to delete Share 'share_2'? ['yes', 'no'] yes
- [Info] Deleting Share share_2
- [Info] Unexporting Share partition 'share_2' at mount point '/shares/share_2'
- [Info] Unmounting the 'Share' partition 'share_2'...
- [Info] Deleting the 'Share' partition 'share_2'...
- [Info] Share share_2 deleted successfully
```

Refer to the *NetBackup Appliance Commands Reference Guide* for more specific details about the command.

See [“About Copilot functionality and share management”](#) on page 91.

NFS export options

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).

See [“Creating a share from the NetBackup Appliance Shell Menu”](#) on page 92.

See [“About Copilot functionality and share management”](#) on page 91.

About viewing storage space information using the `Show` command

This section describes the `Show [Type]` commands and their usage in the NetBackup Appliance Shell Menu. These commands can be accessed from `Main_Menu > Manage > Storage`.

The `[Type]` parameter is required when using the `Show` command.

The following `Show [Type]` commands are described::

- `Show [ALL]` - to view Disk, Partition, and Distribution information together.
See [“Viewing all storage information”](#) on page 103.
- `Show [Disk]` - to view total capacity, unallocated storage capacity, and current status of a disk.
See [“Viewing disk information”](#) on page 106.
- `Show [Distribution]` - to view the distribution of partitions on a disk.
See [“Viewing the partition distribution on disks”](#) on page 111.

Note: The Available and Used Size values displayed for the MSDP partition on the **Manage > Storage > Partitions** page or by using the **Manage > Storage > Show** command on the NetBackup Appliance Shell Menu may not be the full space available or used by the MSDP partition. This is because space is reserved by the file system and also by MSDP. The file system reserves space for it's 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 displayed on the NetBackup Administration Console to know the MSDP statistics.

Viewing all storage information

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

To view all storage information

- 1 Log on to the NetBackup 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.

For a 5330 platform, the appliance displays the storage information as shown in the following example:

```
- [Info] Performing sanity check on disks and partitions... (5 mins approx)
```

```
-----
Disk ID                               | Type   | Total   | Unallocated | Status
-----
```

```
5E000000000000000000000000000000 | System | 930.39 GB | - | n/a
7A30D550001B22423721D79081 | Base | 13.64 TB | 10.84 TB | In Use
```

7A30D550001B22423721D79081 (Base)

```
-----
AdvancedDisk      :    500 GB
- 0               :    500 GB
Configuration     :    25 GB
- 0               :    25 GB
MSDP              :     1 TB
- 0               :     1 TB
MSDP Catalog      :    43 GB
- 0               :    43 GB
NetBackup Catalog :   250 GB
- 0               :   250 GB
Share             :     1 TB
- s1              :     1 TB
```

```
-----
Partition          | Total      | Available  | Used        | %Used | Status
-----
AdvancedDisk       |    500 GB | 495.81 GB | 4.19 GB | 1 | Optimal
Configuration      |    25 GB | 21.52 GB | 3.48 GB | 14 | Optimal
MSDP               |     1 TB | 1015.6 GB | 8.36 GB | 1 | Optimal
MSDP Catalog       |    43 GB | 42.59 GB | 414.99 MB | 1 | Optimal
NetBackup Catalog  |   250 GB | 247.62 GB | 2.38 GB | 1 | Optimal
Share              |     1 TB | 1015.6 GB | 8.34 GB | 1 | Optimal
Unallocated        |  10.84 TB | -         | -         | - | -
```

AdvancedDisk

```
-----
Partition | Total      | Available  | Used        | %Used | Status
-----
0         |    500 GB | 495.81 GB | 4.19 GB | 1 | Mounted
```

Configuration

```
-----
Partition | Total      | Available  | Used        | %Used | Status
-----
0         |    25 GB | 21.52 GB | 3.48 GB | 14 | Mounted
```

MSDP

```
-----
```


Partition	Total	Available	Used	%Used	Status
0	1 TB	1015.6 GB	8.36 GB	1	Mounted

MSDP Catalog

Partition	Total	Available	Used	%Used	Status
0	43 GB	42.59 GB	414.99 MB	1	Mounted

NetBackup Catalog

Partition	Total	Available	Used	%Used	Status
0	250 GB	247.62 GB	2.38 GB	1	Mounted

Share

Partition	Total	Available	Used	%Used	Status
s1	1 TB	1015.6 GB	8.34 GB	1	Mounted

AdvancedDisk

Disk Pool (DP) | Storage Unit (STU)

dp_adv_nbapp2br | stu_adv_nbapp2br

MSDP

Disk Pool (DP) | Storage Unit (STU)

dp_disk_nbapp2br | stu_disk_nbapp2br

Share - s1

Description:

None

Clients | Options

appesx30-vm13 | no_root_squash, rw, secure

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

The sizes that are displayed here for the MSDP partition are different from the MSDP disk pool sizes. See the NetBackup Appliance Administrator's Guide for more information.

Instructions to use a share:

On UNIX systems, a share can be mounted using `nbapp2br.engba.symantec.com:/shares/<Name>`.

Viewing disk information

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

To view disk information

- 1 Log on to the NetBackup 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:

```
Storage> Show Disk
- [Info] Performing sanity check on disks and partitions..(5 mins approx)
-----
Disk ID                               | Type   | Total |Unallocated|Status
-----
50001FD36800000796537BB10F|Operating|930.39 TB| -          | n/a
                               System
50001FD36800000790537BB0FA|Base     | 2.24 TB| 300 GB    | In Use
50001FEE6C00000A36537BB0CB|Expansion|4.5421 TB| 840.92 GB| In Use
```

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

```
Storage> Show Disk
- [Info] Performing sanity check on disks and partitions..(5 mins approx)
-----
Disk ID                               | Type   | Total |Unallocated|Status
-----
5E00000000000000000000000000|System  |930.39 TB| -          | n/a
50001FD36800000790537BB0FA|Base     | 2.24 TB| 300 GB    | In Use
50001FEE6C00000A36537BB0CB|Expansion|4.5421 TB| 840.92 GB| In Use
```

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

For a 5330 platform, the appliance displays the disk information as shown in the following example:

```
Storage> Show Disk
- [Info] Performing sanity check on disks and partitions..(5 mins approx)
-----
Disk ID                               |Type     | Total   |Unallocated| Status
-----
5E00000000000000000000000000|System   | 2.73 TB | -          | n/a
5E00000000000000000000000000|System   | 2.73 TB | -          | n/a
50001FD36800000796537BB10F|Meta     | 5.46 TB | 5.46 TB   | In Use
50001FEE6C00000A38537BB0D5|Meta     | 5.46 TB | 5.37 TB   | In Use
50001FD3680000078A537BB0DC|Data     | 19.10 TB|19.10 TB   | In Use
50001FD3680000078C537BB0E4|Data     | 19.10 TB|19.10 TB   | In Use
50001FD3680000078E537BB0EC|Data     | 19.10 TB| 0 GB      | In Use
50001FD36800000790537BB0FA|Data     | 19.10 TB| 7.30 TB   | In Use
50001FD36800000792537BB102|Data     | 19.10 TB|19.08 TB   | In Use
50001FD36800000794537BB10B|Data     | 19.10 TB| 0 GB      | In Use
```

```
50001FEE6C000000A32537BB0B4|Data | 19.10 TB |19.10 TB | In Use
50001FEE6C000000A34537BB0C3|Data | 19.10 TB |19.10 TB | In Use
50001FEE6C000000A36537BB0CB|Data | 19.10 TB |18.20 TB | In Use
50001FEE6C000000A3A537BB0D8|Data | 19.10 TB | 0 GB | In Use
50001FEE6C000000A3C537BB0E1|Data | 19.10 TB |19.10 TB | In Use
50001FEE6C000000A3E537BB0EA|Data | 19.10 TB |19.10 TB | In Use
```

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

[Table 3-11](#) lists the disk types that can appear depending on your Appliance platform.

Table 3-11 Disk Type

Type	Description	Supported Platforms
System	This category tells you the storage that is occupied by the Appliance operating system, logs etc.	5200, 5220, 5230 5330
Base	This category tells you the storage that is available with the Appliance base unit.	5200, 5220, 5230
Expansion	A storage shelf that is connected to a 5220 or a 5230 appliance appears as a single expansion disk.	5220, 5230
Data	All partitions, except MSDP Catalog, exist on the 5330 Data disk. Examples of partitions that exist on the data disks are MSDP, AdvancedDisk, Configuration etc. There can be six data disks for a Primary Storage Shelf and six for an Expansion Storage Shelf.	5330
Meta	The MSDP Catalog partition exists only on the Meta disk. There can be one Meta disk for a Primary Storage Shelf and one for an Expansion Storage Shelf.	5330
Unknown	This category appears when appliance cannot determine the disk type like when the disk is not accessible.	Not Applicable

Viewing partition information

The `Show Partition` command includes a few different options to view the storage information on the appliance. Options include:

- `All [PartitionType]`
- `Configuration [PartitionType]`
- `Usage [PartitionType]`

Replace `[PartitionType]` with `AdvancedDisk`, `All`, `MSDP`, or `Share`.

The following procedure describes how to use the `Show Partition Configuration` command to view configuration information for a share, using the NetBackup Appliance Shell Menu:

To view partition configuration for a share

- 1 Log on to the NetBackup 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 Partition Configuration Share` command to view the partition information for a share.
- 4 For 52xx platforms, the appliance displays the partition information as shown in the following example:

```
- [Info] Performing sanity check on disks and partitions... (5 mins approx)
Share - s1
```

```
-----
Description:
  None
-----
Clients      | Options
-----
appesx30-vm13 | no_root_squash, rw, secure
-----
```

Instructions to use a share:

On UNIX systems, a share can be mounted using `nbapp2br.engba.symantec.com:/shares/<Name>`.

Viewing the partition distribution on disks

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

To view the partition distribution on a disk

- 1 Log on to the NetBackup 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 following example displays the initiated procedure when you run the `Show [Distribution]` command on a 5330 appliance:

```
Show Distribution
5000294D6C0000214253716C3C (Data)
-----
Configuration      :      25 GB
- 0                :      25 GB

5000294D6C0000214553716C47 (Data)
-----
MSDP               :    19.10 TB
- 3                :    19.10 TB

5000294D6C0000214853716C4E (Data)
-----
AdvancedDisk       :    19.10 TB
- 1                :    19.10 TB

5000294D6C0000214B53716C54 (Meta)
-----
MSDP Catalog       :     5.46 TB
- 0                :     5.46 TB

5000294D6C0000214E53716C59 (Data)
-----
AdvancedDisk       :     1.80 TB
- 2                :     1.80 TB

5000294D6C0000215453716C68 (Data)
-----
MSDP               :    19.10 TB
- 0                :    19.10 TB

5000294D8000001E0741ECBEBD (Data)
-----
MSDP               :    19.10 TB
- 2                :    19.10 TB

5000294D8000001E0A41ECBEC3 (Data)
-----
```

```
MSDP          :    3.60 TB
- 4           :    3.60 TB

5000294D8000001E1341ECBEDE (Data)
-----
MSDP          :   19.10 TB
- 1           :   19.10 TB
```

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.

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 alerts 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

About appliance supported tape devices

The following describes the tape device support for the NetBackup appliance:

Tape library	<p>The NetBackup appliance supports backup to the tape libraries that are of NetBackup type TLD (tape library DLT). DLT is an acronym for digital linear tape.</p> <p>For the TLD types that NetBackup supports, see the Hardware Compatibility List at the following URL:</p> <p>www.netbackup.com/compatibility</p>
Tape drives	<p>The NetBackup appliance supports writing to the tape devices that are capable of SCSI T10 encryption to ensure that the tape media that is moved off-site is secure. Tape encryption requires configuration of the NetBackup Key Management Service (KMS) feature. To know more about KMS support and the list of the tape drives supported with KMS, see the Hardware Compatibility List at the following URL:</p> <p>www.netbackup.com/compatibility</p>
Tape usage	<p>Tapes with the barcode prefix of CLN are treated as cleaning tapes.</p> <p>Tapes with any other barcode prefix are treated as normal tapes.</p>
NetBackup ACS libraries	<p>Starting with appliance version 2.5, NetBackup appliances support the NetBackup type ACS libraries and the configuration of NetBackup ACS robotics on the NetBackup appliance. Appliance administrators can change the ACS entries in the <code>vm.conf</code> file on the local appliance.</p> <p>For complete details about the ACS commands that can be used to modify the <code>vm.conf</code> file, see the <i>Symantec NetBackup Appliance Command Reference Guide</i>.</p>

See [“Adding external robots to the NetBackup appliance”](#) on page 115.

Adding external robots to the NetBackup appliance

After the Fibre Channel HBA card has been installed, you can add external robots to the appliance.

Use the following procedure to add robots to the appliance.

To add an external robot to the appliance

- 1 Set any physical address switches to the appropriate setting as described in the instructions from the vendor.
- 2 Connect the robot to the HBA card as described in the instructions from the vendor.
- 3 Install and configure the robot software so that the robot works with the operating system, as described in the instructions from the vendor. The operating system must be able to recognize the robot before you can configure it to work with the appliance. (This is an optional step.)
- 4 Configure the added robot for backups as follows:

For NetBackup 52xx media server appliances:	Use the NetBackup Administration Console. See to "Configuring robots and drives" in the <i>NetBackup Administrator's Guide, Volume I</i> .
---	---

See ["About appliance supported tape devices"](#) on page 115.

About configuring Host parameters for your appliance

The **Settings > Host** menu enables you to view and edit the following NetBackup settings for your appliance:

- Specify Data Buffer parameters
See ["Configuring data buffer parameters"](#) on page 118.
- Specify Lifecycle parameters
See ["Configuring lifecycle parameters"](#) on page 122.
- Specify Deduplication parameters
See ["Configuring deduplication parameters"](#) on page 124.
- Enable or disable BMR as a server recovery option
See ["About BMR integration"](#) on page 125.

Manage > Host > Data Buffer options

You can configure the parameters for the data buffer shared with NetBackup using the **Manage > Host > Data Buffer** tab in the appliance NetBackup Appliance Web Console. The **Data Buffer Parameters** tab enables you to enter the count 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 NetBackup Appliance Web Console:

Table 3-12 Data Buffer parameters

Fields	Description for the Count field
Data buffer tapes - Count	Enter the total number of shared data buffer tapes used by NetBackup. The default value is 30.
Data buffer tapes - Size	Enter the size of each shared data buffer tape in Bytes. The default value is 262144 Bytes.
Data buffer on disks - Count	Enter the number of shared data buffer disks used by NetBackup. The default value is 30.
Data buffer on disks - Size	Enter the size of each shared data buffer disks in Bytes. The default value is 262144 Bytes.
Data buffer FT - Count	Enter the number of shared data buffer FT storage used by NetBackup. The default value is 16.
Data buffer FT - Size	Enter the size of each shared data buffer FT storage in Bytes. The default value is 262144 Bytes.
Data buffer restore - Count	Enter the number of shared data buffer restore storage used by NetBackup. The default value is 30.
Data buffer NDMP - size	Enter 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	Enter the size of each shared data buffer storage restored in Bytes. The default value is 262144 Bytes.

You can view and change the data buffer parameters using this tab.

Configuring data buffer parameters

You can set the data buffer parameters using the **Manage > Host** menu in the NetBackup Appliance Web Console. The **Host** menu displays the **Data Buffer** tab. You can view and change the data buffer parameters using this tab. The following procedure describes how to view and update your data buffer parameters using the NetBackup Appliance Web Console.

You can also update these parameters using the appliance shell menu. For details, see the *Symantec NetBackup 52xx Series Command Reference Guide*.

To configure data buffer parameters

- 1 Log on to the NetBackup Appliance Web Console.

- 2 Select **Manage > Host > Data Buffer**.

The system displays the **Data Buffer** tab with the default NetBackup data buffer parameters.

- 3 Enter the data buffer parameters in the provided fields. A description of the data buffer parameters is available.

See [“Manage > Host > Data Buffer options”](#) on page 116.

- 4 Click **Save**, to save the updated parameters.

Manage > Host > Lifecycle options

You can set the lifecycle parameters using the **Manage > Host** menu in the NetBackup Appliance Web Console. The **Host** page displays the **Lifecycle** tab. You can view and change the lifecycle parameters using this tab.

[Table 3-13](#) describes the lifecycle parameters that are displayed.

Table 3-13 Lifecycle parameters

Field	Description
Cleanup session interval	<p>Enter the time interval after which the deleted life cycle policies should be cleaned up. The default value is 24 .hours.</p> <p>Select the unit to measure the time from the drop-down list. You can select from the following options:</p> <ul style="list-style-type: none"> ■ Hour(s) ■ Second(s) ■ Minute(s) ■ Day(s) ■ Week(s) ■ Month(s) ■ Year(s)
Duplication group criteria	<p>Enter the duplication group criteria that is used to define how batches are created. The default value is 1.</p>
Image extended retry period	<p>Enter the interval period till NetBackup waits before an image copy is added to the next duplication job. The default value is 2 hours.</p> <p>Select the unit to measure the time from the drop-down list. You can select from the following options:</p> <ul style="list-style-type: none"> ■ Hour(s) ■ Second(s) ■ Minute(s) ■ Day(s) ■ Week(s) ■ Month(s) ■ Year(s)

Table 3-13 Lifecycle parameters (*continued*)

Field	Description
Job submission interval	<p>Set the frequency of job submission for all operations. The default value is 5 minutes.</p> <p>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.</p> <p>Select the unit to measure the time from the drop-down list. You can select from the following options:</p> <ul style="list-style-type: none"> ■ Hour(s) ■ Second(s) ■ Minute(s) ■ Day(s) ■ Week(s) ■ Month(s) ■ Year(s)
Max size per duplication job	<p>Enter the maximum size up to which the batch of images is allowed to grow. The default value is 100 GB.</p> <p>Select the unit to measure the size from the drop-down list. You can select from the following options:</p> <ul style="list-style-type: none"> ■ Byte(s) ■ KB ■ MB ■ GB ■ TB ■ PB
Force interval for small jobs	<p>Enter 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.</p> <p>Select the unit to measure the time from the drop-down list. You can select from the following options:</p> <ul style="list-style-type: none"> ■ Hour(s) ■ Second(s) ■ Minute(s) ■ Day(s) ■ Week(s) ■ Month(s) ■ Year(s)

Table 3-13 Lifecycle parameters (*continued*)

Field	Description
Min size per duplication job	<p>Enter 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.</p> <p>Select the unit to measure the size from the drop-down list. You can select from the following options:</p> <ul style="list-style-type: none"> ■ Byte(s) ■ KB ■ MB ■ GB ■ TB ■ PB
Replica metadata cleanup timer	<p>Enter the number of days after which the Import Manager stops trying to import the image. The default value is 0 hours.</p> <p>Select the unit to measure the time from the drop-down list. You can select from the following options:</p> <ul style="list-style-type: none"> ■ Hour(s) ■ Second(s) ■ Minute(s) ■ Day(s) ■ Week(s) ■ Month(s) ■ Year(s)
Tape resource multiplier	<p>Enter the multiplier for the number of concurrently active duplication jobs that can access a single storage unit. The default value is 2.</p>
Version cleanup delay	<p>Enter 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.</p> <p>Select the unit to measure the time from the drop-down list. You can select from the following options:</p> <ul style="list-style-type: none"> ■ Hour(s) ■ Second(s) ■ Minute(s) ■ Day(s) ■ Week(s) ■ Month(s) ■ Year(s)

Note: The **Import Extended Retry Session Timer**, **Import Session Timer**, and **Duplication Session Interval** parameters have been removed in Appliance 2.6. A new parameter named **Job Submission Interval** has been introduced.

Configuring lifecycle parameters

You can set the lifecycle parameters using the **Manage > Host** menu in the NetBackup Appliance Web Console. The **Host** menu displays the **Lifecycle** tab. You can view and change the lifecycle parameters using this tab. The following procedure describes how to view and update your lifecycle parameters using the NetBackup Appliance Web Console.

You can also update these parameters using the appliance shell menu. For details, see the *Symantec NetBackup 52xx Series Command Reference Guide*.

To configure lifecycle parameters

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Select **Manage > Host > Lifecycle**.

The system displays the **Lifecycle** tab with the default lifecycle parameters. A description of the lifecycle parameters is available.

See [“Manage > Host > Lifecycle options”](#) on page 118.

- 3 Click **Save** to save the updated parameters.

About configuring deduplication solutions

Symantec NetBackup appliance is available with two types of storage solutions. Based on the type of Symantec NetBackup hardware appliance you can choose from the following two types of deduplication solutions:

Table 3-14 Deduplication solutions and appliance matrix

Symantec NetBackup Appliance Series	Deduplication solution applicable	
	Master Server	Media server
Symantec NetBackup Appliance 5220 Series	Media Server Deduplication Option (MSDP)	Media Server Deduplication Option (MSDP)
Symantec NetBackup Appliance 5230 Series	Media Server Deduplication Option (MSDP)	Media Server Deduplication Option (MSDP)

Adding the Deduplication solution to a 5230 media appliance

You can configure the deduplication solution for your Symantec NetBackup Appliance 5230 Series media appliance using the following two pages:

- **Initial Configuration** - You can select the deduplication solution at the time of initial configuration of your appliance.
- **Manage > Storage > Resize** - If you have not configured a deduplication solution at the time of initial configuration you can configure it using the **Resize** option from the **Manage > Storage** menu. For more information, refer to See [“Resizing a partition”](#) on page 76.

Manage > Host > Deduplication

You can set the Media Server deduplication parameters using the **Manage > Host > Deduplication** menu in the NetBackup Appliance Web Console. The **Host** page displays the **Deduplication** tab. You can view and change the deduplication parameters using this tab.

[Manage > Host > Deduplication](#) describes the deduplication parameters that are displayed on the **Deduplication Settings** tab.

Table 3-15 Deduplication parameters

Fields	Description
Log verbosity level	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 Symantec representative.
Debug log file maximum size	Enter the maximum size of the log file in megabytes.
NICs for backup and restore	Enter the IP address or range of addresses of the local network Interface Card (NIC) for maintaining backups and restores.

Table 3-15 Deduplication parameters (*continued*)

Fields	Description
Maximum bandwidth	<p>Enter the maximum bandwidth that is allowed when backing up or restoring data between the media server and the deduplication pool.</p> <p>You cannot configure bandwidth throttling using the NetBackup Appliance Web Console. From the NetBackup Appliance Shell Menu use the Main_Menu > Settings > Deduplication > Tune view option to configure OPTDUP_BANDWIDTH . For more information, refer to the "Settings > Deduplication" topic in the <i>Symantec NetBackup Appliance Command Reference Guide</i>.</p>
Compression	Select to compress optimized duplication data. By default, the files are not compressed.
Encryption	Select the check-box to encrypt the data. By default, files are not encrypted. When you select the check-box the data is encrypted during transfer and on the storage.
Maximum image fragment size	<p>Enter the maximum backup image fragment size in megabytes.</p> <p>Note: Change this value only when directed to do so by a Symantec representative.</p>
Web services retry count	<p>Enter the number of retries that can be attempted in case the Web service fails out or times out.</p> <p>Note: This parameter applies to the PureDisk Deduplication Option only. It does not affect NetBackup deduplication.</p>
Web service call timeout	<p>Enter the parameter to increase or decrease the timeout value for Web service calls made from NetBackup media servers to PureDisk storage units.</p> <p>Note: This parameter applies to the PureDisk Deduplication Option only. It does not affect NetBackup deduplication.</p>
Use local pd.conf settings	Select the check-box to ignore the server settings and use local pd.conf settings. By default this check-box is not selected.
File segment exceptions	Enter the suffixes for log files. The files with these suffice will not be segmented.

Configuring deduplication parameters

You can set the deduplication parameters using the **Manage > Host** menu in the NetBackup Appliance Web Console. The **Host** menu displays the **Deduplication**

tab. You can view and change the MSDP parameters using this tab. The following procedure describes how to view and update your deduplication parameters using the NetBackup Appliance Web Console.

You can also update these parameters using the appliance shell menu. For details, see the *Symantec NetBackup 52xx Series Command Reference Guide*.

To configure deduplication parameters

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Select **Manage > Host > Deduplication**.
The system displays the **Deduplication** tab with the default deduplication parameters.
- 3 Enter the MSDP parameters. For more information about these parameters.
See [“Manage > Host > Deduplication”](#) on page 123.
- 4 Click **Save**, to save the updated parameters.

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.

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 appliance cannot be used as a BMR boot server. This convention is unlike NetBackup, where you can use any master 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 Appliance Web Console”](#) on page 126.

Manage > Host > Advanced options

You can now enable Bare Metal Restore (BMR) from **Manage > Host > Advanced** in the NetBackup Appliance Web Console when the appliance is configured as a master server. If you want to disable BMR on the appliance, you must run the appropriate NetBackup commands. Note that BMR is disabled by default.

The following option appears on Manage > Host > Advanced:

Enable BMR on this Appliance

You can enable BMR by using this option.

See [“Enabling BMR from the NetBackup Appliance Web Console”](#) on page 126.

You cannot enable or disable BMR from the appliance shell menu.

BMR configuration is not required when an appliance is configured as a media server. The **Manage > Host > Advanced** tab does not appear when the appliance is configured in a media server role.

Enabling BMR from the NetBackup Appliance Web Console

You can enable Bare Metal Restore (BMR) from **Manage > Hosts > Advanced** in the NetBackup Appliance Web Console when the appliance is configured as a master server.

If you want to disable BMR on the appliance, you must run the appropriate NetBackup commands. Note that BMR is disabled by default.

To enable BMR from the NetBackup Appliance Web Console

- 1 Log on to the NetBackup Appliance Web Console. Note that the appliance must be configured as a master server.
- 2 Select **Manage > Host > Advanced** tab.
- 3 Check **Enable BMR on this appliance** to enable BMR on the appliance.
- 4 Click **Save**.

Manage > Host > IPMI options

You can reset the IPMI from the **Manage > Host > IPMI** tab in the NetBackup Appliance Web Console. The IPMI must be reset only if the IPMI interface hangs or stops responding. The IPMI reset operation involves restarting the IPMI.

Refer to the following link for the procedure on how to reset the IPMI.

See [“Resetting the IPMI”](#) on page 127.

Note: You can also reset the IPMI from NetBackup Appliance Shell Menu by using the Support > IPMI Reset command. See the NetBackup Appliance Commands Guide for more details.

Resetting the IPMI

Use the following procedure to reset the IPMI. The IPMI must be reset only if the IPMI console hangs or stops responding.

To reset the IPMI

- 1 Log on to NetBackup Appliance Web Console.
- 2 Go to Manage > Host > IPMI.
- 3 Click **Reset IPMI**.
- 4 The following warning appears:

Resetting the IPMI disconnects all current IPMI users. Are you sure you want to reset the IPMI?

Click **Yes** to continue.
- 5 The IPMI is reset. Symantec recommends that you wait for 2 minutes and then attempt to reconnect to the IPMI console.
- 6 In case you cannot access the IPMI console, the appliance must be shut down and then restarted. Perform the following steps:
 - Schedule a convenient time for the appliance shutdown and alert all users.
 - Shut down the appliance.
 - Disconnect all appliance power cables.
 - Wait for 15 seconds and then reconnect the cables.
 - Turn on power to the appliance.

Manage > 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. Starting with v2.6, you can create a checkpoint, rollback the appliance to a checkpoint that you choose, or initiate a factory reset.

From this page, you can click one of the following buttons to begin the process that you want:

- **Create Appliance Checkpoint**

Click this icon to create a user-directed checkpoint on your appliance.

- **Appliance Rollback**

Click this icon to roll back the appliance to a checkpoint that you select.

- **Launch Appliance Factory Reset**

Click this icon to reset your appliance to its original default state.

The following list describes the four different types of checkpoints:

- A factory reset checkpoint. This checkpoint is created during the installation of each new appliance.
- 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 post-upgrade 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 or the appliance shell menu. If an existing user-directed checkpoint already exists it is replaced by any new checkpoint that you create.

See [“About creating an appliance checkpoint”](#) on page 128.

See [“Creating an appliance checkpoint”](#) on page 131.

See [“About appliance rollback ”](#) on page 135.

See [“About NetBackup appliance factory reset”](#) on page 141.

About creating an appliance checkpoint

You can use checkpoints to save a snapshot of the current state of the appliance and then use it to Restore your appliance from that point in case of a future failure.

[Table 3-16](#) contains the following fields and functions that you use to create a checkpoint.

Table 3-16 Create Appliance Checkpoint page

Field	Description
Existing appliance restore checkpoints	<p>This field shows all of the current checkpoints that exist. If no checkpoints exist, the following message appears in the field.</p> <p>No appliance restore checkpoint currently exists. Create an appliance checkpoint to revert to the current state of the appliance.</p> <p>The following describes each of the checkpoint types.</p> <ul style="list-style-type: none"> ■ Pre-upgrade checkpoint This checkpoint is created before a software upgrade is performed. ■ Post-upgrade checkpoint This checkpoint is created after you have upgraded your appliance to a newer software version. You may use this checkpoint if you have a need to roll back your appliance to correct a failure. ■ User-directed checkpoint You are responsible for creating this checkpoint. You can create a checkpoint at any time. Only one user-directed checkpoint can exist at any given time. If a user-directed checkpoint already exists and you create a new checkpoint, the new checkpoint overwrites the existing checkpoint. However, before you can create the new checkpoint, a message appears in the Existing appliance restore checkpoints field and informs you that if you create a new user-directed checkpoint, the new checkpoint overwrites any existing checkpoint. ■ You can also monitor the status of the checkpoint creation process from this field.
The following components of the appliance will be included in the checkpoint:	<p>This field lists all of the components that are included in the checkpoint. The following list describes these components:</p> <ul style="list-style-type: none"> ■ The appliance operating system ■ The appliance software ■ The NetBackup software ■ The network configuration ■ Any previously applied software updates ■ Items not included in the checkpoint: <ul style="list-style-type: none"> ■ The backup data is not included.

Table 3-16 Create Appliance Checkpoint page (*continued*)

Field	Description
Create appliance checkpoint	This field is optional. It enables you to provide a label or description for the checkpoint. What you enter in this field helps you identify the new checkpoint.
Action buttons on this page	<p>Validate</p> <ul style="list-style-type: none"> When you click the Validate button you initiate a validation process that ensures the server is running and in a state to create a new checkpoint. A message appears after the validation is run that informs you whether the validation was successful or not. <ul style="list-style-type: none"> If the validation process is successful the following occurs: <ul style="list-style-type: none"> The Create button becomes active. The following message appears: Checkpoint validation is complete. Click Create to create the new checkpoint. If the validation process is not successful the following occurs: <ul style="list-style-type: none"> The following message appears: Checkpoint validation was unsuccessful. The checkpoint cannot be created. Click here for more information. You can click a link within the message to view more information about the error details. <p>Create</p> <ul style="list-style-type: none"> The Create button becomes active after the checkpoint validation completes successfully. Click Create to begin the checkpoint process. When you create this checkpoint, it replaces any current user-directed checkpoint if one exists. <p>Cancel</p> <p>This button cancels the create appliance checkpoint process.</p>

See [“Creating an appliance checkpoint”](#) on page 131.

See [“Checkpoint creation status”](#) on page 133.

See [“Creating an appliance checkpoint from the appliance shell menu”](#) on page 133.

See [“Manage > Appliance Restore”](#) on page 127.

Creating an appliance checkpoint

You begin the process of creating a user-directed checkpoint from the **Create Appliance Checkpoint** page on the NetBackup Appliance Web Console. The first two fields on this page do not require any input from you. The first field is the **Existing appliance restore checkpoints** field. That field displays the checkpoints that currently exist. The second field shows the components within the appliance that are included in the checkpoint.

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 NetBackup Appliance Web Console

1 Select **Manage > Appliance Restore**.

2 Click **Create Appliance Checkpoint**.

If any checkpoints already exist, those checkpoint appear on the page. In addition, if a user-directed checkpoint already exists, the new checkpoint will replace the old checkpoint.

3 Enter a description in the **Create Appliance Checkpoint** description field at the bottom of the page. This description is a way by which you can identify the new checkpoint.

4 Click **Validate**.

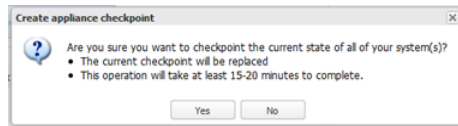
A window appears and shows a validation check is in progress. The validate process ensures that all of the media servers are up and running. A status message appears on the page letting you know whether the checkpoint validation is complete and successful. If the validation is successful and you want to proceed, click **Create**.



If the checkpoint validation was unsuccessful, a status message appears on the page letting you know that the checkpoint cannot be created. A link in the message is provided that you can select to view more information about the media server that is not operational. You should correct that issue and click **Validate** again. Once the validation is successful, click **Create**.

- 5 The **Create Appliance Checkpoint** pop-up appears. If no checkpoint currently exists and you want to proceed, click **Yes**. If a user-directed checkpoint already exists and you want to overwrite that checkpoint, click **Yes**. Otherwise, click **No**.

Note: Once you begin the checkpoint creation process, you cannot perform any other functions on the NetBackup Appliance Web Console until the operation completes.



The **Create Appliance Checkpoint** page refreshes and displays a status of the checkpoint progress for each media server or server. To see more information on the status of the checkpoint creation progress, click the **Details** link.

Create Appliance Checkpoint

i Appliance checkpoint creation in progress. This process may take at least 15-20 minutes to complete.

Status Summary				
Host Name	Current Versions	Progress	Status	Details
192.168.1.13	NetBackup 7.6beta2 Appliance 2.6	<div style="width: 5%; background-color: #ffc107; border: 1px solid #ffc107;"></div> 5%	ACTIVE	Details

See [“Checkpoint creation status”](#) on page 133.

- 6 After the checkpoint creation completes the **Create appliance checkpoint** page displays a status summary that provides the following information:
 - Host name is the IP address of the appliance or appliances that receive the checkpoint.
 - Current NetBackup and appliance software versions installed
 - Progress of the checkpoint creation.
 - Status of the checkpoint.
 - Details of the checkpoint

Click **Finish** to complete the procedure and return to the **Appliance Restore** page.

See [“About creating an appliance checkpoint”](#) on page 128.

See [“Manage > Appliance Restore”](#) on page 127.

Checkpoint creation status

When you begin the user-directed checkpoint process the checkpoint is created for the appliance. Each of the systems is listed in the **Checkpoint creation status** table. This table provides the following information about each system.

Table 3-17 Checkpoint creation status

Field	Description
Host name	The IP address of the appliance that is about to receive the new checkpoint.
Current versions	The versions of the NetBackup software and appliance software that are currently installed on the appliance.
Progress	Displays the percentage of completion for each appliance.
Status	Displays whether the checkpoint operation completed successfully or not. A possible status for this field is: SUCCESS, FAILED, Timed-out.
Details	This field contains a link labeled Details . Click this link to view more detailed information about the status of the create checkpoint operation.

See [“Creating an appliance checkpoint”](#) on page 131.

See [“About creating an appliance checkpoint”](#) on page 128.

See [“Manage > Appliance Restore”](#) on page 127.

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.

- 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.

Note: Once you begin the checkpoint creation process, you are still able to use the NetBackup Appliance Web Console.

See [“Checkpoint creation status”](#) on page 133.

See [“About creating an appliance checkpoint”](#) on page 128.

See [“Manage > Appliance Restore”](#) on page 127.

About rollback to a checkpoint

After you have installed a software update or EEB you may determine that you need to revert back to the previously installed version. This process is referred to as a Rollback operation and it is installed on your appliance by the Symantec update process. Roll back to an appliance checkpoint restores the system to the checkpoint's point-in-time image. That version may be a previous General Availability (GA) version of the software.

When you want to roll back the appliance, you can choose from the following three types of checkpoints.

- **Pre-upgrade checkpoint**
This checkpoint is created before a software upgrade is performed.
- **Post-upgrade checkpoint**
This checkpoint is created after you have upgraded your appliance to a newer version. You may use this checkpoint if you have a need to roll back your appliance to correct a failure.
- **User-directed checkpoint**
A checkpoint that you created.

The following is a list of general guidelines to consider when you revert to a checkpoint:

- Only valid checkpoints are displayed for you to select.
- During a rollback operation you cannot run any user-initiated operations such as backups, restores, or configuration and maintenance operations.
- When you begin a rollback operation from the NetBackup Appliance Web Console, you cannot perform any other functions on the console until the rollback operation completes. That is only true when you perform the operation from theNetBackup Appliance Web Console and not the appliance shell menu.

See [“About appliance rollback ”](#) on page 135.

See [“About appliance rollback validation”](#) on page 136.

See [“About checkpoint rollback status”](#) on page 139.

About appliance rollback

You can roll back your appliance to an existing restore checkpoint using theNetBackup Appliance Web Console, or the NetBackup Appliance Shell Menu. This ability enables you to address any mis-configuration or system failure issues that may have occurred.

To roll back your appliance using the NetBackup Appliance Web Console, open the **Manage > Appliance Restore** page and select **Rollback Appliance**. If no checkpoints exist, a message stating that no checkpoints exist appears on the page. You can return to the **Manage > Appliance Restore** page and select **Create Appliance Checkpoint** and create a user-directed checkpoint.

If checkpoints already exist, they are shown in the **Rollback Appliance** page.

[Table 3-18](#) contains the following fields and functions:

Table 3-18 Rollback Appliance page

Field	Description
Select an appliance checkpoint, to rollback the appliance to a specific checkpoint	<p>This field shows the available checkpoints that you can use to revert your appliance. The available checkpoints can be:</p> <ul style="list-style-type: none"> ■ Pre-upgrade checkpoint A checkpoint that is created before you perform a software upgrade. ■ Post-upgrade checkpoint A checkpoint that is created after you have upgraded your appliance to a newer software version. ■ User-directed checkpoint A checkpoint that you created.
Select the additional actions to be performed during the rollback process	
Version information	<p>If checkpoints exists, you see the table. If no checkpoints exist, this table is not shown. The table provides the following information:</p> <ul style="list-style-type: none"> ■ Host Name ■ Current versions The NetBackup and appliance software versions currently installed before the rollback operation begins. ■ Versions after rollback The NetBackup and appliance software versions that are installed after the rollback operation succeeds.
Action icons	The Preview icon cancels the rollback operation.

See [“About appliance rollback validation”](#) on page 136.

See [“About checkpoint rollback status”](#) on page 139.

About appliance rollback validation

This page displays a list of the appliance configuration components that are rolled back.

Note: During a rollback process, all appliance functions are suspended.

Rolling back to an appliance checkpoint reverts the following components:

- The appliance operating system

- The appliance software
- The NetBackup software
- The network configuration
- Any previously applied software updates
- Items not included in the checkpoint:
 - The backup data is not included.

After you have reviewed the list of actions, click **Validate** to continue with the rollback operation.

The **Rollback Appliance** pop-up window appears. This pop-up informs you that once you start the rollback process, it is irreversible. Click **Yes** to proceed with the rollback operation. Click **No** to stop the rollback process.

See [“About appliance rollback ”](#) on page 135.

See [“About checkpoint rollback status”](#) on page 139.

See [“About appliance rollback ”](#) on page 135.

Rollback to an appliance checkpoint from the NetBackup Appliance Web Console

You can rollback an appliance to a checkpoint that you choose from the NetBackup Appliance Web Console or the appliance shell menu. The following procedures describe these procedures.

To roll back to an existing checkpoint from the NetBackup Appliance Web Console

- 1 Select **Manage > Appliance Restore**.
- 2 Click **Appliance Rollback**.
- 3 Select an available checkpoint from the **Select an appliance checkpoint to rollback the appliance to a specific checkpoint** list.

The list contains only those checkpoints that exist. At most, there can be three checkpoints. A pre-upgrade checkpoint, a post-upgrade checkpoint, and a user-directed checkpoint.

- 4 Determine if you want to restart the appliance automatically after the rollback operation completes. If you do, check the **Restart appliance automatically after rollback** check box.

5 Click **Preview**.

The **Rollback Appliance** page updates and shows a the components that are rolled back during the operation. In addition, the appliances that are going to be rolled back are also displayed on the page.

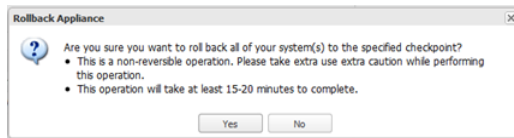
6 Click **Validate**.

The validation check ensures that all media servers are up and running. If all media servers are running, click **Start** to roll back to the selected checkpoint.



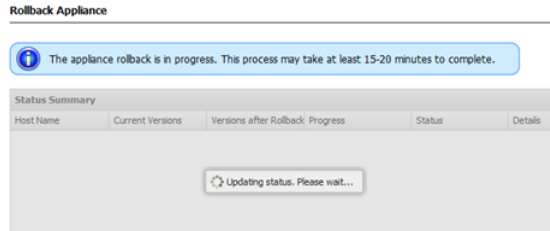
If the checkpoint validation was unsuccessful, you are not able to start the rollback operation. A link is provided that you can select to view more information about the cause of the issue. You can then, correct that issue, and click **Validate**. If the validation is successful, click **Start**.

7 The **Rollback Appliance** pop-up appears. This pop-up informs you that once you start the rollback process, it is irreversible. Click **Yes** to proceed with the rollback operation. Click **No** to stop the rollback process.



Note: Once you begin the rollback process, you cannot perform any other functions on the NetBackup Appliance Web Console until the operation completes.

- 8 The **Rollback Appliance** status page appears so you can monitor the success of the rollback operation for the appliance.



- 9 After the rollback operation completes the compute appliance must be restarted:
- If you chose to automatically restart the appliance after the rollback completes, a **Restart in progress...** pop-up appears. This pop-up window reminds you that the network was reset and connectivity was lost during the Restore process. You must use the remote management port to reconfigure the network settings and reconnect to the NetBackup Appliance Web Console.
 - If you did not choose to automatically restart the appliance after the rollback completes, a **Restart Now!** window appears. This window prompts you to restart each of the servers that were selected to be rolled back. Click **OK** to restart the appliance to complete the rollback operation.

See [“Rollback to an appliance checkpoint from the appliance shell menu”](#) on page 140.

See [“Manage > Appliance Restore”](#) on page 127.

About checkpoint rollback status

Table 3-19 Checkpoint Rollback status

Field	Description
Host name	The IP address of the appliances that are about to be rolled back.
Current versions	The version NetBackup software that is currently installed on the appliance.
Verison after rollback	The version of appliance software that is installed on the appliance after the rollback is complete.

Table 3-19 Checkpoint Rollback status (*continued*)

Field	Description
Progress	Displays the percentage of completion for each appliance.
State	Displays whether the checkpoint operation completed successfully or not. Possible status for this field: Success, Failed, Completed, Timed-out.
Details	This field contains a link labeled Details . Click this link to view more detailed information about the status of the appliance rollback operation.

See [“About appliance rollback validation”](#) on page 136.

See [“About appliance rollback ”](#) on page 135.

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.

- 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 the appliance automatically after the rollback operation completes.
- 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.symantec.com
```

```
Please reconnect to the appliance shell menu to continue
using this appliance.
```

```
The system is going down for reboot NOW!
```

See [“Checkpoint creation status”](#) on page 133.

See [“About creating an appliance checkpoint”](#) on page 128.

See [“Manage > Appliance Restore”](#) on page 127.

About NetBackup 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.

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: 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 (**Manage > Appliance Restore > Retain network configuration**). After the factory reset completes, you can then enable WAN optimization again for the network interface bonds.

If you *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.

From the **Manage > Appliance Restore** page on the NetBackup Appliance Web Console you can click **Launch Appliance Factory Reset** to begin the reset process. Record your network configuration information before you begin a factory reset. After the reset operation completes the appliance is restarted, either automatically or manually. You may need the configuration information to log into the appliance.


Appliance Factory Reset

Select the additional actions to be performed during the factory reset process

- ☐ Retain storage configuration and backup data
- ☐ Retain network configuration
- ☐ Restart Host(s) automatically after reset

A factory reset operation resets the entire system, that includes the following actions

- ➔ Resets the appliance operating system
- ➔ Resets the appliance software
- ➔ Resets the NetBackup software
- ➔ Resets the tape media configuration on the master server
- ➔ Resets the network configuration
- ➔ Resets the storage configuration and backup data

 Symantec recommends that you record your network configuration information before you begin a factory reset. You will need this information to log on to the appliance after it is restarted.

Validate

Start

Cancel

The field, **Select the additional actions to be performed during the factory reset process** contains the following:

- **Retain storage configuration and backup data**

Select this option to save your storage configuration and all backup data on the storage partitions and any connected expansion units.

If you do not select this option, the following occurs:

- All the images on the AdvancedDisk and deduplication storage pools are removed.
- All backup data on the storage partitions and any connected expansion units are reset.
- **Retain network configuration**
Select this option if you want to retain the network configuration of the appliance. If you do not select this option, all network configuration settings will be reset.
- **Restart host(s) automatically after reset**
Select this option if you want to have the appliance restarted automatically after the factory reset completes.

Table 3-20 describes the remaining fields that are contained in the **Appliance Factory Reset** page.

Table 3-20 Appliance factory reset features

Fields	Description
A factory reset operation resets the entire system, that includes the following actions	<p>This part of the Appliance Factory Reset displays all of the areas of your appliance that are reset once you start the factory reset operation.</p> <p>A factory reset operation resets the entire system, which includes resetting the following:</p> <ul style="list-style-type: none"> ■ Appliance operating system ■ Appliance software ■ NetBackup software ■ Tape media configuration on the master server ■ Networking configuration (optionally retain) ■ Storage configuration and backup data (optionally retain)
Action buttons	<p>The following action buttons are available at the bottom of this page:</p> <ul style="list-style-type: none"> ■ Start - Begin the factory reset operation. ■ Cancel - resets the current page.
Versions information	<p>This field appears after you have clicked Validate. It provides you with the following information:</p> <ul style="list-style-type: none"> ■ Current Versions - This field displays the NetBackup and appliance software versions that are currently installed on each appliance. ■ Versions after reset - This field displays the NetBackup and appliance software versions that are installed after the factory reset operation completes successfully.

Note: Image imports after a factory reset, reimage, or during data migration from one master server to another may span from several hours to multiple days to complete depending on the size and number of the images to be imported.

See [“Starting a factory reset from the NetBackup Appliance Web Console”](#) on page 145.

See [“About factory reset status”](#) on page 149.

See [“Manage > Appliance Restore”](#) on page 127.

About factory reset best practices

This topic contains best-practice information about factory reset operations.

- Factory Reset operations are not supported if a 52xx master server or media server has been upgraded to version 2.6.0.1 or later. Factory Reset is only supported after a clean installation of version 2.6.0.1 or later on a 52xx appliance, or if a 52xx appliance is reimaged to version 2.6.0.1 or later
- If you manually configure Nirvanix on an appliance after the initial configuration is complete, then you must first manually unconfigure and delete the Nirvanix configuration. The factory reset process does not clean the Nirvanix configuration.
- When performing a factory reset to a previous software version it is recommended to also reset the storage. The storage will be inaccessible after you perform a factory reset to a previous version on the appliance.
If you perform a factory reset without resetting the storage, you need to apply a patch to update your appliance to the version it was at before you performed the factory reset. You must apply the patch before performing any other operations on the Appliance.
- 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
Symantec Technical Support if the issue persists.
```

Note: The Storage Reset command is only available when the appliance is in a factory state.

- If you remove attached storage disks before performing a factory reset, you need to clear the preserved cache of the RAID controller.
See "Discard RAID preserved cache after performing a factory reset" in the *NetBackup Appliance Troubleshooting Guide* for more information.
- If you remove a storage unit shelf during a factory reset, the factory reset operation can fail. Symantec recommends that you leave all storage unit shelves attached during a factory reset.
- 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 master 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.

Starting a factory reset from the NetBackup Appliance Web Console

The following procedure describes how to start a factory reset operation from the NetBackup Appliance Web Console.

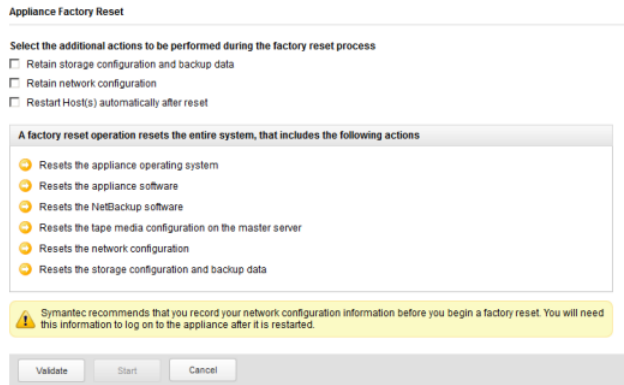
Note: Factory reset operations are not supported if a 52xx master server or media server has been upgraded to version 2.6.0.1. Factory reset is only supported after a clean installation of version 2.6.0.1 on a 52xx appliance, or if a 52xx appliance is reimaged to version 2.6.0.1.

Note: A factory reset operation returns the password to the original, default value.

To begin a factory reset from the NetBackup Appliance Web Console

- 1 Open the **Manage > Appliance Restore** page.
- 2 Click **Launch Appliance Factory Reset**.
- 3 Determine if you want to retain the storage configuration and backup data. If you do, check the **Retain storage configuration and backup data** check box.
Determine if you want to retain the network configuration. If you do, check the **Retain network configuration** check box.
Determine if you want to restart host(s) automatically after the reset completes. If you do, check the **Restart Host(s) automatically after reset** check box.

4 Click **Validate**.




Appliance Factory Reset

Select the additional actions to be performed during the factory reset process

- ☐ Retain storage configuration and backup data
- ☐ Retain network configuration
- ☐ Restart Host(s) automatically after reset

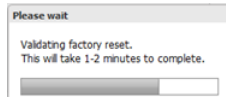
A factory reset operation resets the entire system, that includes the following actions

- Resets the appliance operating system
- Resets the appliance software
- Resets the NetBackup software
- Resets the tape media configuration on the master server
- Resets the network configuration
- Resets the storage configuration and backup data

 Symantec recommends that you record your network configuration information before you begin a factory reset. You will need this information to log on to the appliance after it is restarted.

Validate Start Cancel

After you click **Validate** a pop-up appears to remind you that the validation is in process.



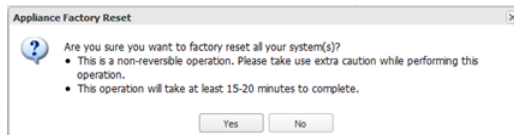
The following results can occur from the validation operation:

- If the validation process completes successfully, a validation complete message appears and you can proceed to Step 6.



5 Click **Start**.

- 6 An **Appliance Factory Reset** pop-up window appears. This window informs you that the factory reset operation is irreversible once it is started.



- Click **Yes** to start the factory reset.

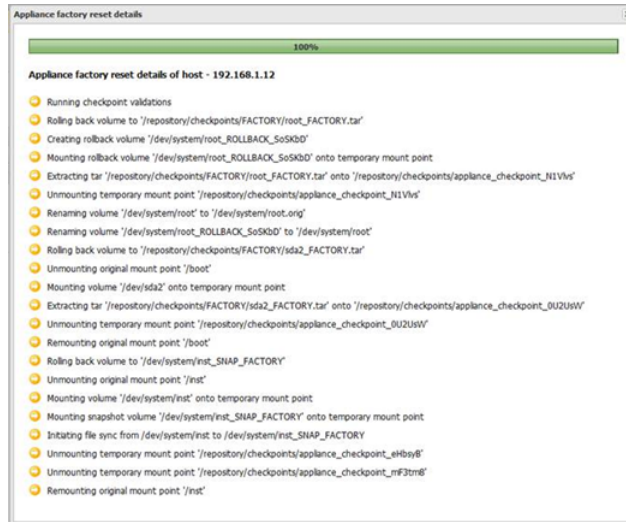
Note: Once you begin the factory reset, you cannot perform any other functions on the NetBackup Appliance Web Console until the operation completes.

- Click **No** to stop the process of performing a factory reset and return the previous page.

After you click **Yes**, the **Appliance Factory Reset** refreshes and displays status summary information. This page shows the progress of the factory reset operation for the appliance. This page shows the following information:

- The name of the appliance to be reset.
- The current version of software that is installed on the appliance before the reset begins.
- The software version that is installed after the reset completes.
- A progress bar that displays a percentage of completion.


The **Details** link in the Status Summary page enables you to view the details of the factory reset for the host that corresponds to the link that you selected.



See [“About factory reset status”](#) on page 149.

- 7 After the reset operation completes, the storage reset operation begins if you did not elect to retain your storage configuration and backup data at the beginning of this procedure.

A storage reset message appears.

 Storage reset is in progress. Click [here](#) for details.

Click on the word **here** to view the details of the storage reset operation.

- 8 After the storage reset operation completes the appliance must be restarted:
 - If you chose to automatically restart the appliance after the reset completes, a **Restart in progress...** pop-up appears. The contents of that pop-up reminds you that the network was reset and connectivity was lost during the reset process. You must use the remote management remote management port to reconfigure the network settings and reconnect to the NetBackup Appliance Web Console.
 - If you did not choose to automatically restart the appliance after the reset completes, a **Restart Now!** window appears. This window prompts you to restart the appliance. Click **OK** to restart the appliance to complete the factory reset operation.
- 9 You must use the remote management port to reconfigure the network settings and reconnect to the NetBackup Appliance Web Console. Perform the following steps:
 - When the appliance restarts and you see the keyboard prompts at the top of the screen, Hit the **F2** function key on the keyboard.
 - Use the left arrow and the right arrow on your keyboard to navigate to the **Server Management** menu.
 - Use the up and down arrows on your keyboard to navigate to the **Baseboard LAN** configuration section.
 - Select the **RMM4 LAN Configuration** section.
 - Enter the network configuration information, such as the IP source [Static], IP, Subnet mask, and Gateway IP addresses.
 - You can now connect to the appliance NetBackup Appliance Web Console.

See [“About NetBackup appliance factory reset”](#) on page 141.

See [“Starting a factory reset from the appliance shell menu”](#) on page 149.

See [“About factory reset status”](#) on page 149.

About factory reset status

This page displays the status of your factory reset operation. The table on this page provides the following information:

Table 3-21

Field name	Description
Host name	Name of the appliance that is about to be reset.
Current version	The version NetBackup software that is currently installed on the appliance.
Version after reset	The version of appliance software that is installed on the appliance after the reset is complete.
Progress	Displays the percentage of completion for each appliance.
Status	Displays whether the checkpoint operation completed successfully or not. A possible status for this field is: Active, Failed, Success, Timed-out .
Details	This field contains a link labeled Details . Click this link to view more detailed information about the status of the create checkpoint operation.

See [“About NetBackup appliance factory reset”](#) on page 141.

See [“Manage > Appliance Restore”](#) on page 127.

Starting a factory reset from the appliance shell menu

The following procedure describes how to start a factory reset operation from the appliance shell menu.

Note: Factory reset operations are not supported if a 52xx master server or media server has been upgraded to version 2.6.0.1. Factory reset is only supported after a clean installation of version 2.6.0.1 on a 52xx appliance, or if a 52xx appliance is reimaged to version 2.6.0.1.

Note: A factory reset operation returns the password to the original, default value.

Note: Image imports during a Factory Reset, reimage or moving data from one master server to another may take a considerable amount of time on the NetBackup 5330 Appliance. This is due to the underlying storage layout in the 5330 hardware.

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.

Appliance factory reset will reset the entire system to the factory installed image. The appliance will have the following components reset to the factory restored settings/image:

- 1) Appliance Operating System
- 2) Appliance Software
- 3) NetBackup Software
- 4) Tape media configuration on the master server
- 5) Networking configuration (optionally retain)
- 6) Storage configuration and backup data (optionally retain)

```
- [Info] Running factory reset validation...please wait (approx 2 mins)
- [Info] Factory reset validation successful.
```

RESET NETWORK CONFIGURATION [Optional]

```
-- Resets the IP and routing configuration.
-- Resets the DNS configuration.
```

```
>> Do you want to reset the network configuration? [yes/no] (yes) no
```

RESET STORAGE CONFIGURATION and BACKUP DATA [Optional]

```
-- Removes all the images on the AdvancedDisk and MSDP storage pools.
-- Resets the storage partitions.
-- Resets storage expansion units, if any.
```

```
>> Do you want to delete images and reset backup data? [yes/no] (yes)
```

```
>> Resetting the storage configuration will remove all backup
data on the storage partitions and any connected expansion
units. This is not reversible. Are you sure you want to
reset storage configuration? [yes/no] (yes)
```

```
>> A reboot of the appliance is required to complete the factory reset.
Reboot automatically after reset? [yes/no] (no) yes
```

```
>> Automatically rebooting after the reset will not provide you with an
opportunity to review the progress/final status of the reset. Are you sure
you would like to automatically reboot? [yes/no] (no) yes
```

- 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]
```

Appliance will make the following version changes:

+-----+			
Appliance	Current Version	Reverted Version	
+-----+			
v49	NetBackup 7.6.0.2 Appliance	NetBackup 7.6.0.2 Appliance	
	2.6.0.2	2.6.0.2	
+-----+			

- 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 following summary messages appear as the factory reset continues:

```
- [Info] PERFORMING APPLIANCE RESET TO FACTORY STATE ON : app2.symantec.com
- [Info] Delete checkpoints (type: NON_FACT) succeeded
- [Info] Reset of the appliance to FACTORY STATE successful.
- [Info] Stopping NetBackup processes... (6 mins approx)
- [Info] Moving NetBackup Appliance Directory to ce-win21-urmil...
- [Info] Acquired lock on the storage.
- [Info] Resetting the storage configuration...
- [Info] Checking whether the 'MSDP' storage partition exists...
- [Info] Initiating deletion of 'MSDP' storage partition...
- [Info] Unmounting the 'MSDP' partition '0'...
- [Info] Deleting the 'MSDP' partition '0'...
- [Info] Checking whether the 'Catalog' storage partition exists...
- [Info] Initiating deletion of 'Catalog' storage partition...
- [Info] Unmounting the 'Catalog' partition '0'...
- [Info] Deleting the 'Catalog' partition '0'...
- [Info] Checking whether the 'Configuration' storage partition exists...
- [Info] Initiating deletion of 'Configuration' storage partition...
- [Info] Unmounting the 'Configuration' partition '0'...
- [Info] Deleting the 'Configuration' partition '0'...
- [Info] Checking whether the 'AdvancedDisk' storage partition exists...
- [Info] Initiating deletion of 'AdvancedDisk' storage partition...
- [Info] Unmounting the 'AdvancedDisk' partition '0'...
- [Info] Deleting the 'AdvancedDisk' partition '0'...
- [Info] Removing the storage configuration...
- [Warning] Failed to query SCSI device '/dev/system/root'.

- [Warning] Failed to query SCSI device '/dev/system/root'.
>> A reboot of the appliance is required to complete the factory reset.
    Reboot now?[yes/no] (no)yes
Rebooting the appliance now...
- [Info] Rebooting app2.symantec.com...
```

Broadcast message from root (Mon Nov 25 11:56:39 2013):

The system is going down for reboot NOW!

- [Info] Rebooting appliance to complete the reset.

Please reconnect to the Appliance shell menu to continue using this appliance

- 5 You must use the remote management remote management port to reconfigure the network settings and reconnect to the NetBackup Appliance Web Console. Perform the following steps:
 - When the appliance restarts and you see the keyboard prompts at the top of the screen, Hit the **F2** function key on the keyboard.
 - Use the left arrow and the right arrow on your keyboard to navigate to the **Server Management** menu.
 - Use the up and down arrows on your keyboard to navigate to the **Baseboard LAN** configuration section.
 - Select the **RMM4 LAN Configuration** section.
 - Enter the network configuration information, such as the IP source [Static], IP, Subnet mask, and Gateway IP addresses.
 - You can now connect to the appliance NetBackup Appliance Web Console.

See [“About NetBackup appliance factory reset”](#) on page 141.

See [“Starting a factory reset from the NetBackup Appliance Web Console”](#) on page 145.

See [“About factory reset status”](#) on page 149.

Manage > License

You can review, add, and delete license keys for your appliance through the NetBackup Appliance Web Console using the **Manage > License** page.

The following describes the license key information that is displayed on the **Manage > License** page:

License Key table

- **Key**
Shows all of the installed license keys.
- **Type**
Describes the license type.
- **Expiry Date**
Indicates when the license expires.

Feature Details table

- **Feature ID**

Identifies the feature number that is associated with the selected license key.

- **Feature Name**

Identifies the feature name that is associated with the selected license key.

See [“Managing license keys on the NetBackup appliance”](#) on page 154.

See [“Adding a permanent license key if an evaluation license key expires”](#) on page 155.

Managing license keys on the NetBackup appliance

The following procedures describe how to view, add, and delete NetBackup option license keys through the appliance user interface or the NetBackup Appliance Shell Menu

To add license keys through the NetBackup Appliance Web Console

- 1 Log in to the NetBackup Appliance Web Console.

- 2 Click **Manage > License**

All installed license keys, associated feature IDs, and associated feature names are displayed.

- 3 To add new license keys, do the following:

- Click **Add**. The following warning message is displayed:

```
This operation restarts NetBackup processes after the
licenses have been added successfully. The NetBackup domain does not
run any job during this time. Are you sure you want to proceed?
```

Click **Yes**.

- In the **Add License Key** dialog box, enter the license key in the **Key** field for the selected server.
- Click **OK**.

To delete a license key through the NetBackup Appliance Web Console

- 1 Log on to the NetBackup Appliance Web Console.

- 2 Click **Manage > License**.

All installed license keys, associated feature IDs, and associated feature names are displayed.

- 3 In the **Key** column, select the license keys that you want to delete by selecting the check box next to the license key number.
- 4 Click **Delete**.

The following message is displayed:

```
Deleting the selected license(s) will disable related
features in NetBackup. This operation restarts NetBackup processes
after the licenses have been deleted successfully. The NetBackup domain
does not run any job during this time. Are you sure you want to proceed?
```

- 5 Click **Yes** to confirm the deletion.

To view, add, and delete license keys through the NetBackup 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.
- 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**.
 - 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**.
 - To remove another license key, press `y`.
 - Repeat the previous step or press `n` to exit.

Adding a permanent license key if an evaluation license key expires

If your evaluation license key expires, you may encounter problems if you need to install or configure 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 appliance stops working.
- A new installation of this release using a USB drive may appear to hang when you configure NetBackup.
- An attempt to run a factory reset fails.
- You are unable to complete an initial configuration of a preinstalled, NetBackup appliance.
- Unable to upgrade from a previous version to this version of the appliance.
- You may even observe the following issues with a preinstalled NetBackup appliance that does not have permanent keys installed.
 - System self-test fails.
 - Backup and restore jobs fail.
 - The user interface does not load.
- A forced, factory reset appears to hang while configuring NetBackup.

To install a permanent license key on a preinstalled NetBackup appliance with an expired evaluation key

- 1 Log on to NetBackup Appliance Shell Menu. Use `admin` as the user name and `P@ssw0rd` as the password.
- 2 Enter `Main_Menu > Manage > License > Add`.
- 3 Enter yes when prompted to continue.
- 4 Enter a valid evaluation or production NetBackup license key when prompted for a NetBackup license key.
- 5 Enter `n` when prompted to add an additional license key.
- 6 Stop the NetBackup processes.

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

- 7 Start NetBackup processes.

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

See [“Manage > License”](#) on page 153.

See [“Managing license keys on the NetBackup appliance”](#) on page 154.

About the Migration Utility

The **Migration Utility** lets you move copies of backup images from the source disk pool to the destination disk pool. It enables you to:

- Migrate (copy) images from source storage to destination storage to seed the destination storage client backup history
- Convert policies so new backups go to the new destination storage
- Accomplish this without impacting existing backup schedules
- Eventually decommission or repurpose the source storage

For v2.6.x the **Migration Utility** feature is applicable with the following conditions:

- Images available for migration are the “latest complete backup picture” for a specific policy/client pair. Which means that it is the last FULL backup for the specific policy/client
For policy types which do not follow the FULL backup convention, other images are included in the migration. The Migration Utility tries to include everything required to represent the latest complete backup picture.
- The latest complete backup picture only includes complete images and images which are “storage lifecycle complete”.
- The migration is not performed using Fibre Channel, this is because data transfer between the following is not supported for v2.6.x:
 - From NetBackup PureDisk to a Media Server Deduplication Pool (MSDP) through a Fibre Channel cable
 - From an MSDP to another MSDP through a Fibre Channel cable

Note: You must make sure that you have the proper credentials to schedule and complete a migration job. To ensure that you have the proper credentials, go to the **Media and Device Management > Credentials > Storage Servers > Media Servers** window in the NetBackup Administration Console. Ensure that the check boxes next to the media servers to be used for your migration job have been selected. Only when these selections have been made can you perform a migration job.

The following diagram provides a brief overview of the Migration Utility feature:

The utility provides the ability to automate the migration jobs by letting you schedule when the migrations run. The utility also tracks the images that have been migrated. Multiple migrations can be scheduled so that they do not interfere with normal backups and duplications.

When you click **Manage > Migration Utility**, the following tabs appear:

- **Selection Criteria**

Use this tab to select the start time, the migration window (duration), the source disk pool where the current backup images reside, and the destination (target) disk pool where you want the images migrated.

When you click **Apply Search Criteria**, the tab is refreshed with a list of all the files on the source disk pool that match the search criteria.

- **Policy Conversion**

Use this tab to change the policy that you want to use for the backups that are now targeted for the destination disk pool.

Once an image has been migrated to the destination disk pool, select the policy name and the policy type on this tab so that backups and duplications for that image are targeted for the destination disk pool.

- **Migration Job Status**

Use this tab to view the status and the result of all the scheduled migration jobs. The most recent job appears at the top of the list.

See [“Selection Criteria”](#) on page 159.

See [“Selecting the search criteria and scheduling the migration job”](#) on page 162.

See [“Policy Conversion”](#) on page 166.

See [“Setting-up a policy conversion map”](#) on page 168.

See [“Migration Job Status”](#) on page 163.

See [“Viewing migration job status and details”](#) on page 166.

See [“Best practices to run a migration job”](#) on page 169.

Selection Criteria

When you navigate to **Manage > Migration** page, the appliance displays the **Selection Criteria** tab. You can use this tab to perform the following tasks:

- Apply the search criteria by selecting the appropriate source disk pool, destination disk pool, and policy types
- View the estimated transfer time to run the migration job
- Schedule the migration job

The **Selection Criteria** page is divided into two sections:

- The first section enables you to apply the search criteria.
- The second section displays the estimates for running a migration job based on the selected parameters. Based on the estimates you can select the policy to run the migration job.

The [Table 3-22](#) describes the information to be provided in the selection criteria. The default settings are most policy types, all policy names, and 60-minute migration time window.

Table 3-22 Selection Criteria for a migration

Search criteria	Description
Source disk pool	<p>Select the appropriate disk pool, from the drop-down list, where the original backup images reside. The source can be any recognized and connected disk pool.</p> <p>Note: You can use the Policy Conversion tab to add a new source disk pool.</p>
Destination disk pool	<p>Select the appropriate disk pool, from the drop-down list, where you want the migrated (copied) backup images to reside. The destination can be any recognized Symantec provided disk pool.</p> <p>Note: You can use the Policy Conversion tab to add a new source disk pool.</p>
Policy type	<p>Click on the check-box to select the policy type from the list of policies displayed. The policies to be migrated are searched based on this selection. For example, if you select the policy type as Standard, all the policies that belong to this type are displayed.</p> <p>You can use the Select All and Clear All links to select or remove the selection of all the policies at the same time.</p>
Policy name	<p>If you know the name of the policy to be migrated, enter the name of that policy. To perform an advanced search, use the * and ? characters as follows:</p> <ul style="list-style-type: none"> ■ Enter *policy to search for policy names that end with the word "policy". ■ Enter policy??? to search for policy names that begin with the word "policy" and include the next three characters in the name.

Table 3-22 Selection Criteria for a migration (*continued*)

Search criteria	Description
Duration of migration window	Enter the expected time duration to run the migration job that allows migration to place limits on the amount of NetBackup catalog data which must be searched. This duration helps you to minimize the effect on NetBackup and avoid returning unwanted information. Searching for images to migrate is a time consuming process, therefore the search process is bounded by the Migration Window Duration .
Apply search criteria	Click to search for the policies that match the selection criteria.

The migration utility begins searching for images matching the criteria. Based on the size of the image(s), destination's transfer rate, and the transfer time the policy's images are added to the **Possible Selections** section. You can use this retrieved information to run the migration job. The [Table 3-23](#) describes the **Possible Selections** section:

Note: Images that are not SLP (Storage Lifecycle Policy) complete are not copied, therefore these images are not included in the **Possible Selections** section.

Table 3-23 Possible Selections

Column heading	Description
Estimated time to run the migration job (minutes)	Based on the policy name selected this bar graph is update to display the estimated utilization of the migration window. The bar graph is uses percentages and minutes to depict the estimated utilization of the migration windows.
Policy	Displays a check box and the name of the policies retrieved based on the search criteria. Select the check-box next to the policy you want to migrate. The bar graph is updated according to the policy selected.
Estimated transfer time	Displays the estimated time to transfer the data when you run the migration job.
Size	Displays the estimated size of the data that will be transferred when you run the migration job.

Table 3-23 Possible Selections (*continued*)

Column heading	Description
Policy Type	Displays the policy type of the policies retrieved based on the search criteria.
Number of clients/Client names	Displays the number of clients in the first row, followed by the client names in the remaining rows.
Image Date	Displays the date on which the data was last backed up for the corresponding client name.
Schedule Migration	<p>After you have evaluated the possible selections, use the following radio buttons to schedule the migration job:</p> <ul style="list-style-type: none"> ■ Start Immediately to run the migration job at the current time. ■ Schedule Migration to enter the run the migration job based on the specified time.

You can now navigate to the following tabs:

- **Schedule migration**
The migration job is scheduled and you can view the status of the migration job when you click the **Migration Job Status** tab.
See [“Migration Job Status”](#) on page 163.
 - **Policy Conversion** tab.
Click this tab to change the policy that you want to use for the backups that are now targeted for the destination disk pool.
See [“Policy Conversion”](#) on page 166.
- See [“Selecting the search criteria and scheduling the migration job”](#) on page 162.
- See [“About the Migration Utility”](#) on page 157.
- See [“Best practices to run a migration job”](#) on page 169.

Selecting the search criteria and scheduling the migration job

This section provides the procedure to select the search criteria using the **Manage > Migration Utility > Selection Criteria** tab.

To select the search criteria and schedule a migration job:

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Manage > Migration Utility > Selection Criteria**.
The appliance displays the **Selection Criteria** tab.
- 3 Enter the selection criteria in the provided fields. A description of the selection criteria is available at [Selection Criteria](#).
- 4 Click **Apply Search Criteria**, to set the search criteria for scheduling a migration job.

Based on the search criteria, the appliance displays the available migration policies and the estimated time to migrated the backed up data using these policies. A description of the possible selections is available at [Selection Criteria](#).

- 5 Select one or more policies whose image(s) for the listed client(s) should be copied from the source storage to the destination storage.

Based on policy name selected the **Estimated time to run the migration job (minutes)** bar graph is update to display the estimated utilization of the migration window.

- 6 To run the migration job you can select from the following two approaches:

Click **Start Immediately** to run the migration job at the current time.

Or

Enter the start time and click **Schedule Migration**.

- 7 Click **Migrate** to run the migration job.

The appliance runs the migration job. You can view the details of the migration job using the **Migration Job Status** tab.

See “[Selection Criteria](#)” on page 159.

See “[About the Migration Utility](#)” on page 157.

See “[Best practices to run a migration job](#)” on page 169.

Migration Job Status

The **Migration Job Status** tab provides a convenient way to coordinate migration jobs, to cancel jobs, to review rolled up migration results, and reports status. This tab lets you view the status and the result of all the scheduled migration jobs. The most recent job appears at the top of the list. Only a single job can be **QUEUED** or **RUNNING** at any time

[Table 3-24](#) describes the status and the result conditions that are reported.

Table 3-24 Migration job reports

Report	Description
Migration Job Id	Displays the Id of the executed migration jobs.
Status	<p>Displays the current status of the migration job.</p> <ul style="list-style-type: none"> ■ QUEUED The migration job is scheduled in the job queue and is waiting to start. Only one job can be queued at any one time. You can choose to cancel a migration job with this status. ■ RUNNING The migration job is currently in progress. Only one job can be run at any one time. You can choose to cancel a migration job with this status. ■ COMPLETE The migration job has completed and a new migration can be started. ■ CANCELED The migration job that had a QUEUED or a RUNNING status was canceled. ■ CANCEL_IN_PROGRESS A very short lived status used to coordinate cancel. ■ POST_PROCESSING The data transfer is complete and the utility is wrapping up the results.
Start Time	Displays the time when the migration job was executed.
Planned Duration (min)	Displays the planned duration, in minutes, estimated for executing the migration job.
Actual Duration (min)	Displays the actual duration, in minutes, taken to execute the migration job.
Images Copied	Displays the total number of backup images that have been copied during migration.

Table 3-24 Migration job reports (*continued*)

Report	Description
Outcome	<p>Displays the final outcome of how the migration job was executed.</p> <ul style="list-style-type: none"> SUCCESS The migration job has completed successfully with no errors. That is N of N images were successfully copied. To see a list of the job details, click on the associated link for that job. SUCCESS* The migration job has completed successfully with no errors. That is N of N images were successfully copied. The * next to the outcome signifies that you should examine the job details. To see a list of the job details, click on the associated link for that job. PARTIAL The migration job is either in progress or it was not able to migrate all of the files in the job. That is a subset of N images were successfully copied. To see a list of the job details, click on the associated link for that job. FAILED The migration job was not able to migrate any of the files in the job. That is zero images were successfully copied. To see a list of the job details, click on the associated link for that job.
Job Details	<p>Displays the Details link. Click to view the log of the migration job executed. It displays the NetBackup image copy details and the migration transfer rate information</p>
Cancel Job	<p>This button can be used to cancel a migration job that is currently being executed.</p>

See [“Viewing migration job status and details”](#) on page 166.

See [“Selection Criteria”](#) on page 159.

See [“Policy Conversion”](#) on page 166.

See [“About the Migration Utility”](#) on page 157.

See [“Best practices to run a migration job”](#) on page 169.

Viewing migration job status and details

This section provides the procedure to view the details of the migration job and to cancel a migration job, using the **Manage > Migration Utility > Migration Job Status** tab.

To view the details of the migration job:

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Manage > Migration Utility > Migration Job Status**.

The appliance displays the **Migration Job Status** tab. It lists all the migration jobs executed using the **Selection Criteria** tab.

- 3 Click on the **Details** link to view the details of how the migration job was executed.

The appliance displays the details of the migration job.

The following procedure describes how to cancel a migration job.

To cancel a migration job:

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Manage > Migration Utility > Migration Job Status**.

The appliance displays the **Migration Job Status** tab. It lists all the migration jobs executed using the **Selection Criteria** tab.

- 3 Select the check box next to the migration job you want to cancel.

Note: You can cancel only those jobs with the status as **Scheduled** or **In progress**.

- 4 Click **Cancel**.

The Cancel operation is recorded in the job details of the migration job.

See [“Migration Job Status”](#) on page 163.

See [“About the Migration Utility”](#) on page 157.

See [“Best practices to run a migration job”](#) on page 169.

Policy Conversion

The **Policy Conversion** tab is an important operation, however, it is an optional operation. That is why the default landing page for the migration utility is the **Selection Criteria** tab. The **Policy Conversion** tab enables you to perform the following tasks:

- Add new source and destination disk pools by mapping them to your existing source disk pools and destination disk pools.
- Updates the NetBackup policies over to using the new destination storage for backups, post successful migration.
- Policy conversion is configured by a policy conversion map. Each source storage has its own unique map.

The **Policy Conversion** tab includes two sections:

- **Select Policy Conversion map**
- **Policy Conversion map details**

[Table 3-25](#) describes the information you must enter to **Select Policy Conversion map** section.

Table 3-25 Select Policy Conversion map fields and buttons

Fields and buttons	Description
Source Storage / Map name	Select a policy conversion map from the drop-down list. There is a policy conversion map for every possible source storage in the NetBackup domain.
Load and Activate map	Click to load the current map for the selected source storage.

The **Policy Conversion map details** is split in two columns **Storage Lifecycle Policies** and **Storage Units**. When you visit the **Policy Conversion** tab for the first no map exists, so the utility locates all Storage Lifecycle Policies (SLPs) and Storage Units (STUs) that reference the given source disk pool and displays them in the respective columns. [Table 3-26](#) describes the information you must enter to change the source disk pools and the destination disk pools.

Table 3-26 Policy Conversion map details data entry fields and options

Field	Description
Storage Lifecycle Policies (SLP) - Current	Select the current SLP, to be mapped, that references to the given source disk pool.
Storage Lifecycle Policies (SLP) - New	Enter the name of the new SLP to be mapped to the current SLP.
Storage Units (STU) - Current	Select the current STU, to be mapped, that references to the given source disk pool.

Table 3-26 Policy Conversion map details data entry fields and options
(continued)

Field	Description
Storage Units (STU) - New	Enter the name of the new STU to be mapped to the current STU.
Comit new map	Click to save and active the mapping. If SLPs or STUs are added, removed, or modified in NetBackup, the Current columns are automatically modified to match the latest system state. If SLPs or STUs are added, removed, or modified in NetBackup, the Storage Lifecycle Policies (SLP) - Current and Storage Lifecycle Policies (SLP) - New columns are automatically modified to match the latest system state.

See [“Setting-up a policy conversion map”](#) on page 168.

See [“Selection Criteria”](#) on page 159.

See [“Migration Job Status”](#) on page 163.

See [“About the Migration Utility”](#) on page 157.

See [“Best practices to run a migration job”](#) on page 169.

Setting-up a policy conversion map

This section provides the procedure to set up a policy conversion map. In your migration policies, you add new source and destination disk pools by mapping them to your existing source disk pools and destination disk pools. The migration utility updates the policy such that new backups use the new destination storage in place of the old source storage.

To set up a policy conversion map:

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Manage > Migration Utility > Policy Conversion**.
The appliance displays the **Policy Conversion** tab.
- 3 Select a policy conversion map from the **Source Storage / Map name** the drop-down list.

4 Click **Load and Activate map**.

When you visit the **Policy Conversion** tab for the first time no map exists, so the utility locates all Storage Lifecycle Policies (SLPs) and Storage Units (STUs) that reference the given source disk pool and displays them in the respective columns.

5 From the **Policy Conversion map details** section, select the current SLP, to be mapped, that references to the given source disk pool in the **Storage Lifecycle Policies (SLP) - Current** field.

6 Enter the name of the new SLP to be mapped to the current SLP in the **Storage Lifecycle Policies (SLP) - New** field.

7 From the **Policy Conversion map details** section, select the current STU, to be mapped, that references to the given source disk pool in the **Storage Unit (STU) - Current** field.

8 Enter the name of the new STU to be mapped to the current STU in the **Storage Unit (STU) - New** field.

9 Click **Commit new map** to map and activate the SLPs and STUs.

The appliance uses the information to map the SLPs and STUs. If the action is successful the SLPs or STUs are added, removed, or modified in NetBackup, the **Storage Lifecycle Policies (SLP) - Current** and **Storage Lifecycle Policies (SLP) - New** columns are automatically modified to match the latest system state.

See [“Policy Conversion”](#) on page 166.

See [“About the Migration Utility”](#) on page 157.

See [“Best practices to run a migration job”](#) on page 169.

Best practices to run a migration job

The following best practices should be kept in mind while run a migration job, using the migration utility:

- Do not run multiple instances of the Migration Utility concurrently on the same appliance nor anywhere within the NetBackup domain.
 - When you attempt to run multiple instances on the same appliance can cause the utility to generate incorrect estimates in the **Possible Selections** section.
 - When you attempt to run multiple instances within the NetBackup domain for the same source and destination combination can cause the utility to generate incorrect estimates in the **Possible Selections** section.

- Select one appliance in the NetBackup domain to be the “Migration Utility Appliance” and only run the utility from that appliance. The utility saves job information on the appliance and can be accessed from the given appliance.
- If your master server is an appliance select the master server appliance to be the “Migration Utility Appliance.” As the migration utility requires access to the NetBackup domain (for example, policy, storage, and catalog) information, using a master server provides a better performance in generating the list of **Possible Selections**.
- The migration utility supports only a single job to be **QUEUED** or **RUNNING** at one time. No other Migration Utility activity is supported until the job reaches **COMPLETE** or **CANCELLED**.
- After you have made the selection and click **Migrate**, refresh the **Possible Selections** section, using the **Apply search criteria** button. When a job is **QUEUED** or **RUNNING** the utility will return immediately with 0 possible selections.
- Do not attempt to reuse the options from the **Possible Selections** across multiple migrations. The list of **Possible Selections** must be brought up to date using the **Apply search criteria** button, once the previous job completes.

See [“Selection Criteria”](#) on page 159.

See [“About the Migration Utility”](#) on page 157.

See [“Policy Conversion”](#) on page 166.

See [“Migration Job Status”](#) on page 163.

Software release updates for NetBackup Appliances

Symantec provides bundled, release-update packages for the appliance that you can download from the Symantec Support website. From the NetBackup Appliance Web Console or the NetBackup Appliance Shell Menu, you can check the Symantec Support website and determine if a software update is available.

The bundled packages include updates for the following appliance software applications:

- Linux operating system
- NetBackup server
- NetBackup Appliance Web Console

Starting with NetBackup appliance version 2.6.0.2, NetBackup clients are no longer included with NetBackup appliance release updates. If you want to store clients on the appliance, a separate client package is available to download. The client package

is available from the same location as the server release updates and includes the NetBackup Administration Console.

Note: Client versions that are stored on the appliance do not have to match the NetBackup version that is currently installed on the appliance.

To access available appliance software release updates, refer to the following topics:

See [“Download software updates directly to the NetBackup appliance”](#) on page 179.

See [“Download software updates to the NetBackup appliance using client share”](#) on page 180.

See [“Downloading and installing NetBackup appliance software from NetBackup Appliance Web Console”](#) on page 175.

See [“Installing NetBackup appliance software using the NetBackup Appliance Shell Menu”](#) on page 183.

Guidelines to install a software update

To facilitate installing or upgrading the NetBackup Appliance software, it is recommended that you follow certain guidelines to perform the software upgrade.

Preparing for a software upgrade process:

- Identify a period of downtime for your appliance to upgrade the appliance software. The upgrade process provides the estimated time that is required for completing the process. You can choose to proceed or reschedule it at a different time so that you can continue your work.
- Follow the same order as traditional NetBackup upgrades, for the Appliance upgrades. Begin by updating the Master server followed by the Media server appliances.
- If a traditional NetBackup master server is used with a media server appliance, that master server must have either the same or a later version of NetBackup as the media server appliance. For example, before you upgrade a media server appliance with NetBackup Appliance version 2.6, first upgrade the master server to NetBackup version 7.6.

Before you initiate a software upgrade process:

- When you upgrade a NetBackup appliance, the FTMS server is restarted automatically. As a result, the Fibre Channel (FC) ports must be rescanned to allow any SAN Client computers to reconnect to the Fibre Transport (FT) devices.

To rescan the FC ports, after the upgrade has been completed, refer to:

- Step 9 of the procedure to install software updates through the NetBackup Appliance Web Console
- Step 4 of the procedure to install software updates through the NetBackup Appliance Shell Menu
- If you plan to upgrade more than one media server, you must perform the upgrade procedure on each media server.
- According to the requirement from the software update, the Web service may not be available during the upgrade process. The Web service may be unavailable for a few minutes or throughout the entire upgrade process. How long the Web services are unavailable depends on the type of the software update you download. Therefore, you cannot use the NetBackup Appliance Web Console until the Web service is restored.

While the Web services are unavailable and before you can open the NetBackup Appliance Web Console again, you can run the following command to view the upgrade process.

```
Main > Manage > Software > UpgradeStatus
```

Note: This command is available only for upgrades from version 2.6.0.1 and later and cannot be used for upgrades from 2.5.x.

- According to the requirement from the software update, the system may restart several times during the upgrade process. While the system restarts, the NetBackup Appliance Web Console and any SSH-based connection to the server is unavailable until the restart process completes. You can use the Symantec Remote Management interface to view the system restart status.
- When you perform an appliance upgrade, Symantec recommends that you take precautions to avoid loss of connectivity. Any loss of connectivity during an upgrade results in failure. The computer that you use to upgrade 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

Note: If the upgrade fails, the upgrade process attempts to roll back all software to the previously installed version. The error is logged in the appliance logs, and the administrator is notified. You can consult the `/log` directory for further error information.

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 current processes being run on the appliance.
- Checks if there are any active NetBackup jobs. The upgrade process only proceeds if it is determined that no active jobs are detected.

Only after the required criteria is met, the appliance software is upgraded, and the appliance version is updated to the latest release update level.

Manage > Software Updates

Use the **Manage > Software Updates** tab to view and initiate the installation of a software upgrade on your appliance.

The Software Update page displays the following sections:

- **Downloaded Software Updates** - This section displays:
 - The current software version that is installed on your appliance.
 - The downloaded software updates (packages) that can be installed on your appliance
- **Online Software Updates** - This section displays the software updates available for downloading and then installing on your appliance.

[Table 3-27](#) displays the fields and buttons from the **Downloaded Software Updates** section.

Table 3-27 Downloaded Software Updates

Field name	Description
Available Software Update	Shows the name and the version of the appliance software updates that are already downloaded and available to install.

Table 3-27 Downloaded Software Updates (*continued*)

Field name	Description
Version	Shows the version of NetBackup Appliance software that is available for installation.
NetBackup Version	Shows the version of NetBackup software that is included with that version of the appliance software update.
Size	Shows the size of the software update to help you ensure that you have enough space on the appliance to accommodate the installation.
Details	Click Details to view additional information about the software update.
Install	<p>Selected a software update to install and click Install to start the upgrade process.</p> <p>Certain software updates may display pre-installation pop-up windows that require user inputs before you proceed further. You may be required to:</p> <ul style="list-style-type: none"> ■ Answer the questions that appear in each pop-up window. After all questions are answered, the server upgrade list is displayed with the names of the servers that you have selected to upgrade. ■ Click Next. When the Confirmation Required window appears, enter your user name and password. The upgrade process begins and the progress is shown in the NetBackup Appliance Web Console.
Delete	<p>If you determine that you do not need or want to install a downloaded software update, remove it from the list as follows:</p> <ul style="list-style-type: none"> ■ Click the radio box next to the downloaded software update that you want to delete. ■ Click Delete. <p>To obtain a software update that was deleted, download it again from the Online Software Updates table.</p>

Table 3-28 displays the fields and buttons from the **Online Software Updates** section. This table remains visible throughout the upgrade process.

Table 3-28 Online Software Updates

Field name	Description
Online Software Update	This column displays the version of the appliance software update that you can select to download to the appliance.
Version	Shows the version of NetBackup Appliance software that is available for installation.
Size	This column displays the version of NetBackup software that is included with the version of the appliance software that you can select to download.
Download Progress	This column displays the progress of the software download. For example, 2.2G/2.9G downloading.
Download	<p>After you have selected a software update version, click Download to start the download process.</p> <p>The table refreshes to show the status of the download. If you decide to cancel the download, click the red X next to the selected software update on the right side of the table.</p>

See [“Downloading and installing NetBackup appliance software from NetBackup Appliance Web Console”](#) on page 175.

See [“Guidelines to install a software update”](#) on page 171.

Downloading and installing NetBackup appliance software from NetBackup Appliance Web Console

This topic explains how to upgrade an appliance from the NetBackup Appliance Web Console. Before you begin the upgrade procedure, read the guidelines that pertain to the upgrade process.

To upgrade your appliance using the NetBackup Appliance Web Console

- 1 Log on to the appliance and open the NetBackup Appliance Web Console.
- 2 Select **Manage > Software Updates**.
- 3 From the **Software Updates** page determine if there are any software updates available for installation in the **Downloaded Software Updates** table.

- If the table contains the software update that you want to install, proceed to Step 4.
 - If the table does not contain a software update that you want to install, then you must first download the software update. From the **Online Software Updates** table on the page, select a software update and click **Download**. During the download operation, the progress and status of download is displayed in the **Download Progress** column. After the download process completes successfully, the software update is shown in the **Available Software Update** column of the **Downloaded Software Updates** table.
- 4 Select the check box that is associated with the software update that you want to install and click **Install**.

The following events occur after you click **Install**:

- The **Software Updates** page refreshes and presents a table that displays the server (master or media) that is to be upgraded. The table also shows the name and version of the software update.

Note: If you plan to upgrade more than one media server, you must run this upgrade procedure on each media server.

- An interactive, preinstallation check window appears. You must provide answers to the preinstallation questions. Then select **Finish** to exit the preinstallation check window.
- 5 Click **Next** on the **Downloaded Software Updates** table.
- 6 The **Confirm** pop-up window displays the server (master or media) that you are about to upgrade.

If this information is correct, click **Next**. If the information is not correct, click **Cancel**.

- 7 Clicking **Next** opens a **Confirmation Required** pop-up window. An administrator must enter a user name and password as a final step before the software installation or the upgrade begins. After you enter the user name and password, click **Confirm**. If you want to stop or exit the installation, click **Cancel**.

The **Software Updates** page refreshes and updates the information that is displayed in **Downloaded Software Updates** table. This table displays the progress (in percentage) and the status of the software installation.

Note: According to the requirement from the software update, the Web service may not be available during the upgrade process. See [the section called “Before you initiate a software upgrade process:”](#) on page 171. for more information.

- 8 After the status of the server reaches 100%, the information in the title line of the table clarifies whether the upgrade was successful. The following status can occur depending on whether the upgrade was successful or not:

- **The appliance version is <the target version> and not in upgrade state.** If the target version appears it indicates that the upgrade was successful. Click **Finish** to complete the process.

- **The appliance version is <the original version> and not in upgrade state.** If the original version appears it indicates a failed upgrade and an automatic rollback has taken place. The rollback returns the server back to the original version.

- **Failed to create the PRE_UPGRADE checkpoint, please resolve this issue first**

A checkpoint creation process is performed automatically before the upgrade operation begins. That checkpoint is used to enable the server to roll back to it, if the upgrade fails. If the failure message appears, it indicates that the creation of the checkpoint failed, and the upgrade operations were not performed. You must determine what caused the issue and resolve it before you can attempt the upgrade again.

- **Self-Test failed on <nodename >, please resolve the issue first.** The self-test operation is automatically executed before the upgrade operation begins. If the self-test operation fails, the upgrade process does not continue. If this issue occurs, you must attempt to resolve it before you continue.

- 9 Complete this step only if your backup environment includes SAN client computers.

The Fibre Channel (FC) ports must be rescanned to allow any SAN client computers to reconnect to the Fibre Transport (FT) devices. The rescan must be done from the NetBackup CLI view on the appliance.

To rescan the FC ports:

- Enter the following command to see a list of NetBackup user accounts:

```
Manage > NetBackupCLI > List
```

- Log in to this appliance as one of the listed NetBackup users.

- Run the following command to rescan the FC ports:

```
nbftconfig -rescanallclients
```

- If any SAN clients still do not work, run the following commands on each of those clients in the order as shown:

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
```

- If any SAN clients still do not work, you must manually initiate a SCSI device refresh at the OS level. The method to accomplish this depends on the operating system that the client is running. Once the refresh has completed, attempt the `nbftconfig -rescanallclients` command again.
- If any SAN clients still do not work, restart those clients.

Note: If you have any SLES 10 or SLES 11 SAN clients that still do not work, Symantec recommends that you upgrade the QLogic driver on those clients. For the affected SLES 10 clients, upgrade to version 8.04.00.06.10.3-K. For the affected SLES 11 clients, upgrade to version 8.04.00.06.11.1.

See [“Download software updates directly to the NetBackup appliance”](#) on page 179.

See [“Download software updates to the NetBackup appliance using client share”](#) on page 180.

See [“Installing NetBackup appliance software using the NetBackup Appliance Shell Menu”](#) on page 183.

Downloading NetBackup appliance software and client packages from the NetBackup Appliance Shell Menu

You can download NetBackup appliance software and client packages from the NetBackup Appliance Shell Menu using any of the following methods:

- [Download software updates directly to the NetBackup appliance](#)
- [Download software updates to the NetBackup appliance using client share](#)

Download software updates directly to the NetBackup appliance

This topic describes downloading the software release updates directly on to the NetBackup appliance.

To use this method, the appliance requires Internet access to download the files or packages from the Symantec Support website.

To download software release updates directly on to the NetBackup appliance:

- 1 Log on to the NetBackup Appliance Shell Menu as an administrator.
- 2 Enter the following command to determine if a software update is available from the Symantec Support website:

```
Main_Menu > Manage > Software > List AvailablePatch
```

- 3 Enter the appropriate command as follows to download a software update or a client package:

- For software updates:

```
Main_Menu > Manage > Software > Download
```

```
SYMC_NBAPP_update-<version>-<release>.x86_64.rpm
```

Where *<version>* is the version of software release and *<release>* is the software version release number.

- For a UNIX client package:

```
Main_Menu > Manage > Software > Download
```

```
SYMC_NBAPP_addon_nbclient_<platformname>-<version>-<release>.x86_64.rpm
```

Where *<platformname>* is the client platform or operating system name, *<version>* is the version of the client package, and *<release>* is the software version release number.

For example:

```
Main_Menu > Manage > Software > Download
```

```
SYMC_NBAPP_addon_nbclient_Solaris-7.6.0.2-SLES11.x86_64.rpm
```

- For a Windows client package:

```
Main_Menu > Manage > Software > Download
```

```
SYMC_NBAPP_addon_nbwin_<platformname>-<version>-<release>.x86_64.rpm
```

Where *<platformname>* is the client platform or operating system name, *<version>* is the version of the client package, and *<release>* is the software version release number.

For example:

```
Main_Menu > Manage > Software > Download
SYMC_NBAPP_addon_nbwin-7.6.0.2-SLES11.x86_64.rpm
```

- 4 Enter the following command to verify that the rpm is downloaded successfully.

```
Main_Menu > Manage > List Downloaded
```

Download software updates to the NetBackup appliance using client share

This topic describes downloading the software release updates or client packages to a NetBackup appliance using a client share method.

Note: If downloading the software updates directly to the NetBackup appliance fails, you may use this method to download the appliance software release update or client package on your appliance

Perform this method from a computer that is connected to the appliance and that also has Internet access. Internet access is needed to download the files or packages from the Symantec Support website to the appliance.

To download software release updates or client packages to a NetBackup appliance using a client share method:

- 1 Log on to the NetBackup Appliance Shell Menu as an administrator.
- 2 Enter the following command to open the NFS and the CIFS shares:

```
Main_Menu > Manage > Software > Share Open
```

- 3 Map or mount the appliance share directory as follows:

Windows systems

Map the following appliance CIFS share on your computer:

UNIX systems

Mount the following appliance NFS share:

- `mkdir -p /mount/<appliance-name>`
- `mount`
`<appliance-name>:/inst/patch/incoming`
`/mount/<appliance-name>`

On Windows systems, you are prompted to provide the user name (`admin`) and its corresponding password.

- 4 To download the release updates, enter the following URL to go to the Symantec Support site where the release update and client packages are posted:

`http://www.symantec.com/business/support/index?page=landing&key=58991`

- 5 Download and unzip or untar the release update or the client package as follows:

- For release updates

The release update `.rpm` file name may be split into multiple files with names. The following example demonstrates a software update file that is split into three files:

```
NB_Appliance_N_<version>-<release>.x86_64-tar-split.1of3
NB_Appliance_N_<version>-<release>.x86_64-tar-split.2of3
NB_Appliance_N_<version>-<release>.x86_64-tar-split.3of3
```

Where `<version>` is the version of software release and `<release>` is the software version release number.

To continue with release update downloading, go to step 6.

- For client packages

Client packages are not split and use the following naming convention:

```
SYMC_NBAPP_addon_nbwin_<version>.x86_64.rpm OR
SYMC_NBAPP_addon_nbclient_<platform and version>.x86_64.rpm
```

Where `<platform and version>` is the specific platform operating system and the NetBackup version of the client package. For example:

```
SYMC_NBAPP_addon_nbclient_HP-UX-IA64-7.6.0.2-SLES11.x86_64.rpm
```

To continue with client package downloading, go to step 8.

- 6 Use one of the following commands to join (and extract) the release update `.rpm` files:

- For Windows, use a `copy /b` command similar to the following to join three split files:

```
copy /b NB_Appliance_N_<version>-<release>.x86_64-tar-split.1of3+
NB_Appliance_N_<version>-<release>.x86_64-tar-split.2of3+
NB_Appliance_N_<version>-<release>.x86_64-tar-split.3of3+
NB_Appliance_N_<version>-<release>.tar
```

Note: This command is one string. Make sure that it contains no spaces when you enter it. In addition, `<version>` is the version of software release and `<release>` is the software version release number.

Use Windows WinRAR utilities to uncompress the resulting `.tar` file, `NB_Appliance_N_<version>-<release>.tar`.

The resulting files are:

```
SYMC_NBAPP_update-<version>-<release>.x86_64.rpm
update.rpm.md5_checksum
```

- For UNIX, use a `cat` command similar to join three split files:

```
cat NB_Appliance_N_<version>-<release>.x86_64-tar-split.1of3<space>
  NB_Appliance_N_<version>-<release>.x86_64-tar-split.2of3<space>
  NB_Appliance_N_<version>-<release>.x86_64-tar-split.3of3 | tar xvf -
```

Note: This command is one string. In the example, there is one space between each package that is identified with, "`<space>`". In addition, `<version>` is the version of software release and `<release>` is the software version release number.

Resulting files from the preceding command:

```
SYMC_NBAPP_update-<version>-<release>.x86_64.rpm
update.rpm.md5_checksum
```

Note: Symantec recommends that you use GNU tar version 1.16 or higher instead of tar to extract packages on UNIX systems. See the following Technote for more information about extracting images.

<http://www.symantec.com/docs/TECH154080>

7 Compute the md5 checksum value for the

`SYMC_NBAPP_update-<version>-<release>.x86_64.rpm` as follows:

- For Windows systems:

To compute the md5 checksum, click on the following link for details:

<http://support.microsoft.com/kb/889768>

- For UNIX systems, run the following command:

```
md5sum SYMC_NBAPP_update-<version>-<release>.x86_64.rpm
```

Verify that the checksum value matches the content of the `update.rpm.md5_checksum` file.

- 8 Copy this release update or client package `.rpm` 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.

- 9 After you have successfully copied the release update or client package `.rpm` into the mounted share, unmap or unmount the shared directory.
- 10 From 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 run the `Share Close` command, 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`

- 11 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.

Installing NetBackup appliance software using the NetBackup Appliance Shell Menu

After you have downloaded a software update to the appliance, it can be installed from the NetBackup Appliance Shell Menu using this procedure. If you perform an upgrade from the NetBackup Appliance Shell Menu, the NetBackup Appliance Web Console is still available for use during the upgrade operation.

[Table 3-29](#) displays command options from the `Software > List` commands that let you view, verify, and check the details of the available software release updates.

Table 3-29 Manage > Software > List command options

Command name	Description
Main_Menu > Manage > Software > List AddOns	Lists software add-ons that are installed on the appliance.
Main_Menu > Manage > Software > List AvailablePatch	Checks the Symantec site for any software updates that are available.
Main_Menu > Manage > Software > List Details All	Lists all the software release updates that were applied to your appliance during the factory installation.
Main_Menu > Manage > Software > List Details Base	Lists all the software release updates that were applied to your appliance during the factory installation.
Main_Menu > Manage > Software > List Downloaded	Lists the detailed information of a downloaded software update.
Main_Menu > Manage > Software > List EEBs	Shows a detailed listing of all of the factory-installed Emergency Engineering Binaries (EEBs).
Main_Menu > Manage > Software > List Version	Displays the software version that is currently installed on your appliance.

To install a software update that has been downloaded to the appliance using the NetBackup Appliance Shell Menu

- 1 Log on to the NetBackup Appliance Shell Menu and run the following command to install the software release update.

```
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 matches the update name that was downloaded on the appliance.

- 2 Watch the onscreen progress of the upgrade to see an estimated completion time. To see the current status of the upgrade, enter the following command:

```
Main_Menu > Manage > Software > UpgradeStatus
```

Note: This command is available only for upgrades from version 2.6.0.1 and later and cannot be used for upgrades from 2.5.x.

- 3 The upgrade may force the appliance to restart several times. After the upgrade has completed and 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.

- 4 Complete this step only if your backup environment includes SAN client computers.

The Fibre Channel (FC) ports must be rescanned to allow any SAN client computers to reconnect to the Fibre Transport (FT) devices. The rescan must be done from the NetBackup CLI view on the appliance.

To rescan the FC ports:

- Enter the following command to see a list of NetBackup user accounts:

```
Manage > NetBackupCLI > List
```

- Log in to this appliance as one of the listed NetBackup users.

- Run the following command to rescan the FC ports:

```
nbftconfig -rescanallclients
```

- If any SAN clients still do not work, run the following commands on each of those clients in the order as shown:

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
```

- If any SAN clients still do not work, manually initiate a SCSI device refresh at the OS level. The refresh method depends on the operating system of the client. Once the refresh has completed, attempt the `nbftconfig -rescanallclients` command again.
- If any SAN clients still do not work, restart those clients.

Note: If you have SLES 10 or SLES 11 SAN clients that still do not work, Symantec recommends upgrading the QLogic driver on those clients. For the affected SLES 10 clients, upgrade to version 8.04.00.06.10.3-K. For the affected SLES 11 clients, upgrade to version 8.04.00.06.11.1.

Appliance servers to upgrade

After you click **Install** to install a software update, the **Manage > Software Updates** page refreshes and displays the following tables:

- **Install Software Update**
This table displays the servers that are to be upgraded with the software update that you selected to install.
- **Online Software Updates Available**
This table remains visible throughout the upgrade process. It shows the available software updates that are applicable to your appliance that you can download.

Table 3-30 Servers identified for the software update

Field name	Description
Server	The name of the server that is currently configured in your master server environment. In a cluster configuration, multiple media servers are displayed.
Software Update Name	The name of the software update that you have selected for installation.
Software Update Version	The new version of the appliance software on the server after the software is updated successfully.
Next	<p>Click Next to continue with the upgrade process after selecting the servers to upgrade. After you click Next, a pop-up window appears that lists the selected servers.</p> <p>To continue, do the following:</p> <ul style="list-style-type: none"> ■ Confirm that the server upgrade list is correct. ■ When the Confirmation Required window appears, enter your user name and password. That is the final confirmation step before the upgrade operation begins.
Cancel	<p>Click Cancel to cancel or exit the upgrade process.</p> <p>The Next and Cancel buttons are located on the top-right corner of the table.</p>

See [“Software Updates Installation Status”](#) on page 187.

See [“Manage > Software Updates”](#) on page 173.

Software Updates Installation Status

After you enter your user name and password and click **Confirm** to confirm the software installation, the **Manage > Software Updates** page refreshes and displays the following two tables:

- **Install Software Update**
This table lets you view the progress and the status of the software installation as it applies to each server that you selected to upgrade.
After the upgrade has completed on all servers, click **Finish**.
- **Online Software Updates Available**
This table remains visible throughout the upgrade process. It shows the available software updates that are applicable to your appliance that you can download.
See [“Manage > Software Updates”](#) on page 173.

[Table 3-31](#) describes the information about the installation status of the software update.

Table 3-31 Software update installation status

Field name	Description
Server	The servers that were selected for the software update installation.
Status	Displays whether each server is online or offline.
Installation Progress	Shows the progress (in percent) of installation and for each server. For example, "15%".
Installation Status	Displays the status of the installation. For example, "The appliance is running self-test on <i><applianceName></i> ...".

Note: The installation of the software update requires the NetBackup Appliance Web Console temporarily owing to the upgrade of certain web console components. To monitor the installation status, log on to the NetBackup Appliance Shell Menu and run the `Manage > Software > UpgradeStatus` command.

See [“Appliance servers to upgrade”](#) on page 186.

See [“Manage > Software Updates”](#) on page 173.

About installing an EEB

Emergency engineering binaries are provided to customer on an individual basis to meet specific needs for that customer. If you have one or more EEBs that you want to install you should store them locally so that you can upload them to the appliance using the NetBackup Appliance Shell Menu.

See [“Installing an EEB”](#) on page 188.

Installing an EEB

You install an emergency engineering binary (EEB) the same way as you would install a software update. You can use the appliance shell menu to install an EEB on an appliance. When you install an EEB you must be logged into the appliance where you intend to install the binary. You should also contact Symantec Technical Support to obtain the EEB that you need to install and store it locally on your computer. In addition, If you have multiple EEBs to install, you can only install one EEB at a time.

To install an EEB using the NetBackup Appliance Web Console, refer to the following section.

To upload and install an appliance emergency engineering binary using the NetBackup Appliance Shell Menu

- 1 You should perform this procedure from a computer that is connected to the appliance as well as to the Internet.
- 2 Open an SSH session and log on to the appliance as an administrator.
- 3 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:

UNIX systems

Mount the following appliance NFS share:

`<appliance-name>:/inst/patch/incoming`

Note that on Windows systems, you are prompted to provide the user name, `admin`, and its corresponding password.

- 5 Copy the EEB from your local computer to this mapped directory.
You should have already obtained the EEB from Symantec Technical Support.
- 6 Unmap or unmount the directory after you have successfully downloaded the EEB.

- 7 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 in Step 3, 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.

- 8 Enter the following command to list the EEBs that are available for downloading

```
Main_Menu > Manage > Software > List Downloaded
```

- 9 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 [“About installing an EEB”](#) on page 188.

About installing NetBackup Administration Console and client software

You can use two different methods to install the NetBackup client software on the clients that you want to backup. You can install NetBackup client software on clients as follows:

- Use CIFS and NFS shares and run scripts to install the software silently. Depending on the operating system, you run the `quickinstall.exe` script or the `unix-client-install` script. This is a silent install. The scripts do not prompt you for any user-related questions. They automatically update the NetBackup configuration on client with the appliance server name as the Master server.
- Select a link on the appliance login page to download the packages and install the software.

On the appliance login page, you can click on the **Software** link to download a package that contains the NetBackup Administration Console and the NetBackup client software.

You can also elect to download and install the NetBackup Administration Console. To download and install the client software, you perform the following functions:

- Choose the client type that you want to install.
- Select the software package to download.
- Unzip or untar the package.
- Run the install (UNIX) or setup.exe (Windows) script.
- Update the NetBackup configuration on client with the Master Server information (for example, `bp.conf` on UNIX systems).

See [“Installing NetBackup client software through CIFS and NFS shares”](#) on page 190.

Installing NetBackup client software through CIFS and NFS shares

After all appliance configuration has been completed, you can use the following procedures to install Windows and UNIX client software on the clients that are used with your NetBackup appliances. These procedures explain how to obtain the software packages through a CIFS or an NFS share.

Note: If you have existing NetBackup clients that you want to use with the appliance master server, they must be version 6.0 or later. For these clients, you only need to add the appliance master server name to the client.

NetBackup Windows client software installation through a CIFS share

To install NetBackup client software on a Windows client through a CIFS share

- 1 On the appliance where the client software resides, log in to the NetBackup Appliance Shell Menu with your administrator credentials.
- 2 Open the CIFS share using the following command:

```
Main > Settings > Share ClientInstall Open
```

- 3 On the Windows client computer where you want to install the NetBackup client software, log on as the administrator.
- 4 Open a map or a directory to the following CIFS shared folder on the appliance:

```
\\<appliance_name>\install
```

- 5 Click on the Windows executable, **quickinstall.exe**.

This action installs the NetBackup client software and adds the appliance master server name on the client.

- 6 On the appliance, close the shared directory using the following command:

```
Main > Settings > Share ClientInstall Close
```

NetBackup UNIX client software installation through an NFS share

To install NetBackup client software on a UNIX client through an NFS share

- 1 On the appliance where the client software resides, log in to the NetBackup Appliance Shell Menu with your administrator credentials.

- 2 Open the NFS share using the following command:

```
Main > Settings > Share ClientInstall Open
```

- 3 On the UNIX client computer where you want to install the NetBackup client software, log on as root.

- 4 Mount the following NFS share:

```
<appliance_name>:/inst/client
```

- 5 Browse the files within the NFS share directory. Files that are similar to the following appear:

.packages	clientconfig	quickinstall.exe
PC_Cln	docs	unix-client-install

- 6 Run the `unix-client-install` script.

This action installs the NetBackup client software.

- 7 Add the appliance master server name to the `bp.conf` file on the client as follows:

- On the client, navigate to the following location:

```
cd /usr/opensv/netbackup
```

- Enter `ls` to see the contents of the directory.

- Open the `bp.conf` file in a text editor.

- Enter the fully qualified host name of the appliance master server.

- Save your changes and close the file.

8 On the appliance, close the shared directory using the following command:

```
Main > Settings > Share ClientInstall Close
```

See “[About installing NetBackup Administration Console and client software](#)” on page 189.

See “[Downloading NetBackup client packages to a client from a NetBackup appliance](#)” on page 192.

Downloading NetBackup client packages to a client from a NetBackup appliance

You can download NetBackup client software from a NetBackup appliance to any client that you want to back up. The NetBackup Appliance Web Console logon page provides a **Download Packages** section to download the client packages.

The packages are listed by operating system type in a drop-down box as follows:

- All
- Windows
- Linux
- Solaris
- AIX
- HP
- BSD
- Mac OS
- VMware vCenter Plug-in

Note: If you download Linux, UNIX, Solaris, AIX, or BSD packages, Symantec recommends GNU tar version 1.16 or higher to extract the .tar packages.

For more information, see the following Technote on the Symantec Support website:

<http://www.symantec.com/docs/TECH154080>

In addition to the downloading instructions, this procedure also includes the steps to extract and install the downloaded files on to the client.

To download NetBackup client packages from a NetBackup appliance to a client

- 1 Log in to the client that you want to back up.
- 2 Open a browser window and enter the appliance URL.
- 3 In the middle of the landing page, in the section **Download Packages**, click on the drop-down box to see the list of packages.
- 4 Right-click the selected package and specify the location to download it onto the client.

Example locations are as follows:

- On Windows platforms, download the package to `C:\temp` or to the desktop. To determine the type of hardware on your Windows system, right-click **My Computer** and select **Properties**.
- On Linux or UNIX platforms, download the package to `/tmp`.

Note: If the message **No packages found** appears after you make a selection, that client package is not currently installed on the appliance. Refer to the following topic to download client packages on to the appliance:

- 5 Unzip or untar the package.
- 6 Install the client software as follows:
 - Windows systems
Click the **setup.exe** file.
 - UNIX systems
Run the `.install` script.
- 7 After you have successfully installed the client software, add the appliance master server name to the client as follows:

Windows systems

- After NetBackup has been installed on the client, open the Backup, Archive, and Restore interface.
Start > All Programs > Symantec NetBackup > Backup, Archive, and Restore
- From the Backup, Archive, and Restore interface, select **File > Specify NetBackup Machines and Policy Type...**
- From the **Specify NetBackup Machines and Policy Type** dialog, enter the server name in the field **Server to use for backups and restores**. Then click **Edit Server List** and click **OK**.
- In the dialog box that appears, enter the fully qualified host name of the appliance master server and click **OK**.
- Close the Backup, Archive, and Restore interface.
- Restart the NetBackup Client Services by opening a Windows Command prompt. Then, enter `services.msc` and press **Enter**.

UNIX systems

- On the client, navigate to the following location:
`cd /usr/opensv/netbackup`
- Enter `ls` to see the contents of the directory.
- Open the `bp.conf` file in a text editor.
- Enter the fully qualified host name of the appliance master server.
- Save the changes and close the file.

See [“Installing NetBackup client software through CIFS and NFS shares”](#) on page 190.

See [“Downloading the NetBackup Administration Console to a Windows computer from a NetBackup appliance”](#) on page 194.

Downloading the NetBackup Administration Console to a Windows computer from a NetBackup appliance

You can download the NetBackup Administration Console software from a NetBackup appliance to a Windows computer that you want to use to access the appliance. The Windows computer does not require NetBackup installation to use the administration console. The logon page of the NetBackup Appliance Web Console provides a **Download Packages** section to download the NetBackup Administration Console package.

In addition to the downloading instructions, this procedure also includes the steps to extract and install the downloaded files on to the client.

To download the NetBackup Administration Console package from a NetBackup appliance to a Windows computer

- 1 Log into the Windows computer that you want to use for appliance access.
- 2 Open a browser window and enter the appliance URL.
- 3 In the middle of the landing page, in the section **Download Packages**, click on the drop-down box and select **Windows**.
- 4 When the package file name appears under the drop-down box, right-click on it and select either **Download Linked File** or **Download Linked File As**, then specify the location to download the package onto the Windows computer.

For example, download the package to `C:\temp` or to the desktop.

- 5 Unzip the package.
- 6 Install the administration console software as follows:
 - On the client, navigate to the `Addons/JavaInstallFiles` directory.
 - Click on the **setup.exe** file.

See [“Downloading NetBackup client packages to a client from a NetBackup appliance”](#) on page 192.

See [“Installing NetBackup client software through CIFS and NFS shares”](#) on page 190.

Troubleshooting the NetBackup-Java Administration Console on a non-English Windows system

If you install the NetBackup-Java Administration Console on a non-English Windows system to administer the NetBackup server inside a NetBackup appliance, the console can hang when you attempt to log in to the NetBackup server. To avoid this issue, use the following workaround:

- Modify the `install_path\Java\setconf.bat` file on the Windows system where the NetBackup-Java Administration Console is installed and set the `NBJAVA_FILE_ENCODING` parameter with the proper encoding. Use the same encoding as you previously set on the appliance system with the `SystemLocale` command.

To determine the coding name, refer to the Canonical Name for `java.nio` API and `java.lang` API column in the Supported Encodings document on the following website:

[Oracle Supported Encodings Documentation](#)

For example, if you set a UTF-8 locale like `zh_CN.utf8` or `ja_JP.utf8` on your appliance system, the canonical name for `java.nio` API and `java.lang` API is UTF8. Uncomment the `SET NBJAVA_FILE_ENCODING` parameter in the `install_path\Java\setconf.bat` file, and specify UTF8 (in this example) as follows: `REM SET NBJAVA_FILE_ENCODING=` becomes: `SET NBJAVA_FILD_ENCODING=UTF8`

For more information on the `SystemLocale` command, refer to the following section:

See [“About the NetBackup Appliance Web Console login page”](#) on page 24.

You can also find this information in the *Symantec NetBackup Appliance Command Reference Guide*.

Manage > Additional Servers

From the **Manage > Additional Servers** page you can add or delete additional servers. This tab lets you add an entry to the NetBackup `bp.conf` file. The `bp.conf` file allows communication to occur between the appliance and the Windows NetBackup Administration Console, so you can manage your appliance through that console. You must add the host name of a media server to the additional servers before configuring the media server.

See [“Managing additional servers to the appliance”](#) on page 196.

Managing additional servers to the appliance

The following procedures enable you to add or delete servers from the **Additional Servers** page on the NetBackup Appliance Web Console.

Use the following procedure to add additional servers to the appliance.

To add an additional server:

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Manage > Additional Servers**.
- 3 Click the **Add** button.

The **Add Additional Server** dialog box is displayed.

- 4 In the **Server Name** field, enter the name of the server that you want to add, and then click **OK**.

Note: You can add multiple server name entries separated using a comma(.).

The appliance displays the following message:

```
Additional server(s) added successfully.
```

- 5 Click **Cancel** to exit the **Add Additional Server** dialog box.

Use the following procedure to delete servers from the appliance.

To delete an additional server

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Manage > Additional Servers**.

The **Additional Servers** page displays a list of all the additional servers added to your appliance.

- 3 Select the check box against the server that you want to delete, and then click the **Delete** button.
- 4 The following warning is displayed:

```
Are you sure you want to proceed?
```

- 5 Click **Yes** to delete the selected server. The following message is displayed:

```
Additional server(s) deleted successfully.
```

- 6 To delete all the servers from the appliance, select the **Server Name** check box, and click **Delete**.

See [“Manage > Additional Servers”](#) on page 196.

Manage > Certificates

Use the **Manage > Certificates** page to generate a new certificate from the NetBackup Appliance Web Console. 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 appliance supports the generation of the following certificate types:

- vCenter

■ SCVMM

To generate the certificates for your client

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Go to the **Manage > Certificates** page.
- 3 In the **Client Hostname** text box, enter the client hostname.
- 4 Click **Generate**.

The certificate `<hostname>.zip` has been generated and downloaded to the local directory that you selected.

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 [“Manage > Additional Servers”](#) on page 196.

Managing NetBackup appliance using the NetBackup Appliance Shell Menu

This chapter includes the following topics:

- [Expanding the bandwidth on the NetBackup appliance](#)
- [About configuring the maximum transmission unit size](#)
- [About OpenStorage plugin installation](#)
- [About mounting a remote NFS](#)
- [About running NetBackup commands from the appliance](#)
- [About Auto Image Replication between appliances](#)

Expanding the bandwidth on the NetBackup appliance

The NetBackup 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. Link aggregation is enabled by default when you perform the initial network configuration from the NetBackup Appliance Web Console or the NetBackup Appliance Shell Menu.

You can use the NetBackup 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

About configuring the maximum transmission unit size

The MTU property controls the maximum transmission unit size for an Ethernet frame. The standard maximum transmission unit size for Ethernet is 1500 bytes (without headers). In supported environments, the MTU property can be set to larger values up to 9000 bytes. Setting a larger frame size on an interface is commonly referred to as using jumbo frames. Jumbo frames help reduce fragmentation as data is sent over the network and in some cases, can also provide better throughput and reduced CPU usage. To take advantage of jumbo frames, the Ethernet cards, drivers, and switching must all support jumbo frames. Additionally, each server interface that is used to transfer data to the appliance must be configured for jumbo frames.

Symantec recommends that if you configure the MTU property of an interface to values larger than 1500 bytes, make sure that all systems that are connected to the appliance on the specific interface have the same maximum transmission unit size. Such systems include but are not limited to NetBackup clients and remote desktops. Also verify the network hardware, OS, and driver support on all systems before you configure the MTU property.

You can configure the MTU property for an interface by using the `SetProperty` command in the NetBackup Appliance Shell Menu.

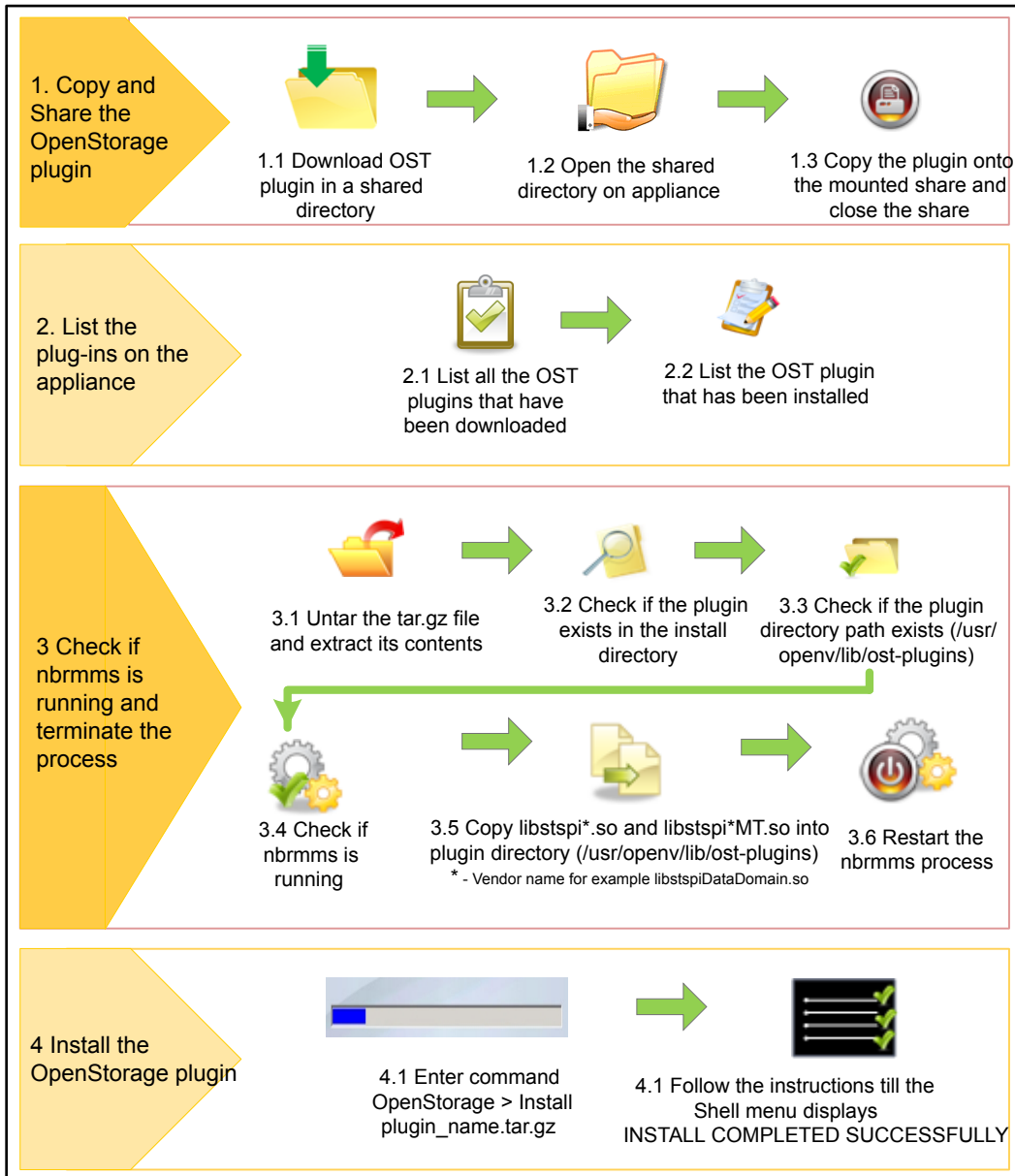
See the `SetProperty` command in the *Symantec NetBackup Appliance Command Reference Guide*.

About OpenStorage plugin installation

You can install and open an OpenStorage (OST) plugin on the **NetBackup Appliance** using the NetBackup 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 4-1 OpenStorage plugin installation process



See “Installing OpenStorage plugin” on page 202.

See “Uninstalling OpenStorage plugin” on page 203.

For more information about `Main > Manage > OpenStorage` commands refer to *NetBackup™ Appliance Command Reference Guide*.

Installing OpenStorage plugin

The following procedure describes how to install the OpenStorage (OST) plugin through the NetBackup Appliance Shell Menu.

To install the OpenStorage plugin

- 1 Log on to the NetBackup 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\incoming_plugins
and the NFS share nbappphostname:/inst/plugin/incoming
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 master appliances.

The appliance initiates the installation process as displayed in the following example:

```
Welcome to the installation of plugin_name.tar.gz
- [Info] Checking if upgrade is running from the console...failed

WARNING: Symantec recommends that this upgrade is run from
the appliance console.
>> Are you sure you want to continue? (yes/no)                yes
- [Info] Extracting the contents of the tar file                ok
- [Info] Terminating the nbrmms process before proceeding
  with the installation.                                       ok
- [Info] Executing the install script
- [Info] Install script exited successfully!
- [Info] Restarting nbrmms                                     ok
- Successfully installed the plugin plugin_name.tar.gz
```

See [“About OpenStorage plugin installation”](#) on page 200.

See [“Uninstalling OpenStorage plugin”](#) on page 203.

Uninstalling 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 master 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 200.

See [“Installing OpenStorage plugin”](#) on page 202.

About mounting a remote NFS

You can use the NetBackup Appliance Shell Menu, to mount a remote Network File System (NFS) onto the appliance server. You can now mount NFS using a simpler interface through the `Manage > MountPoints` menu. To work with the NFS drive, you can use the following commands in the NetBackup Appliance Shell Menu.

Table 4-1 Commands to work with NFS drive

Command	Descriptions
Mount	Use the <code>Mount</code> command to mount an NFS drive.

Table 4-1 Commands to work with NFS drive *(continued)*

Command	Descriptions
List	Use the <code>List</code> command to list all the existing mount points on your appliance.
Unmount	Use the <code>Unmount</code> command to un-mount a previously mounted NFS drive.

See [“Mounting an NFS remote drive”](#) on page 205.

See [“Unmounting an NFS drive”](#) on page 207.

In certain circumstances, you may find that a NetBackup Appliance NFS share is not accessible. If this issue occurs, use the NetBackup 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.

For more information about `Main > Manage > MountPoints` commands refer to *NetBackup™ Appliance Command Reference Guide*

Mounting an NFS remote drive

This procedure describes how to mount your remote NFS drive.

To mount an NFS remove drive

- 1 Log in to the NetBackup Appliance Shell Menu using your administrator's credentials.

- 2 Type the `Main > Manage> MountPoints`

The appliance lists all the commands under in the `MountPoints` menu.

- 3 To mount your remote NFS drive, type the following command:

- 4 `Mount RemotePath MountPoint [FileSystemType] [options]`

This command includes the following parameters:

	<i>RemotePath</i>	<i>MountPoint</i>	[<i>FileSystemType</i>]	[<i>Options</i>]
Description	Provide the address of a device or a directory to be mounted on to your appliance.	Provide the name of the directory where the NFS drive should be mounted. Note: An error is displayed in case of the following situations: <ul style="list-style-type: none">■ If the directory name is incorrect.■ If the directory with given name does not exist, a directory is created.■ If the directory with given name is already mounted at a mount point.	Specify the type of the device to be mounted.	Specify any additional options to be passed to the appliance along with the <code>Mount</code> command.
Format	<code>HOST:DIRECTORY</code>	The directory name must start with <code>/</code> and must have the correct directory name.		You can only use options specific for mounting the NFS drive.
Parameter type	Mandatory	Mandatory	Optional	Optional
Example	<code>suryan. engba. symantec.com :/build1</code>	<code>/mymounts/moun1</code>	<code>NFSv3</code> or any other supported type by the underlying <code>Mount</code> command.	<code>ro</code> is used to mount the device as read only.

5 The appliance mounts your remote NFS drive.

Note: If you mount a remote share and then restart the appliance, the mount is re-established on the next boot. The mount points are persistent across all the restart and there is no exception to this rule.

To list and view the mounted devices

- 1 Log in to the NetBackup Appliance Shell Menu using your administrator credentials.

- 2 Type the `Main > Manage > MountPoints`

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 Appliance NFS share is not accessible. If this issue occurs, use the NetBackup 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 [“About mounting a remote NFS”](#) on page 204.

Unmounting an NFS drive

This procedure describes how to unmount an NFS drive.

To unmount an NFS drive

- 1 Log in to the NetBackup Appliance Shell Menu using your administrator credentials.

- 2 Type the `Main > Manage > MountPoints`

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: <ul style="list-style-type: none">■ 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	<i>/mymounts/moun1</i>	

- 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 [“About mounting a remote NFS”](#) on page 204.
- See [“About mounting a remote NFS”](#) on page 204.

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 Appliance administrators can provide access for multiple NetBackup administrators and audit the activity of these administrators. In addition, NetBackup Appliance administrators can manage the NetBackup administrator accounts from the `Main > Manage > NetBackupCLI` view within the NetBackup Appliance Shell Menu. From the `NetBackupCLI` view, a NetBackup Appliance administrator can

create, delete, and list NetBackup administrator accounts as well as manage their user account passwords.

See [“About NetBackup administrator capabilities”](#) on page 209.

See [“Creating NetBackup administrator user accounts ”](#) on page 214.

See [“Managing NetBackup administrator user account passwords”](#) on page 216.

See [“Auditing NetBackup Administrator accounts”](#) on page 217.

See [“Deleting NetBackup administrator user accounts ”](#) on page 217.

See [“Viewing NetBackup administrator user accounts”](#) on page 218.

About NetBackup administrator capabilities

NetBackup administrators have superuser privileges and share a common home directory within a restricted shell. From this restricted shell, the NetBackup administrators can do the following:

- Use a base command name, an absolute or a relative path, or a shell script as a way to execute NetBackup commands.
- Have full NetBackup logging capabilities.

The following list shows the NetBackup commands that a NetBackup administrator can run with superuser privileges and the directories that contain the NetBackup commands.

- `/usr/opensv/netbackup/bin/*`
- `/usr/opensv/netbackup/bin/admincmd/*`
- `/usr/opensv/netbackup/bin/goodies/*`
- `/usr/opensv/volmgr/bin/*`
- `/usr/opensv/volmgr/bin/goodies/*`
- `/usr/opensv/pdde/pdag/bin/mtstrmd`
- `/usr/opensv/pdde/pdag/bin/pdcfg`
- `/usr/opensv/pdde/pdag/bin/pdusercfg`
- `/usr/opensv/pdde/pdconfigure/pdde`
- `/usr/opensv/pdde/pdcr/bin/*`

Note: Because there are NetBackup commands on a NetBackup appliance, it is possible that some of the command arguments are not supported.

The following list shows the commands and scripts that you cannot run from the directories:

- Library files - The files that end with the `.so` or `.so64` extensions.
- Notify scripts - Scripts that contain `notify` string within the file name.
- File list files - The files that end with the `.filelist` extension.

See [“About running NetBackup commands from the appliance”](#) on page 208.

See [“About running NetBackup commands”](#) on page 210.

See [“Creating NetBackup administrator user accounts ”](#) on page 214.

See [“Deleting NetBackup administrator user accounts ”](#) on page 217.

See [“Viewing NetBackup administrator user accounts”](#) on page 218.

About running NetBackup commands

NetBackup administrators can use multiple methods to execute NetBackup commands from the restricted NetBackup 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 Appliance shell:

- Using a base command name. For example,
 - `# bpps`
 - `# nbemmcmd -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/nbemmcmd -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 [“About creating a NetBackup touch file”](#) on page 211.

See [“About operating systems commands”](#) on page 213.

See [“About best practices”](#) on page 213.

See [“About known limitations”](#) on page 214.

About creating a NetBackup touch file

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/lib/ost-plugins`
- `/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 [“About running NetBackup commands”](#) on page 210.

See [“About operating systems commands”](#) on page 213.

See [“About best practices”](#) on page 213.

See [“About known limitations”](#) on page 214.

Loading the NetBackup notify scripts

The `cp-nbu-notify` utility is similar to `cp-nbu-config` utility that is added to the NetBackup Appliance to modify the NetBackup notify scripts, like the `start` and `exit` notification scripts to be run after each job.

The NetBackup CLI users can modify the notify scripts from the following script locations:

- /usr/opensv/netbackup/bin
- /usr/opensv/volmgr/bin

Note: The `cp-nbu-notify` assumes that the notify script pre-exists either in the actual location as a sample file or its goodies directory as a template. If a sample or template notify script does not exist in these directories, then the script that you may try to load is not considered valid.

To install or edit the notify scripts:

- 1 Login to the appliance as a NetBackupCLI user and then create the notify script in the home directory.
- 2 Enter `cp-nbu-notify` command to install the script:

```
cp-nbu-notify <notify-script>
```

The appliance displays the following messages:

```
NetBackup Appliance admin must review and
approve this operation.
Enter admin password:
```

- 3 When the command prompts for admin password, enter the Appliance admin password (not the NetBackupCLI password). The password is needed for security purpose to make sure that the notify script is approved by the Appliance admin.

When the password is successfully verified the notify script is automatically loaded in the right location.

Note: The source notify script must exist in the home directory or its subdirectory.

Caution: You can only copy the notify scripts. Not any other scripts in the NetBackup install path. Execution of any external script through the notify script can lead to a security issue.

About operating systems commands

The following rules apply to the operating system commands:

- The following commands were available in the previous releases are still 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 [“About running NetBackup commands”](#) on page 210.

See [“About creating a NetBackup touch file”](#) on page 211.

See [“About best practices”](#) on page 213.

See [“About known limitations”](#) on page 214.

About best practices

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 `${bpps}`.
`bpps="sudo /usr/opensv/netbackup/bin/bpps"`
 - The following command enables you to use the variable `${nbemmcmd}`.
`nbemmcmd="sudo /usr/opensv/netbackup/bin/admincmd/nbemmcmd"`

- 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 “[About running NetBackup commands](#)” on page 210.

See “[About operating systems commands](#)” on page 213.

See “[About best practices](#)” on page 213.

See “[About known limitations](#)” on page 214.

About known limitations

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 “[About running NetBackup commands](#)” on page 210.

See “[About creating a NetBackup touch file](#)” on page 211.

See “[About operating systems commands](#)” on page 213.

See “[About best practices](#)” on page 213.

Creating NetBackup administrator user accounts

NetBackup 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.

Symantec 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 the *NetBackup Appliance Command Reference Guide* for additional information about this command and its use.

See [“About running NetBackup commands from the appliance”](#) on page 208.

See [“About NetBackup administrator capabilities”](#) on page 209.

See [“Managing NetBackup administrator user account passwords”](#) on page 216.

See [“Auditing NetBackup Administrator accounts”](#) on page 217.

See [“Deleting NetBackup administrator user accounts ”](#) on page 217.

See [“Viewing NetBackup administrator user accounts”](#) on page 218.

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 NetBackup administrator capabilities”](#) on page 209.

See [“Creating NetBackup administrator user accounts ”](#) on page 214.

See [“Managing NetBackup administrator user account passwords”](#) on page 216.

See [“Auditing NetBackup Administrator accounts”](#) on page 217.

See [“Deleting NetBackup administrator user accounts”](#) on page 217.

See [“Viewing NetBackup administrator user accounts”](#) on page 218.

Managing NetBackup administrator user account passwords

After the NetBackup Appliance administrator has created a NetBackup administrator account, the appliance administrator can manage the password of that account through the NetBackup Appliance Shell Menu.

[Table 4-2](#) describes the functions that you can perform as you manage your account passwords.

Table 4-2 Managing NetBackup administrator user account passwords

Function	Command
The NetBackup Appliance administrator can specify a maximum number of days that a password is valid for a user or users.	<pre>Main > Manage > NetBackupCLI > PasswordExpiry Age UserName Days</pre> <p>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.</p>
The NetBackup Appliance administrator can force a password to expire immediately for one or more users.	<pre>Main > Manage > NetBackupCLI > PasswordExpiry Now UserName</pre> <p>You use the <i>UserName</i> variable to specify the user or users. Enter <i>All</i> to expire the password for all users.</p>
The NetBackup Appliance administrator can view the password expiry information.	<pre>Main > Manage > NetBackupCLI > PasswordExpiry Show UserName</pre> <p>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.</p>
The NetBackup 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.	<pre>Main > Manage > NetBackupCLI > PasswordExpiry Warn UserName Days</pre> <p>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.</p>

See [“About running NetBackup commands from the appliance”](#) on page 208.

See [“About NetBackup administrator capabilities”](#) on page 209.

See [“Logging on as a NetBackup administrator”](#) on page 215.

See [“Creating NetBackup administrator user accounts ”](#) on page 214.

See [“Auditing NetBackup Administrator accounts”](#) on page 217.

See [“Deleting NetBackup administrator user accounts ”](#) on page 217.

See [“Viewing NetBackup administrator user accounts”](#) on page 218.

Auditing NetBackup Administrator accounts

NetBackup Appliance administrators can monitor the activity of each NetBackup administrator account. That means a NetBackup Appliance administrator can monitor the NetBackup commands that a NetBackup administrator executes. To audit that activity from the NetBackup Appliance Shell Menu, the NetBackup 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 214.

See [“Managing NetBackup administrator user account passwords”](#) on page 216.

See [“Deleting NetBackup administrator user accounts ”](#) on page 217.

See [“Viewing NetBackup administrator user accounts”](#) on page 218.

Deleting NetBackup administrator user accounts

NetBackup 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 the *NetBackup Appliance Command Reference Guide* for additional information about this command and its use.

See [“About running NetBackup commands from the appliance”](#) on page 208.

See [“About NetBackup administrator capabilities”](#) on page 209.

See [“Creating NetBackup administrator user accounts”](#) on page 214.

See [“Managing NetBackup administrator user account passwords”](#) on page 216.

See [“Auditing NetBackup Administrator accounts”](#) on page 217.

See [“Viewing NetBackup administrator user accounts”](#) on page 218.

Viewing NetBackup administrator user accounts

NetBackup 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 the *NetBackup Appliance Command Reference Guide* for additional information about this command and its use.

See [“About running NetBackup commands from the appliance”](#) on page 208.

See [“About NetBackup administrator capabilities”](#) on page 209.

See [“Creating NetBackup administrator user accounts”](#) on page 214.

See [“Managing NetBackup administrator user account passwords”](#) on page 216.

See [“Auditing NetBackup Administrator accounts”](#) on page 217.

See [“Deleting NetBackup administrator user accounts ”](#) on page 217.

About Auto Image Replication between appliances

Auto Image Replication is the ability to replicate backups that are generated in one NetBackup domain to storage in other NetBackup domains, often across various geographical sites.

You can perform Auto Image Replication between appliances in the following manner:

- Auto Image Replication between NetBackup appliances
More information on how to perform Auto Image Replication between NetBackup appliances is available.
See [“About Auto Image Replication between NetBackup appliances”](#) on page 219.
- Auto Image Replication between NetBackup appliances and deduplication appliances
More information on how to perform Auto Image Replication between a NetBackup appliance and a deduplication appliance is available.
See [“About Auto Image Replication between NetBackup appliances and deduplication appliances”](#) on page 224.

About Auto Image Replication between NetBackup appliances

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 appliances.

To configure Auto Image Replication between two NetBackup appliances, you need to perform the following tasks:

Step No.	Task	Reference
1.	Establish trust between the two master servers	See “Adding a trusted master server” on page 220.
2.	Review the prerequisites for Auto Image Replication.	See “Prerequisites for Auto Image Replication” on page 221.

Step No.	Task	Reference
3.	Configure the replication target	See "Configuring a replication target" on page 221.
4.	Configure storage lifecycle policy on source and target domains	See the section named 'Creating a storage lifecycle policy' in <i>Symantec NetBackup Administrator's Guide, Volume I</i> .

Adding a trusted master server

You can configure a trust relationship between multiple NetBackup domains. To do so, in a source domain you specify the remote master servers with which you want to add a trust relationship. Use the following procedure in the source domain to add a remote master server as a trusted master server.

A trust relationship between domains helps with replication operations.

Note: If either the source or remote master server is clustered, you must enable inter-node communication on all of the nodes in the cluster. Do so before you add the trusted master server.

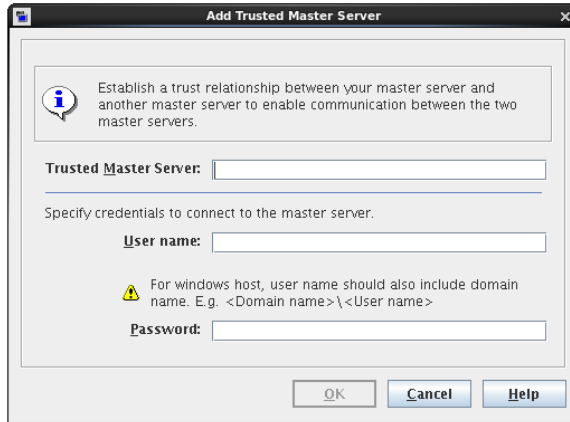
To add a trusted master server

- 1 In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Master Servers** in the left pane.
- 2 In the right pane, select the master server.
- 3 On the **Actions** menu, click **Properties**.
- 4 In the properties dialog box left pane, select **Servers**.
- 5 In the **Servers** dialog box, select the **Trusted Master Servers** tab.

- 6 On the **Trusted Master Servers** tab, click **Add**.

The **Add a New Trusted Master Server** dialog box appears.

The following is an example of the dialog box:



- 7 In the **Add a New Trusted Master Server** dialog box, enter the following and then click **OK**:
- The fully-qualified host name of the remote master server.
 - The logon account **User name** of the remote master server host.
 - The **Password** for the logon account of the remote master server host.
- 8 Repeat step 6 and step 7 for each master server with which you want to add a trust relationship.
- 9 When you finish adding trusted master servers, click **OK**.

Prerequisites for Auto Image Replication

The following prerequisites must be followed before you set up replication configuration between NetBackup appliances:

- The target storage server type must be the same that is configured in the target master server domain.
- The target storage server name must be the same that is configured in the target master server domain.

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 master server and a replication target.

In the **Target Master Server** drop-down list, select the master server of the domain to which you want to replicate data. All trusted master 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 master 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 master 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 the target appliance's deduplication storage server.

Password: *appliance dedupe password*

Use the following procedure to determine the Appliance deduplication password.

See [“Determining the appliance deduplication password”](#) on page 223.

- 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 *Symantec NetBackup Administrator's Guide, Volume I for UNIX, Windows, and Linux*.

Determining the appliance deduplication password

The following credentials are required to configure Auto Image Replication between appliances.

- **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 master server and one or more appliance media servers, the deduplication password is the same for all servers. In this case, use the appliance master server's shell menu to retrieve the deduplication password.

For more information about Auto Image Replication, refer to the *Symantec NetBackup™ Administrator's Guide, Volume I for UNIX and Linux* or the *Symantec NetBackup™ Administrator's Guide, Volume I for Windows*.

About Auto Image Replication between NetBackup appliances and deduplication appliances

The backups that are generated in NetBackup appliances can be replicated to the storage pools in one or more deduplication appliances. You can configure Auto Image Replication from a NetBackup appliance on one domain to a deduplication appliance on another domain.

To configure Auto Image Replication from a NetBackup appliance to a deduplication appliance, you are required to enter the user name and password for the target deduplication appliance.

The following credentials are required to configure Auto Image Replication from a NetBackup appliance to a deduplication appliance:

- **username:** `root`
- **password:** `P@ssw0rd` or a custom password that you have configured for the SPA (Storage Pool Authority)

For more information about Auto Image Replication, refer to the *Symantec NetBackup™ Administrator's Guide, Volume I for UNIX, Windows and Linux*.

Understanding the NetBackup appliance settings

This chapter includes the following topics:

- [About modifying the appliance settings](#)
- [Settings > Notifications](#)
- [Settings > Network](#)
- [Settings > Date and Time](#)
- [Settings > Authentication](#)
- [Settings > Password Management](#)

About modifying the appliance settings

After you have successfully configured your appliance you can use the NetBackup Appliance Web Console and the NetBackup Appliance Shell Menu to change various settings for your appliance. You can use the **Settings** tab in the Symantec NetBackup Appliance Web Console to view and configure the following settings.

[Table 5-1](#) describes the settings that are available from **Settings > Configuration** menu:

Table 5-1 Settings > Notification

Sub Menu	Lets you...	Topic
Alert configuration	Configure the SNMP, SMTP, and Call Home settings.	See “Settings > Notifications > Alert Configuration” on page 227.
Registration	Register the details of your appliance and your contact information.	See “Settings > Notification > Registration” on page 238.

[Table 5-2](#) describes the settings that are available from **Settings > Network** menu:

Table 5-2 Settings > Network

Sub Menu	Lets you...	Topic
Network	View and change network configuration settings.	See “Settings > Network > Network Settings” on page 243.
Host	Configure the host name, for either DNS or non-DNS systems	See “Settings > Network > Host” on page 262. See “Changing DNS and Host Name Resolution (non-DNS) configuration settings” on page 263.
Fibre Transport Configuration	Configure fibre transport settings for your appliance.	See “Settings > Network > Fibre Transport” on page 259. See “Changing the Fibre Transport settings” on page 260.

[Table 5-3](#) describes the settings that are available from the **Settings > Password** menu:

Table 5-3 Settings > Password

Sub Menu	Lets you...	Topic
Password	Change the admin password for your appliance.	See “Settings > Password Management” on page 293.

[Table 5-4](#) describes the settings that are available from the **Settings > Date and Time** menu:

Table 5-4 Settings > Date and Time

Sub Menu	Lets you...	Topic
Date and Time Configuration	Change the date and time on your appliance.	See “ Settings > Date and Time ” on page 265.

[Table 5-5](#) describes the settings that are available from **Settings > Authentication** menu:

Table 5-5 Setting > Authentication

Sub Menu	Lets you...	Topic
Authentication	Manage the following three types of user authentication: <ul style="list-style-type: none">■ LDAP■ Active Directory■ Kerberos-NIS	See “ Settings > Authentication ” on page 273.
User Management	Add new local users and create user groups for accessing your appliance.	See “ Settings > Authentication > User Management ” on page 287.

Settings > Notifications

The **Settings > Notifications** menu displays the following tabs:

- **Alert Configuration** - enables you to provide the SMTP, SNMP, and Call Home settings. See “[Settings > Notifications > Alert Configuration](#)” on page 227.
- **Registration** - enables you to register the appliance and your contact information. See “[Settings > Notification > Registration](#)” on page 238.

Settings > Notifications > Alert Configuration

The **Settings > Notifications > Alert Configuration** page provides you with one location from where you can enable SNMP, SMTP, and Call Home alert notifications. The page is divided into three sections each dedicated to enable and provide details for **SNMP**, **SMTP**, and **Call Home**.

Under **Alert Configuration** is the **Notification Interval** field. You must enter the time interval in minutes between two subsequent notifications for the SNMP and the SMTP configurations. The time interval should be in multiples of 15 and it should not be zero.

Configuring SNMP

Table 5-6 lists the fields from the **SNMP** (Simple Network Management Protocol) section.

Table 5-6 SNMP Server Configuration settings

Fields	Description
Enable SNMP Alert	Select this check box to enable SNMP alert configuration.
SNMP Server	<p>Enter the SNMP Server host name. You can enter a host name or an IP address to define this computer. The IP address can be an IPv4 or IPv6 address. Only global-scope and unique-local IPv6 addresses are allowed.</p> <p>Notification of the alerts or traps that are generated in Appliance are sent to this SNMP manager.</p> <p>Note: The NetBackup Appliance supports all the SNMP servers in the market. However, the ManageEngine™ SNMP server and the HP OpenView SNMP server are tested and certified for version 2.6.</p> <p>See “About IPv4-IPv6-based network support” on page 264.</p>
SNMP Port	<p>Enter the SNMP Server port number. If you do not enter anything for this variable, then the default port is 162.</p> <p>Note: Your firewall must allow access from the appliance to the SNMP server through this port.</p>
SNMP Community	<p>Enter the community to which the alerts or traps are sent. For example, Backup Reporting Department.</p> <p>You can enter a value that you configured on your SNMP server. For example, you can enter a company name or a name like, <code>admin_group</code>, <code>public</code>, or <code>private</code>. If you do not enter anything, then the default value is <code>public</code>.</p>

The SNMP MIB file serves as a data dictionary that is used to assemble and interpret SNMP messages. If you configure SNMP, you must import the MIB file into the monitoring software so that the software can interpret the SNMP traps. You can check the details of the MIB file from the SNMP Server Configuration pane. To check details about the SNMP MIB file, click **View SNMP MIB file**. An SNMP MIB file opens.

For information on how to send a test SNMP trap after configuration, see the following tech note on the Symantec Support website:

www.symantec.com/docs/TECH208354

Configuring SMTP

The SMTP mail server protocol is used for outgoing Email. You can configure SMTP from the NetBackup Appliance Web Console (**Settings > Alert Configuration > SMTP Server Configuration**).

You can also use the following command in the NetBackup Appliance Shell Menu to configure the SMTP server and add a new Email account:

```
Main_Menu > Settings > Alerts > Email SMTP Add Server [Account]
[Password], where Server is the host name of the target SMTP server that is used
to send emails. [Account] and [Password] are optional parameters to identify the
name of the account and the account password if authentication is required.
```

For more information, see the *NetBackup Appliance Command Reference Guide*.

[Table 5-7](#) lists the fields from the **SMTP** section of the NetBackup Appliance Web Console.

Table 5-7 SMTP Server Configuration settings

Fields	Description
SMTP Server	Enter the SMTP (Simple Mail Transfer Protocol) Server host name. Notifications of the alerts that are generated in Appliance are sent using this SMTP server. The IP address can be an IPv4 or IPv6 address. Only global-scope and unique-local IPv6 addresses are allowed. See "About IPv4-IPv6-based network support" on page 264.
Software Administrator Email	Enter the Email ID of the software administrator, to receive software alerts that are specific to the Symantec NetBackup Appliance software. This Email ID that you designate receives alerts for the following software conditions: <ul style="list-style-type: none">■ Host information such as:<ul style="list-style-type: none">■ Disk information.■ Overall backup status.■ Results of last seven backups for each client.■ An Email of your catalog backup disaster recovery file.■ A patch installation success report.
Hardware Administrator Email	Enter the Email ID of the hardware administrator, to receive hardware alerts that are specific to the Symantec NetBackup Hardware Appliance. For example, hardwareadmin@usergroup.com See "About Email notification from a NetBackup appliance" on page 45. for more information about potential hardware alerts.

Table 5-7 SMTP Server Configuration settings (*continued*)

Fields	Description
Sender Email	Enter the Email ID to receive any replies to the alerts or the reports that are sent by the Appliance.
SMTP Account	Enter the user name to access the SMTP account. Note: You maybe asked to enter a user name as some SMTP servers may require user name and password credentials to send an email.
Password	Enter the password for the above mentioned SMTP user account. Note: You maybe asked to enter a password as some SMTP servers may require user name and password credentials to send an email.

You can configure this server to send email reports to a proxy server or to the Symantec Call Home server.

The following describes the supported proxy servers:

- Squid
- Apache
- TMG

Note: NTLM authentication in the proxy configuration is also supported.

Starting with NetBackup Appliance 2.6.1.1, all email notifications that get generated by the appliance use the same SMTP settings. These emails include hardware monitoring notifications and NetBackup job notifications. The configuration settings are located under **Settings > Notification > Alert Configuration** in the NetBackup Appliance Web Console or `Main_Menu > Settings > Alerts` in the NetBackup Appliance Shell Menu. These settings override any previous SMTP setup you may have previously used to send NetBackup job notifications.

Note: If you had already configured the appliance SMTP settings before you upgraded to NetBackup Appliance 2.6.1.1, you may need to re-save the configuration in order for NetBackup to use it. In the NetBackup Appliance Web Console, go to **Settings > Notification > Alert Configuration** and click **Save**. Or in the NetBackup Appliance Shell Menu, go to `Main_Menu > Settings > Alerts` and resubmit the SMTP and SenderID settings.

Configuring Call Home

Table 5-8 lists the fields from the **Call Home Configuration** section.

Table 5-8 Call Home Configuration settings

Fields	Description
Enable Call Home	Select this check box to enable Call Home alert configuration.
Enable Proxy Server	Select this check box to enable proxy.
Enable Proxy Tunneling	Select this check box if your proxy server supports SSL tunneling.
Proxy Server	Enter the name of the proxy server.
Proxy Port	Enter the port number of the proxy server.
Proxy Username	Enter the user name to log into the proxy server.
Proxy Password	Enter the password for the user name to log into the proxy server.

When Call Home is enabled, you can test whether or not Call Home is working correctly by clicking the **Test Call Home** option that is available below the Call Home configuration settings.

Note: The **Test Call Home** option is active on the NetBackup Appliance Web Console only when Call Home is enabled.

Configuring Alert Configuration settings

This section provides the procedure to configure the SNMP, SMTP, and Call Home server settings using the **Settings > Notification > Alert Configuration** page.

To configure the SNMP, SMTP, and Call Home server settings

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Notification > Alert Configuration**.

The system displays the **Alert Configuration** page.

The **Alert Configuration** page is divided into three sections to enable and provide details for **SNMP**, **SMTP**, and **Call Home**.

- 3 In the **Notification Interval** field enter the time interval in minutes between two subsequent notifications, for **SNMP**, **SMTP**, and **Call Home** alert configurations.

4 Enter the SNMP settings in the provided fields. A description of the SNMP parameters is available in [Table 5-6](#).

5 Enter the SMTP settings in the provided fields. A description of the SMTP parameters is available in [Table 5-7](#).

The appliance uses the global server settings to send email notifications to the SMTP server that you specify.

6 Enter the Call Home settings in the provided fields. A description of the Call Home parameters is available in [Table 5-8](#).

7 Click **Save**, to save the SNMP, SMTP, and Call Home settings.

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 Appliance Version supports SNMP v2.

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, 1.3.6.1.4.1.2682.1).

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 check the details of the SNMP MIB file from the **Settings > Notifications > Alert Configuration** page of the NetBackup Appliance Web Console. To configure the appliance SNMP manager to receive hardware monitoring related traps, click **View SNMP MIB file** in the **SNMP Server Configuration** pane.

You can also view the SNMP MIB file with the `Settings > Alerts > SNMP ShowMIB` command in the NetBackup Appliance Shell Menu.

About Call Home

Your appliance can connect with a Symantec AutoSupport server and upload hardware and software information. Symantec 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 Symantec AutoSupport server. This feature of the appliance is referred to as Call Home. It is enabled by default.

AutoSupport in appliance uses the data that is gathered by Call Home to provide proactive monitoring for the appliance. If Call Home is enabled, the appliance uploads hardware and software information (or the Call Home data) to Symantec AutoSupport server periodically at an interval of 24 hours by default.

If you determine that you have a problem with a piece of hardware, you might want to contact Symantec support. The Technical Support engineer uses the serial number of your appliance and assesses the hardware status from the Call Home data. To know the serial number of your appliance from the NetBackup Appliance Web Console, go to the **Monitor > Hardware > Health details** page. To determine the serial number of your appliance using the shell menu, go to the `Monitor > Hardware` commands. For more information about the `Monitor > Hardware` commands, refer to the *NetBackup Appliance Command Reference Guide*.

Use the **Settings > Notification** page to configure Call Home from the NetBackup Appliance Web Console. Click **Alert Configuration** and enter the details in the **Call Home Configuration** pane.

[Table 5-9](#) describes how a hardware failure is reported when the feature is enabled or disabled.

Table 5-9 What happens when Call Home is enabled or disabled

Monitoring status	Hardware failure routine
Call Home enabled	<p>When a hardware failure occurs, the following sequence of alerts occur:</p> <ul style="list-style-type: none">■ The appliance uploads all the monitored hardware and software information to a Symantec 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.<ul style="list-style-type: none">■ An error message by email to notify you of the hardware failure once an error is detected.■ A resolved message by email to inform you of any hardware 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	<p>No data is sent to the Symantec AutoSupport server. Your system does not report hardware errors to Symantec to enable faster problem resolution.</p>

The following list contains all the information that is monitored and sent to Symantec AutoSupport server for analysis.

- CPU
- Disk
- Fan
- Power supply
- RAID group
- Temperatures
- Adapter
- PCI
- Fibre Channel HBA
- Network card
- Partition information
- MSDP statistics

- Storage connections
- Storage status
- 52xx Storage Shelf - Status of disk, fan, power supply, and temperature
- 5330 Primary Storage Shelf - Status of disk, fan, power supply, temperature, battery backup unit (BBU), controller, volume, and volume group
- 5330 Expansion Storage Shelf - Status of disk, fan, power supply, and temperature
- NetBackup Appliance software version
- NetBackup version
- Appliance model
- Appliance configuration
- Firmware versions
- Appliance, storage, and hardware component serial numbers
See [“Hardware components that are monitored”](#) on page 40.

See [“Settings > Notifications > Alert Configuration”](#) on page 227.

See [“Configuring Call Home from the NetBackup Appliance Shell Menu”](#) on page 235.

See [“About AutoSupport”](#) on page 240.

See [“Monitor > Hardware options”](#) on page 36.

Configuring Call Home from the NetBackup Appliance Shell Menu

You can configure the Call Home details from the **Settings > Notification** page.

You can configure the following Call Home settings from the NetBackup Appliance Shell Menu:

- [Enabling and disabling Call Home from the NetBackup Appliance Shell Menu](#)
- [Configuring a Call Home proxy server from the NetBackup Appliance Shell Menu](#)
- Testing whether or not Call Home works correctly by running the `Settings > Alerts > CallHome > Test` command.

If you enable Call Home, you can use the `Settings > Alerts > CallHome Registration` command to configure the contact details for your appliance by entering the following information:

- The name of the person who is the first point of contact and responsible for the appliance.
- The address of the contact person.

- The phone number of the contact person.
- The email address of the contact person.

To learn more about the `Main > Settings > Alerts > CallHome` commands, refer to the *Symantec NetBackup Appliance Command Reference Guide*.

For a list of the hardware problems that cause an alert, see the following topics:

See [“Monitor > Hardware options”](#) on page 36.

See [“About Call Home”](#) on page 233.

See [“About Email notification from a NetBackup appliance”](#) on page 45.

Enabling and disabling Call Home from the NetBackup Appliance Shell Menu

You can enable or disable Call Home from both, the NetBackup Appliance Web Console and the NetBackup Appliance Shell Menu. Call Home is enabled by default.

To enable or disable Call Home from the NetBackup Appliance Shell Menu

- 1 Log on to the NetBackup Appliance Shell Menu.
- 2 To enable Call Home, run the `Main > Settings > Alerts > CallHome Enable` command.
- 3 To disable Call Home, run the `Main > Settings > Alerts > CallHome Disable` command.

For more information on `Main > Settings > Alerts > CallHome` commands, refer to the *Symantec NetBackup Appliance Command Reference Guide*.

Configuring a Call Home proxy server from the NetBackup 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 Symantec AutoSupport server. This option is disabled by default.

To add a Call Home proxy server from the NetBackup Appliance Shell Menu

- 1 Log on to NetBackup 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.
- 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 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.

Understanding the Call Home workflow

This section explains the mechanism that Call Home uses to upload data from your appliance to the Symantec AutoSupport server.

Call Home uses HTTPS (secure and encrypted protocol) with port number 443 for all communication with Symantec 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 Symantec 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.

All communications are initiated by the appliance. Your appliance needs access to <https://receiver.appliance.veritas.com>.

The appliance Call Home feature uses the following workflow to communicate with AutoSupport servers:

- Access a port to <https://receiver.appliance.veritas.com> every 24 hours.

- Perform a self-test operation to <https://receiver.appliance.veritas.com>.
- If the appliance encounters an error state, all hardware logs from past three days are gathered along with the current log.
- The logs are then uploaded to the Symantec 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 233.

See “[About AutoSupport](#)” on page 240.

About the Product Improvement Program

The NetBackup Appliance Product Improvement Program uses Call Home to capture installation deployment and product usage information. The information that Symantec 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 Symantec identify improvements in product features, testing, technical support, and future requirements.

You can enable or disable the Product Improvement Program from the NetBackup Appliance Shell Menu. This option is not available from the NetBackup Appliance Web Console.

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 Appliance Shell Menu

- 1 Log on to the NetBackup 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.

For more information on the `Main > Settings > Alerts > CallHome` commands, refer to the *NetBackup Appliance Command Reference Guide*.

Settings > Notification > Registration

You can register an appliance and enter your contact information from the **Registration** tab that is available under the **Settings > Notification** menu.

Registration of your NetBackup appliance helps to make sure that you are alerted to product updates and other important information about your appliance.

You may also complete the registration while configuring your appliance or in advance of installation from the MyAppliance portal at <https://my.appliance.veritas.com>. The [MyAppliance portal](https://my.appliance.veritas.com) offers more detail and contact information options than the other registration methods. Visit the portal for additional information.

This topic provides the necessary data entry fields to register an appliance with Symantec from the **Registration** tab of the NetBackup Appliance Web Console.

[Table 5-10](#) describes the data entry fields that are related to specific information sections and the type of information to enter in the fields.

Table 5-10 Data entry fields for the appliance registration

Section and related field name	Description
Provide the appliance name that we can refer to in our communications with you.	
Appliance Name	Enter a name for the appliance.
Provide the details of the physical location of the appliance.	
Company Name	Enter your company name.
Street	Enter the name of the street, where the appliance is located.
City	Enter the name of the city, where the appliance is located.
State or Province	Enter the name of the state, where the appliance is located.
Zip or Postal Code	Enter the ZIP Code.
Country	Enter the name of the country, where the appliance is located.
Provide the contact details of the official point of contact.	
Contact Name	Enter the name of the primary contact in regard to your appliance or your backup environment.
Contact Number	Enter the primary phone number for the contact name. This number should be the one that is most likely to reach the contact person.

Table 5-10 Data entry fields for the appliance registration (*continued*)

Section and related field name	Description
Contact Email	Enter the business email address for the Contact Name that you identified earlier.

If your appliance is provisioned and has Internet connectivity, the registration details populate automatically. In case the appliance is not provisioned, the following message is displayed:

Please verify and update the appliance registration information that Symantec has on file for this appliance.

You can also register your appliance using the `Main > Settings > Alerts > CallHome Registration` commands under the NetBackup Appliance Shell Menu. For more information, refer to the *Symantec NetBackup Appliance Command Reference Guide*.

Moving an appliance from one physical location to another

To move an appliance from one physical location to another, consider the following points to ensure continuance of maintenance and support coverage

- Certain locations or regions of the world may not be enabled or set up to handle field service calls for parts replacement.
- Certain locations or regions may not be able to meet the defined Service Level Agreement (SLA) contract(s) to which the appliance may be associated with.
- Customers should not move an appliance to another country.
- If it is imperative to move the appliance, you must contact your account access team at Symantec to understand the ramifications or impact (if any) to the Service agreements associated with the appliance.
- After you have moved the appliance, it is critical to update your registration details such as contact details and location information on the appliance to ensure continuance of coverage.

See [“About AutoSupport”](#) on page 240.

See [“Settings > Notifications > Alert Configuration”](#) on page 227.

About AutoSupport

The AutoSupport feature lets you register the appliance and your contact details at the Symantec support website. Symantec support uses this information to resolve

any issue that you report. The information allows Symantec support to minimize downtime and provide a more proactive approach to support.

Provide the registration details for your appliance using one of the following provisions:

- The [MyAppliance portal](#) before you install the appliance
- The appliance initial configuration on the **Registration** page
- The NetBackup Appliance Web Console by navigating to **Settings > Notification > Registration** page
- The NetBackup Appliance Shell Menu by running the `Settings > Alerts > CallHome Registration` command. For more information about this command, refer to the *NetBackup Appliance Command Reference Guide*.

You can register by entering the following basic information:

- Name: Your name, company name
- Address, where the appliance is physically located: City, street, state, ZIP Code
- Contact information: Phone number, email address

The support infrastructure is designed to allow Symantec support to help you in the following ways:

- Proactive monitoring lets Symantec support to automatically create cases, fix issues, and dispatch any appliance parts that might be at risk.
- The AutoSupport infrastructure within Symantec analyzes the Call Home data from appliance. This analysis provides proactive customer support for hardware failures, reducing the need for backup administrators to initiate support cases.
- With AutoSupport ability, Symantec 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 hardware and 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 of hardware failure, and see usage trends. The appliance sends health data every 30 minutes.

The information that you provide for appliance registration helps Symantec support to initiate resolution of any issue that you report. However, if you want to provide additional details such as a secondary contact, phone, rack location, and so on, you can visit <https://my.symantec.com>.

See [“Settings > Notification > Registration”](#) on page 238.

Settings > Network

The **Settings > Network** menu displays the following tabs:

- **Network Settings** - enables you to configure network and routing settings for your appliance.
See [“Settings > Network > Network Settings”](#) on page 243.
- **Host** - enables you to reconfigure your appliance's host settings.
See [“Settings > Network > Host”](#) on page 262.
- **Fibre Transport** - enables you to reconfigure the Fibre Transport settings.
See [“Settings > Network > Fibre Transport”](#) on page 259.

You can also configure the network settings using the `Main_Menu > Network` commands from the NetBackup Appliance Shell Menu. For more information refer to the *Symantec NetBackup Appliance Command Reference Guide*.

VLAN configuration for NetBackup Appliances

Starting with NetBackup Appliance version 2.6.0.3, you can configure VLANs in your existing network environments.

The concept of a Virtual Local Area Network (VLAN) is devised to logically partition a physical network for creating multiple distinct broadcast domains. These broadcast domains can be segmented on the basis of organization functions, teams within a function, or applications. Although the properties of VLANs are same as those of LANs, VLANs have pivotal advantages over the traditional LANs in the following ways:

- Allows the formation of virtual workgroups.
- Enhances network performance.
- Simplifies network administration.
- Provides better security.
- Reduces the overall costs of network management.

To configure VLAN for your appliance from the NetBackup Appliance Web Console, use the **Network** tab on the **Settings > Network** page.

To configure VLAN from the NetBackup Appliance Shell Menu, run the `Main_Menu> Network > VLAN` command.

See [“Settings > Network > Network Settings”](#) on page 243.

Settings > Network > Network Settings

The **Settings > Network** menu directs you to its default **Network Settings** page. The **Network Settings** page enables you to configure and update the network settings for your appliance. These network settings are applied at the time of initial configuration.

The **Network Settings** page is divided into two panes. The first pane contains the **Interface Properties** and **Routing Properties** tabs. The second pane contains **Network Configuration** pane.

The taskbar underneath the **Interface Properties** tab enables you to complete the following tasks:

Table 5-11 Taskbar elements under the Interface Properties tab

This function...	Lets you...
Filter by Network Interface	Filter the network interface by its name. If you enter the name of a physical interface in the field, the resultant displays information for the physical interface along with information of any bond that is created over the physical interface. For example, if <i>eth2</i> is a part of <i>bond1</i> , then the filter criteria for <i>eth2</i> displays information for <i>bond1</i> too.

Table 5-11 Taskbar elements under the Interface Properties tab (*continued*)

This function...	Lets you...
Edit	<p>Edit network interface properties. Use this button to edit MTU, remove an IP address, and assign an IP address on a selected network interface.</p> <p>Note: You must select a single network interface to edit its properties. If you select multiple interfaces, the Edit button is disabled.</p> <p>You can edit the following properties depending on the type of interface that is selected for editing:</p> <ul style="list-style-type: none"> ■ MTU - Use to update the maximum transmission unit (MTU) size for the selected interface. <p>Note: This field is available only for physical and bond interfaces.</p> <ul style="list-style-type: none"> ■ Description - Use to update the description for the selected VLAN device. <p>Note: This field is available only for VLAN devices. Further, the provision to add a description for the VLAN is available only through the NetBackup Appliance Web Console.</p> <ul style="list-style-type: none"> ■ Remove IP Interface - Use to remove an IP address. ■ Assign IP - Use to update or assign an IP address. <p>The Assign IP section lets you edit the following fields:</p> <ul style="list-style-type: none"> ■ IP Address [IPv4] - Enter the IPv4 address. ■ Netmask IP Address [IPv4] - Enter netmask information for the IPv4 address. ■ IP Address [IPv6] - Enter the IPv6 address. ■ Prefix size [IPv6] - Enter the prefix size for the IPv6 address. ■ Enable WAN optimization Enables or disables WAN (wide area network) optimization for individual network interfaces and network interface bonds. See “About WAN Optimization” on page 248.
Delete	<p>Delete multiple virtual interfaces. For example, <i>bond1</i>, <i>bond2</i> or <i>vlan2</i>, <i>vlan3</i>, <i>vlan4</i>.</p> <p>Note: You cannot delete multiple network interfaces simultaneously. Further, you cannot delete a physical interface.</p> <p>In addition, you cannot delete an interface that is a part of a bond or that has a VLAN tagged to it.</p>

The taskbar below the **Routing Properties** tab lets you delete routing information for a selected network interface using the **Delete** button.

The **Interface Properties** tab and the **Routing Properties** tab provide the following information:

Table 5-12 Interface Properties tab and Routing Properties tab information

Field names	Description
-------------	-------------

Interface Properties: Click this tab to view the existing network interface configuration settings for the appliance.

Network Interface	Displays the NIC (network interface card) number. For example, eth1 or vlan1. Note: A private interface (eth0) can not be edited from the NetBackup Appliance Web Console. However, you can edit a private interface from the NetBackup Appliance Shell Menu. Note: On a NetBackup 5330 Appliance, the number of Ethernet ports that you can edit on the Network Settings page depends on the PCIe configuration of the appliance. See “NetBackup 5330 compute node Ethernet port configurations” on page 247.
Description	Displays information that is entered for a VLAN interface. For example, HR domain, Finance domain.
IP Address [IPv4 or IPv6]	Displays the IPv4 or the IPv6 address of the network connection.
Subnet Mask	Displays the subnet mask value that corresponds to the IP address.
Speed	Displays the current speed of the network connection. For example, 1Gb/s.
Cable State	Displays the status of the cable connection as Plugged or Unplugged.
Link State	Displays the status of network connection as Up or Down.
Link Aggregation	Displays whether a physical interface is a part of a bond. If the physical interface is a part of a bond, the field displays YES.
Reserved	Displays if the network is reserved or not.
WAN optimization	Displays the WAN optimization status of each network interface. Status messages include Enabled or Disabled.

Table 5-12 Interface Properties tab and Routing Properties tab information
(continued)

Field names	Description
VLAN	Display whether a VLAN is tagged to a network interface. If a VLAN is tagged to a network interface the field displays YES.
Routing Properties: Click this tab to view the existing routing configuration settings for the appliance.	
Network Interface	Displays the NIC (network interface card) number. For example, eth1.
Destination IP	Displays the network IP address of a destination network.
Destination Subnet Mask	Displays the subnet value that corresponds to the IP address.
Gateway	Displays the address of the network point that acts as an entrance to another network.

In addition, the network interfaces that you find in the **Interface Properties** tab and the **Routing Properties** tab also provide links to access detailed network properties. Clicking a network interface opens a properties window for the selected network interface. The window provides information about the selected network interface.

The following table describes the type of network configurations that you can perform.

Table 5-13 Network Configuration pane options

Operation	Description
Create Bond	Provides the data entry fields to create a network bond. See “Creating a bond” on page 255.
Tag VLAN	Provides the data entry fields to tag a VLAN over a network interface. See “Tagging VLAN” on page 256.
Add Static Route	Provides the data entry fields to add network routing information. See “Adding static route” on page 258.

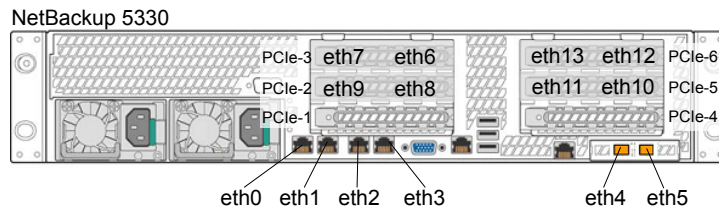
See [“VLAN configuration for NetBackup Appliances”](#) on page 242.

NetBackup 5330 compute node Ethernet port configurations

The rear panel of the NetBackup 5330 compute node contains six PCIe slots, which are populated according to five different supported configurations. The PCIe slot configuration determines the number of Ethernet ports that are available.

[Figure 5-1](#) shows where each Ethernet port is located on the rear panel of the appliance.

Figure 5-1 NetBackup 5330 compute node Ethernet port locations



All NetBackup 5330 Appliances include the following ports, which are built in along the base of the rear panel:

- 1-Gb ports: eth0, eth1, eth2, and eth3
- 10-Gb ports: eth4 and eth5

The 10-Gb Ethernet network interface cards that are installed in the PCIe slots contain additional ports. The number of ports depends on the PCIe slot configuration of your compute node.

[Table 5-14](#) shows the available Ethernet ports for each PCIe slot configuration.

Table 5-14 NetBackup 5330 compute node PCIe Ethernet port configurations

Option	Slot and Ethernet port numbers
A (four 10-Gb Ethernet cards)	<ul style="list-style-type: none"> ■ Slot 2: eth8 (right), eth9 (left) ■ Slot 3: eth6 (right), eth7 (left) ■ Slot 5: eth10 (right), eth11 (left) ■ Slot 6: eth12 (right), eth13 (left)
B (three 10-Gb Ethernet cards)	<ul style="list-style-type: none"> ■ Slot 2: eth8 (right), eth9 (left) ■ Slot 3: eth6 (right), eth7 (left) ■ Slot 5: eth10 (right), eth11 (left)
C (two 10-Gb Ethernet cards)	<ul style="list-style-type: none"> ■ Slot 2: eth8 (right), eth9 (left) ■ Slot 3: eth6 (right), eth7 (left)
D (one 10-Gb Ethernet card)	<ul style="list-style-type: none"> ■ Slot 3: eth6 (right), eth7 (left)

Table 5-14 NetBackup 5330 compute node PCIe Ethernet port configurations
(continued)

Option	Slot and Ethernet port numbers
E (no 10-Gb Ethernet cards)	N/A

See [“Settings > Network > Network Settings”](#) on page 243.

About WAN Optimization

The Wide Area Network (WAN) Optimization feature applies various techniques to improve outbound network traffic from your appliance.

This feature includes the following benefits:

- Improves NetBackup Auto Image Replication (AIR) performance.
NetBackup AIR 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 occur.
- Benefits those appliances for which the traffic is sent across on slower networks. 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 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.

You can enable or disable WAN Optimization for individual network interfaces and network interface port bonds from **Settings > Network > Interface Properties** tab

in the NetBackup Appliance Web Console. You can also use the NetBackup Appliance Shell Menu.

For more information about using WAN Optimization commands in the NetBackup Appliance Shell Menu, refer to *Symantec NetBackup™ Appliance Commands Reference Guide*.

Table 5-15 WAN Optimization operations

Operation	Description	NetBackup Appliance Shell Menu	NetBackup Appliance Web Console
Enable	The <code>Enable</code> command is used to enable the WAN optimization settings. The WAN optimization feature is enabled by default. See “How to enable WAN optimization for a network interface port or a network interface port bond” on page 250.	Yes	Yes
Disable	The <code>Disable</code> command is used to disable the WAN optimization settings. You can disable this setting using the NetBackup Appliance Web Console or the NetBackup Appliance Shell Menu. See “How to disable WAN optimization for a network interface port or a network bond” on page 251.	Yes	Yes

Table 5-15 WAN Optimization operations (*continued*)

Operation	Description	NetBackup Appliance Shell Menu	NetBackup Appliance Web Console
Status	The <code>Status</code> command is used to view WAN optimization reports. See “Viewing the WAN optimization status” on page 252.	Yes	Yes

See [“Settings > Network > Fibre Transport”](#) on page 259.

See [“Settings > Network > Host”](#) on page 262.

How to enable WAN optimization for a network interface port or a network interface port bond

Use the following procedure to enable WAN optimization for a network interface port or a network interface port bond.

To enable WAN optimization for a network interface port or a network interface port bond

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Network**.
- 3 On the Network Settings page, under the **Interface Properties** tab, select a network interface.
- 4 Click **Edit**.

The **Edit Network Interface Properties** dialog box appears.

- 5 To enable WAN optimization, select **Enable WAN optimization**.
- 6 Click **Save**.

The following message appears while the appliance enables WAN optimization for the selected network interface:

```
Updating network configuration...
```

After the appliance successfully enables WAN optimization, the following message appears under the **Network Settings** page name:

```
WAN optimization for [selected eth port or bond] was enabled  
successfully.
```

In addition, the status of the selected network interface changes to **Enabled** in the **WAN optimization** column of the **Interface Properties** tab.

Note: If you run a factory reset of the appliance, note the following:

A factory reset disables WAN optimization for all network interface port bonds when you retain your network configuration. To retain your network configuration, you can select **Retain network configuration** in the NetBackup Appliance Web Console (**Manage > Appliance Restore > Retain network configuration**). After the factory reset completes, you can then enable WAN optimization again for the network interface port bonds.

If you choose *not* to retain your network configuration, all network interface port 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.

How to disable WAN optimization for a network interface port or a network bond

Use the following procedure to disable WAN optimization for a network interface port or a network bond.

To disable WAN optimization for a network interface port or a network bond

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Network**.
- 3 On the Network Settings page, under the **Interface Properties** tab, select a network interface.
- 4 Click **Edit**.

The **Edit Network Interface Properties** dialog box appears.

- 5 To disable WAN optimization, deselect **Enable WAN optimization**.
- 6 Click **Save**.

The following message appears while the appliance disables WAN optimization for the selected network interface:

```
Updating network configuration...
```

After the appliance successfully disables WAN optimization, the following message appears under the **Network Settings** page name:

```
WAN optimization for [selected eth port or bond] was disabled  
successfully.
```

In addition, the status of the selected network interface changes to **Disabled** in the **WAN optimization** column of the **Interface Properties** tab.

Viewing the WAN optimization status

The `Status` command displays the WAN optimization status of the network interface ports and the network interface port bonds.

- If WAN Optimization is disabled, the connection is not optimized.
- If the WAN Optimization status is changed (from disabled to enabled or vice versa), the status of existing connections is immediately updated.

To view the WAN optimization status

- 1 Log in to the NetBackup Appliance Shell Menu.
- 2 To view the WAN Optimization option, type the following command:

```
Main_Menu > Network > WANOptimization
```

All of the options for the WAN Optimization command appear.

- 3 To view the WAN optimization status, type the following command:

```
status
```

The appliance displays the WAN optimization status in a table that resembles the following example:

Bond	Interface	State	IP address	WAN Optimization
bond0	eth4	Plugged		Disabled
	eth5	Plugged		
	eth0	Unplugged	192.168.00.00	Enabled
	eth1	Plugged	10.200.00.00	Disabled
	eth2	Plugged		Enabled
	eth3	Plugged		Enabled

Network and VLAN configuration guidelines

To facilitate network configuration and administration, it is recommended that you follow certain guideline to configure or update your network settings.

Guidelines for creating a network interface bond (NIC bond):

- Ensure that the network interfaces that participate in bond formation have the same port speed (i.e. either 1GB or 100GB).
- At least one of the network interfaces that participates in bond formation must be plugged.
- Ensure that none of the network interfaces that are selected for creating the bond have any VLANs tagged to them.

- Verify that any of the selected network interfaces are not already part of another bond.

Note: When configuring multiple network interfaces as a NIC bond, use the NetBackup Appliance Shell Menu or the NetBackup Appliance Web Console to configure the bond. NIC bonds that are configured with tools other than the recommended appliance tools appear as *Disabled* when you run the WAN optimization `Status` command. They also appear as *Disabled* when you view them in the NetBackup Appliance Web Console.

Use either the NetBackup Appliance Shell Menu or the NetBackup Appliance Web Console to enable these NIC bonds.

Guidelines for tagging a VLAN:

- Ensure that the selected interface or ethernet device is plugged.
- Verify that the selected interface is not a part of a bond.
- The selected interface must not have an IP address configured to it. If the selected interface is configured with an IP address, you must first remove the IP address and then tag a VLAN to it.

To remove an IP address from the NetBackup Appliance Web Console

- Log on to the NetBackup Appliance Web Console.
- Go to the **Setting > Network** menu. The appliance displays the default Network Settings page.
- From the **Interface Properties** tab, select the interface for which you want to remove the IP address.
- Click the **Edit** button that is located below on the **Interface Properties** tab. The appliance displays the editable fields for the selected interface.
- Select the check box against **Remove IP Interface**.
- Click **OK** to save the changes.

To remove an IP address from the NetBackup Appliance Shell Menu

- Log on to the NetBackup Appliance Shell Menu.
- Run the `Network > Unconfigure InterfaceName [IPAddress]` command.
- Enter the name of the interface for which you want to unconfigure the IP address. In addition, you may also provide the IP address to be unconfigured.

Creating a bond

Use the following procedure to create a bond between two or more network interfaces.

To create a bond

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Network** tab. The appliance displays the default **Network Settings** page.
- 3 Click **Create Bond**.
- 4 In the **Network Configuration** section, enter the network interface information that is required to create a bond using the following fields:

Field name	Description
Select Interface	<p>Select the interface or the device name between which you want to create the bond.</p> <p>To bond multiple Network Interface Cards (NICs), consider the following guidelines:</p> <ul style="list-style-type: none">■ The Network Interface drop-down list shows appliance Ethernet ports available for creating a bond. Select two or more interfaces to create a bond. To deselect an interface, click it again.■ You can enter either an IPv4 address or an IPv6 address. Multiple or duplicate IP addresses are not excepted for a NIC or bond.■ Only NICs of the same type and speed can be bonded. <p>See “Network and VLAN configuration guidelines” on page 253. for additional guidelines on creating a bond.</p>

Field name	Description
Bond Mode	<p>Select the bond mode to configure bonding.</p> <p>The eight available modes are:</p> <ul style="list-style-type: none">■ balance-rr■ active-backup■ balance-xor■ broadcast■ 802.3ad■ balance-tlb■ balance-alb <p>The default mode is balance-alb. Some bond modes require additional configuration on the switch or the router. You should take additional care when you select a bond mode.</p> <p>For more information about bond modes, see the following documentation:</p> <p>http://www.kernel.org/doc/Documentation/networking/bonding.txt</p>
IP Address [IPv4 or IPv6]	<p>Enter the IPv4 or the IPv6 address to be used for this appliance. Only global-scope and unique-local IPv6 addresses are allowed.</p>
Subnet Mask	<p>Enter the subnet mask value that corresponds to the IP address.</p>

5 To add the network configuration details for creating the bond, click **Add**.

The new entries are configured on the appliance and are listed automatically in the read-only fields of the **Interface Properties** tab.

To create a bond using the NetBackup Appliance Shell Menu, run the `Main_Menu > Network > LinkAggregation Create` command. For detailed information on the `LinkAggregation Create` command, refer to the *NetBackup Appliance Command Reference Guide*.

See “[Tagging VLAN](#)” on page 256.

See “[Adding static route](#)” on page 258.

Tagging VLAN

Use the following procedure to tag VLAN into your existing network environment.

To tag VLAN

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Network** tab. The appliance displays the default **Network Settings** page.
- 3 In the **Network Configuration** section, expand the **Tag VLAN** option and enter the network information that is required to tag a VLAN using the following fields:

Field Name	Description
Select Interface	Select the network interface or the device name to which you want to tag the VLAN. See “Network and VLAN configuration guidelines” on page 253. for additional guidelines on tagging a VLAN.
Description	Enter a description for the VLAN. For example, Finance or Human Resource.
VLAN Id	Enter a numeric identifier for the VLAN. For example, 1 or 10.
IP Address [IPv4 or IPv6]	Enter the IPv4 or the IPv6 address to be used for this appliance.
Subnet Mask	Enter the subnet mask value that corresponds to the IP address.

- 4 Click **Add** to add the configuration information for tagging VLAN into to your existing network environment.
- 5 To enter information for tagging additional VLANs, click the **+** sign to add a row. To remove any of the rows, click the **-** sign that is adjacent to the **Subnet Mask** field.

The new entries are configured on the appliance and are listed automatically in the read-only fields of the **Interface Properties** tab.

To tag VLAN from the NetBackup Appliance Shell Menu, run the `Main_Menu > Network > VLAN Tag` command. For detailed information on the `VLAN Tag` command, refer to the *NetBackup Appliance Command Reference Guide*.

See [“Creating a bond”](#) on page 255.

See [“Adding static route”](#) on page 258.

Adding static route

Use the following procedure to add or update the network routing information for your appliance.

To add network routing information for your appliance

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Network > Network** tab. The appliance displays the **Network Settings** page.
- 3 In the **Network Configuration** section, expand the **Add Static Route** option and enter the network interface information that is required to add routing information using the following fields:

Field Name	Description
Destination IP	<p>Enter the network IP address of a destination network.</p> <p>Enter the network IP address of a destination network. For the initial appliance configuration, this field contains a default value that cannot be changed. When you configure another destination IP, you must enter the appropriate address.</p>
Destination Subnet Mask	<p>Enter the subnet value that corresponds to the IP address.</p> <p>Enter the subnet value that corresponds to the IP address. For the initial appliance configuration, this field contains a default value that cannot be changed. When you configure another route, you must enter the appropriate value.</p>
Gateway	<p>Enter the address of the network point that acts as an entrance to another network.</p>
Network Interface	<p>The appliance can use multiple network interface cards (NICs). This column displays the network device name. for example, eth0 or bond0 or vlan1.</p>

- 4 Click **Add** to add the network routing information for your appliance.

The new entries are configured on the appliance and are listed automatically in the read-only fields of the **Routing Properties** tab.

See [“Creating a bond”](#) on page 255.

See [“Tagging VLAN”](#) on page 256.

Settings > Network > Fibre Transport

The Fibre Transport (FT) options let you set up the appliance for FT use with SAN Clients or NetBackup deduplication appliances. By default, the FT options are disabled and the configuration of one option does not affect the other one.

The following describes the FT options:

Table 5-16 FT option descriptions

FT option	Description
Enable SAN Client Fibre Transport on the Media Server (use FT for backups to this appliance) <ul style="list-style-type: none">■ 2 target port Fibre Channel connection■ 4 target port Fibre Channel connection	<p>This option lets you change the port configuration of appliance Fibre Channel (FC) HBA cards for SAN Client FT use.</p> <p>The following describes the FC HBA cards that are affected:</p> <ul style="list-style-type: none">■ NetBackup 5220 - FC HBA cards in slots 2 and 4■ NetBackup 5230 and NetBackup 5330 - FC HBA cards in slots 5 and 6 <p>By default, the option is disabled and all ports are in the initiator mode.</p> <p>When the option is enabled and 2 target port Fibre Channel connection is selected, Port 1 on all affected FC HBA cards is set to the target mode. The appliance can now use these ports for deduplicated backups with the use of FT.</p> <p>When the option is enabled and 4 target port Fibre Channel connection is selected, Port 1 and Port 2 on all affected FC HBA cards are set to the target mode. The appliance can now use these ports for deduplicated backups with the use of FT.</p> <p>Before you enable this option, be aware of the following requirements and behavior:</p> <ul style="list-style-type: none">■ To use this option, a SAN Client license key must reside on the master server that is associated with this appliance. If FT is not currently used and you want to use the SAN Client feature, you must first obtain a SAN Client license key. To obtain the appropriate license key, contact technical support. Once you have the license key, you must add it to the master server.■ When this option is enabled or changed, a warning appears to alert you that the appliance requires a restart. Before you enable this option, it is recommended that you first suspend or cancel all jobs.

Table 5-16 FT option descriptions (*continued*)

FT option	Description
Enable Fibre Transport for duplication and backups on a Deduplication Appliance	<p>This option lets you configure this appliance for use with a NetBackup 5020 or 5030 Deduplication Appliance. By default, this option is disabled and the appliance cannot communicate with a deduplication appliance.</p> <p>When the option is enabled, the appliance can use FT for duplication and backups to a deduplication appliance.</p> <p>When this option is enabled, you must also enable Fibre Channel communication on the associated or targeted NetBackup 5020 or 5030. For complete information, see the <i>Symantec NetBackup Deduplication Appliance Software Administrator's Guide</i>. Refer to the section "Verifying, enabling, or disabling Fibre Channel communication".</p>

Changing the Fibre Transport settings

Use the following procedure to change the Fibre Transport settings.

Before you change the Fibre Transport (FT) settings, read the following important information:

- When the FT SAN Client feature is enabled or changed, a message appears to alert you that the appliance requires a restart. Before you enable or change this feature, it is recommended that you first suspend or cancel all jobs.
- When the FT for duplication feature is enabled or changed, the deduplication storage daemons are restarted. Before you enable or change this feature, it is recommended that you first suspend or cancel all jobs.

To change the Fibre Transport settings

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Network**, then select **Fibre Transport**.
- 3 Click to enable the **Enable SAN Client Fibre Transport on the Media Server (use FT for backups to this appliance)**
- 4 To enable the SAN Client FT option, do one of the following:
 - 2 target port configuration
Click **Enable SAN Client Fibre Transport on the Media Server (use FT for backups to this appliance)** and select **2 target port Fibre Channel connection**. Then, click **Save**.

When the message appears to alert you that the appliance requires a restart, click **OK** to continue or click **Cancel** to prevent a restart. Clicking **Cancel** does not change the state of the feature.

- 4 target port configuration

Click **Enable SAN Client Fibre Transport on the Media Server (use FT for backups to this appliance)** and select **4 target port Fibre Channel connection**. Then, click **Save**.

When the message appears to alert you that the appliance requires a restart, click **OK** to continue or click **Cancel** to prevent a restart. Clicking **Cancel** does not change the state of the feature.

- 5 Click to enable the **Enable the Fibre Transport to a Deduplication appliance (for duplication or backups)**.

Note: To use this feature with a NetBackup Deduplication Appliance, you must also enable Fibre Channel communication on the associated NetBackup 5020 or 5030. For complete information, see the *Symantec NetBackup Deduplication Appliance Software Administrator's Guide*. Refer to the section "Verifying, enabling, or disabling Fibre Channel communication".

- 6 To enable FT for duplication and backups to a NetBackup 5020 or 5030, click **Enable the Fibre Transport to a Deduplication appliance (for duplication or backups)**. Then, click **Save**.

Note: To use this feature with a NetBackup Deduplication Appliance, you must also enable Fibre Channel communication on the associated NetBackup 5020 or 5030. For complete information, see the *Symantec NetBackup Deduplication Appliance Software Administrator's Guide*. Refer to the section "Verifying, enabling, or disabling Fibre Channel communication".

- 7 Click **Save** to apply the changed settings.
- 8 To disable either one of the FT options, click the option to clear the check mark. Then, click **Save**.

- 9 To disable either one of the FT options, deselect the option to clear the check mark. Then, click **Save**.

If you selected to disable the FT SAN Client feature, an alert appears to inform you that the appliance requires a restart. Click **OK** to continue or click **Cancel** to prevent a restart. Clicking **Cancel** does not change the state of the feature.

If you selected to disable the FT for duplication feature, an alert appears to inform you that the deduplication storage daemons require a restart. Click **OK** to continue or click **Cancel** to prevent a restart. Clicking **Cancel** does not change the state of the feature.

- 10 After the appliance has been restarted, verify the FT settings that you selected as follows:
 - Log on to the NetBackup Appliance Web Console.
 - Click **Settings > Network**, then select **Fibre Transport**.
 - Verify that the settings are correct.

See [“Settings > Network > Fibre Transport”](#) on page 259.

Settings > Network > Host

The **Settings > Network > Host** tab enables you to configure the DNS configuration settings for DNS systems and the Host Name Resolution settings for non-DNS systems.

The **Settings > Network > Host** tab displays the **Host name** of your appliance.

Note: The host name can only be set during an initial configuration session. After the initial configuration has completed successfully, you can re-enter initial configuration by performing a factory reset on the appliance.

See [“About NetBackup appliance factory reset”](#) on page 141.

The remaining part of the **Settings > Network > Host** tab is divided into the following two sections:

- **Domain Name System** displays the fields for entering DNS configuration details.
- **Host Name Resolution** displays the fields for configuring systems that use the host name (non-DNS) details.

Changing DNS and Host Name Resolution (non-DNS) configuration settings

Use the following procedure to change or add the DNS and Host Name Resolution (non-DNS) configuration settings.

To change the DNS configuration settings

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Network > Host** tab.
- 3 Enter the appropriate information in the **DNS** data entry fields as follows:

Fields	Description
DNS IP Address(es)	<p>Enter the IP address of the DNS server. To enter multiple DNS server names, use a comma character as the delimiter between each name.</p> <p>The address can be either IPv4 or IPv6. Only global-scope and unique-local IPv6 addresses are allowed.</p> <p>See “About IPv4-IPv6-based network support” on page 264.</p>
Domain Name Suffix	Enter the suffix name of the DNS server.
Search Domain(s)	You can enter one or more DNS search domain names to search when an unqualified host name is given. To enter multiple search domain names, use a comma character as the delimiter between each name.

- 4 Click **Save**.

To change the Host Name Resolution (non-DNS) configuration settings

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Network > Host** tab.

- 3 Enter the **Host Name Resolution** configuration information using the following fields:

Fields	Description
IP Address	Enter the IP address of the appliance. The address can be either IPv4 or IPv6. Only global-scope and unique-local IPv6 addresses are allowed. See “About IPv4-IPv6-based network support” on page 264.
Fully qualified host name	Enter the Fully Qualified Host Name (FQHN) of the appliance.
Short host name	Enter the short name of the appliance. After you enter all of the necessary information in these fields, you must click Add .

- 4 Click **Save**.

About IPv4-IPv6-based network support

NetBackup appliances are 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.

Either the NetBackup Appliance Web Console or the NetBackup Appliance Shell Menu can be used to enter the IPv4 and IPv6 address information.

Review the following considerations for IPv6 addresses:

- NetBackup appliances do not support a pure IPv6 network. An IPv4 address must be configured for the appliance, otherwise the initial configuration (which requires the command `hostname set`) is not successful. For this command to work, at least one IPv4 address is required.

For example, suppose that you want to set the `hostname` of a specific host to `v46`. To do that, first make sure that the specific host has at least one IPv4 address and then run the following command:

```
Main_Menu > Network > Hostname set v46
```

- 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 master 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 master server, enter the IPv6 address of the appliance media server as follows:
Example:

```
Main > Network > Hosts add 9ffe::45 v45 v45
```

```
Main > Appliance > Add v45 <password>
```


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 enter only one IPv4 address for a network interface card (NIC) or bond. However, you can enter multiple IPv6 addresses for a NIC or bond.
- Network File System (NFS) or Common Internet File System (CIFS) protocols are supported over an IPv4 network on appliance. NFS or CIFS are not supported on IPv6 networks.
- The NetBackup client can now communicate with the media server appliance over IPv6.
- The `Main_Menu > Network > Hosts` command supports multiple IPv6 addresses to be assigned to the same host name having one network interface card (NIC). However, only one IPv4 address can be assigned to a specific host name having one NIC using this command.
- You can add an IPv6 address of a network interface without specifying a gateway address.
For more details, see the *NetBackup Appliance Command Reference Guide*.

Settings > Date and Time

On the **Settings > Date and Time** page, you can change the date, the time, and the time zone parameters that are added at the time of initial configuration.

Use the following procedure to change the date and time settings post-configuration.

To change the date, the time, and the time zone configuration

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Date and Time**.

3 Enter the appropriate information in the fields:

- | | |
|--------------------------|--|
| Select Time Zone | To assign a time zone to the appliance, click on the Time zone drop-down box and select the appropriate region, country, and time zone. |
| Set Date and Time | <p>You can select any one of the following options to set the date and the time for the appliance.</p> <ul style="list-style-type: none">■ Use NTP server date and time settings - Use this option to synchronize the appliance with an NTP server. In the Server IP or Host name field, specify the IP address or the host name of the NTP server■ Specify date and time - Use this option to manually specify the date and time. In the Date field, click the calendar to select the appropriate date (in month, date, and year or the mm/dd/yyyy format). In the Time field, enter the time in hh:mm:ss format. |

4 Click **Save**.

You can also configure the Date and Time settings using the `Main > Network > Date` commands under the NetBackup Appliance Shell Menu. For more information on the `Date` command refer to the *Symantec NetBackup Appliance Command Reference Guide*.

Settings > Authentication

The NetBackup appliance provides you authentication and authorization functions to help provide controlled user access to various administration interfaces. You can manage users both by GUI and NetBackup CLI.

- The **Authentication** feature lets you configure the appliance to authenticate various types of users so that they can access and manage the appliance.
- The **Authorization** feature lets you grant various types of users and user groups with specific access privileges on the NetBackup appliance. See [“Settings > Authentication > User Management”](#) on page 287.

For more information about the `Authentication` and `Authorization` commands, refer to the *NetBackup Appliance Command Reference Guide*.

About configuring user authentication

[Table 5-17](#) describes the options that are provided in the NetBackup Appliance Web Console and NetBackup Appliance Shell Menu for configuring the appliance to authenticate various types of users and grant them access privileges.

Table 5-17 User authentication management

User type	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Local (native user)	<p>Use the Settings > Authentication > User Management tab in the NetBackup Appliance Web Console to add local users.</p> <p>See “About authorizing NetBackup appliance users” on page 270.</p>	<p>The following commands and options are available under <code>Settings > Security > Authentication > LocalUser</code>:</p> <ul style="list-style-type: none">■ <code>Clean</code> - Delete all of the local users.■ <code>List</code> - List all of the local users that have been added to the appliance.■ <code>Password</code> - Change the password of a local user.■ <code>Users</code> - Add or remove one or more local users.

Table 5-17 User authentication management (*continued*)

User type	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
LDAP	<p>You can perform the following LDAP configuration tasks under Settings > Authentication > LDAP:</p> <ul style="list-style-type: none"> ■ Add a new LDAP configuration. ■ Import a saved LDAP configuration from an XML file. ■ Add, edit, and delete configuration parameters for the LDAP server. ■ Identify and attach the SSL certificate for the LDAP server. ■ Add, edit, and delete attribute mappings for the LDAP server. ■ Export the current LDAP configuration (including users) as an XML file. This file can be imported to configure LDAP on other appliances. ■ Disable and re-enable the LDAP configuration. ■ Unconfigure the LDAP server. <p>Use the Settings > Authentication > User Management tab in the NetBackup Appliance Web Console to add LDAP users and user groups.</p> <p>See “About authorizing NetBackup appliance users” on page 270.</p>	<p>The following commands and options are available under Settings > Security > Authentication > LDAP:</p> <ul style="list-style-type: none"> ■ Attribute - Add or delete LDAP configuration attributes. ■ Certificate - Set, view, or disable the SSL certificate. ■ ConfigParam - Set, view, and disable the LDAP configuration parameters. ■ Configure - Configure the appliance to allow LDAP users to register and authenticate with the appliance. * ■ Disable - Disable LDAP user authentication on the appliance. ■ Enable - Enable LDAP user authentication on the appliance. ■ Export - Export the existing LDAP configuration as an XML file. ■ 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. ■ Import - Import the LDAP configuration from an XML file. ■ 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 or object classes. ■ Show - View the LDAP configuration details. ■ Status - View the status of LDAP authentication on the appliance. ■ Unconfigure - Delete the LDAP configuration. ■ Users - Add or remove one or more LDAP users. Only the users groups that already exist on the LDAP server can be added to the appliance.

Table 5-17 User authentication management (*continued*)

User type	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Active Directory	<p>You can perform the following AD configuration tasks under Settings > Authentication > Active Directory:</p> <ul style="list-style-type: none"> ■ Configure a new Active Directory configuration. ■ Unconfigure an existing Active Directory configuration. <p>Use the Settings > Authentication > User Management tab in the NetBackup Appliance Web Console to add Active Directory users and user groups.</p> <p>See “About authorizing NetBackup appliance users” on page 270.</p>	<p>The following commands and options are available under Settings > Security > Authentication > ActiveDirectory:</p> <ul style="list-style-type: none"> ■ Configure - Configure the appliance to allow AD users to register and authenticate with the appliance. ■ 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. ■ 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 - Delete the AD configuration. ■ 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.
Kerberos-NIS	<p>You can perform the following Kerberos-NIS configuration tasks under Settings > Authentication > Kerberos-NIS :</p> <ul style="list-style-type: none"> ■ Configure a new Kerberos-NIS configuration. ■ Unconfigure an existing Kerberos-NIS configuration. <p>Use the Settings > Authentication > User Management tab in the NetBackup Appliance Web Console to add Kerberos-NIS users and user groups.</p> <p>See “About authorizing NetBackup appliance users” on page 270.</p>	<p>The following commands and options are available under Settings > Security > Authentication > Kerberos:</p> <ul style="list-style-type: none"> ■ Configure - Configure the appliance to allow NIS users to register and authenticate with the appliance. ■ 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. ■ List - List all of the NIS users and user groups that have been added to the appliance. ■ Status - View the status of NIS and Kerberos authentication on the appliance. ■ Unconfigure - Delete the NIS and Kerberos configuration. ■ 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.

Generic user authentication guidelines

Use the following guidelines for authenticating users on the appliance:

- Only one remote user type (such as LDAP, Active Directory (AD), and NIS) can be configured for authentication on an appliance at a given point in time. For example, if you currently authenticate LDAP users on an appliance, you must unconfigure LDAP on that appliance before you can switch to authenticating AD users.
- 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 Appliance Shell Menu.
- You cannot add a new user or a user group to an appliance if it has the same user name, user ID, or group ID as an existing user on that appliance.

See [“About authorizing NetBackup appliance users”](#) on page 270.

About authorizing NetBackup appliance users

[Table 5-18](#) describes the options that are provided for authorizing new and existing users or user groups through the NetBackup Appliance Web Console and NetBackup Appliance Shell Menu:

Table 5-18 User authorization management

Task	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Manage users	<p>The following options are available under Settings > Authentication > User Management</p> <ul style="list-style-type: none">■ View all of the users that have been added to the appliance.■ Expand and view all belonging users to a single user group.■ Add and delete local users.■ Add and delete LDAP/AD/Kerberos-NIS users and user groups.	<p>Use the Settings > Security > Authentication commands to add, delete, and view appliance users.</p> <p>See “About configuring user authentication” on page 267.</p>

Table 5-18 User authorization management (*continued*)

Task	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Manage user permissions (roles)	<p>The following options are available under Settings > Authentication > User Management:</p> <ul style="list-style-type: none"> ■ Grant and revoke the Administrator role for users and user groups. ■ Grant and revoke the NetBackupCLI role for users and user groups. ■ Synchronize members of registered user groups with Administrator role. 	<p>The following commands and options are available under Main > Settings > Security > Authorization:</p> <ul style="list-style-type: none"> ■ Grant Grant the Administrator and NetBackupCLI roles to specific users and users groups that have been added to the appliance. ■ List List all of the users and user groups that have been added to the appliance, along with their designated roles. ■ Revoke Revoke the Administrator and NetBackupCLI roles from specific users and users groups that have been added to the appliance. ■ SyncGroupMembers Synchronize members of registered user groups.

Notes about user management

- 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 Appliance Shell Menu.
- The NetBackupCLI role can be assigned to a maximum of nine (9) user groups at any given time.
- Active Directory (AD) user groups and user names support the use of a hyphen character in those names. The hyphen must appear between the first and the last character of a user name or a user group name. AD user names and user group names cannot begin or end with a hyphen.

NetBackup 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 5-19 User roles and privileges

User role	Privileges
NetBackupCLI	Users can only access the NetBackup CLI.
Administrator	Users can access the following: <ul style="list-style-type: none">■ NetBackup Appliance Web Console■ NetBackup Appliance Shell Menu■ NetBackup Administration Console

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 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 Appliance Shell Menu, an extra step is required. The user must enter the `switch2admin` command from the NetBackup CLI to access the NetBackup Appliance Shell Menu.

Granting privileges to users and user groups can be done as follows:

- From the NetBackup Appliance Web Console, on the **Settings > Authentication > User Management** page, click on the **Grant Permissions** link.
- From the NetBackup 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 [“About configuring user authentication”](#) on page 267.

See [“About authorizing NetBackup appliance users”](#) on page 270.

Settings > Authentication

The NetBackup appliance uses the built-in Pluggable Authentication Module (PAM) plug-in to support various authentication methods. The following directory service users can be configured and registered to log on to the appliance:

- Lightweight Directory Access Protocol (LDAP)
- Active Directory (AD)
- Kerberos-Network Information Service (Kerberos-NIS)

Settings > Authentication > LDAP

You can use the **Settings > Authentication** page of the NetBackup Appliance Web Console to configure the appliance to use LDAP server as a directory source to access user information and authenticate the users and user groups to access the appliance. But, only one authentication type can be configured in this appliance at one time. You can also import or export the LDAP configuration settings between multiple appliances.

Prerequisites

- You must have NetBackup Appliance 2.6 or higher installed to configure LDAP user authentication.
- LDAP schema must be RFC 2307 or RFC 2307bis compliant.
- 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.

Adding an LDAP server configuration

To configure an LDAP server

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication > LDAP** to expand the **LDAP Server Configuration**.
- 3 Select **Add new configuration**.

The appliance displays the fields to create a new configuration.

- 4 Enter the configuration information based on the following fields:

Field	Description	Example
Server Name/IP	Enter the FQDN or 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.	
Base DN	Enter the base directory name which is the top level of the LDAP directory tree.	OU= ExampleUsers, dc= mydomain
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.	DC=com
Password	Enter the password to access the LDAP server.	
Common User Name	Enter the name of an existing LDAP user on your LDAP server.	NBUApplianceAdmin
Common Group Name	Enter the name of an existing LDAP user group on your LDAP server.	

Field	Description	Example
SSL Certificate Required	<p>Displays a drop-down list to enable SSL certificate for your LDAP server. The drop-down list displays the following options:</p> <ul style="list-style-type: none"> ■ Yes - Select to enable adding an SSL certificate ■ No - Select to continue configuring the LDAP server without the SSL certificate ■ Start TLS <p>Note: When you use the Start TLS 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 Set Certificate option. For more information, refer to See "Setting the SSL certification" on page 276.</p>	
Validate UIDs and GIDs for Conflicts	Select the check-box to validate the User IDs and Group IDs and identify conflicting entries between the NetBackup appliance and the LDAP server.	

Note: The **Common User Name** and **Common Group Name** fields are not required to complete LDAP configuration. However, if you do not complete those fields, no LDAP users or LDAP groups appear under **Settings > Authentication > User Management** until you manually add them.

- 5 Click **Configure** to configure LDAP authentication using the entered parameters. The appliance configures and enables the new LDAP server and displays the **Attribute Mappings** and **Configuration Parameters** table.

Importing an LDAP server configuration

You can use the **Authentication Server Configuration** tab to import the details of an LDAP server and configure it with your appliance. The following procedure describes the steps to import a .xml file that includes the LDAP server configuration

details. The NetBackup appliance configures and connects to the LDAP server using these details.

Note: The `.xml` file must be saved and made available in the `/inst/patch/incoming` directory on the appliance.

To import an LDAP server configuration

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication > LDAP** to expand the **LDAP Server Configuration**.
- 3 Select the **Import existing configuration** option.
The appliance displays the **File Name** field.
- 4 Enter the absolute path to the `.xml` file in the **File Name** field.
The `.xml` file must be saved and made available in the `/inst/patch/incoming` directory on the appliance.
- 5 Click **Import**.
The appliance imports the `.xml` file. The appliance configures and connects to the LDAP server using the XML details.

Setting the SSL certification

You can use the **Authentication Server Configuration** tab 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 **Set SSL certificate** option is enabled only after the LDAP server is configured. The SSL certificate must be saved and made available in the `/inst/patch/incoming` directory on the appliance.

To set the SSL certificate

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication**.
The appliance displays the **Authentication Server Configuration** tab with the details of the configured LDAP server.

- 3 Click on the **Set Certificate** option that is displayed at the end of the tab.
The appliance displays a pop-up box to enter the path to the SSL certificate.

Note: The LDAP validation starts only after the server's root certificate is explicitly set using the **Set Certificate** option.

- 4 Enter the absolute path to the SSL certificate file in the **File Path** field.
The SSL certificate must be saved and made available in the `/inst/patch/incoming` directory on the appliance.
- 5 Click **OK**.
The appliance imports the SSL certificate and is used to authenticate the LDAP Server.

Exporting an LDAP configuration

You can use the **Authentication Server Configuration** tab 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 a `.xml` file.

Note: The **Export** option is enabled only after the LDAP server is configured.

To export the configuration file

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication**.
The appliance displays the **Authentication Server Configuration** tab with the details of the configured LDAP server.
- 3 Click on the **Export** option that is displayed at the end of the tab.
The appliance displays a pop box to enter the path for exporting the `.xml` file.
- 4 Enter a name for the `.xml` file.
You can only save the `.xml` file to the `/inst/patch/incoming` directory on the appliance.
- 5 Click **OK**.
The appliance converts the configuration details into an `.xml` file and exports it to the specified location.

Unconfiguring LDAP user authentication

You can use the **Authentication Server Configuration** tab to unconfigure LDAP user authentication. The following procedure describes the steps to unconfigure the LDAP server configuration.

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.

To unconfigure an LDAP server

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication**.

The appliance displays the **Authentication Server Configuration** tab with the details of the configured LDAP server.

- 3 Click on the **Unconfigure** option that is displayed at the end of the tab.

The appliance displays the following message:

```
Do you want to unconfigure the LDAP server?
```

- 4 Click **OK** to continue unconfiguring the LDAP server.

The appliance deletes the LDAP settings.

Enabling the LDAP server configuration

You can use the **Authentication Server Configuration** tab to enable the 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.

To enable the configured server

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication**.

The appliance displays the **Authentication Server Configuration** tab with the details of the configured LDAP server.

If the LDAP configuration is disabled, the following message is displayed on the **Server Configuration** tab next to the **Enable** option:

```
LDAP authentication is disabled.
```

- 3 Click on the **Enable** option.

The appliance displays the following message:

```
Are you sure you want to enable the configuration?
```

- 4 Click **OK** to enable the LDAP configuration.

The appliance enables the LDAP Server.

Disabling the LDAP server configuration

You can use the **Authentication Server Configuration** tab to disable LDAP authentication without unconfiguring it. The following procedure describes the options to disable LDAP user authentication.

To disable the configured server

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication**.

The appliance displays the **Authentication Server Configuration** tab with the details of the configured LDAP server.

If the LDAP configuration is enabled, the following message is displayed on the **Server Configuration** tab next to the **Disable** option.

```
LDAP authentication is enabled.
```

- 3 Click on the **Disable** option.

The appliance displays the following message:

```
Are you sure you want to disable the LDAP server?
```

- 4 Click **OK** to disable the LDAP server.

The appliance disables the LDAP server.

Deleting LDAP configuration parameters

When you configure LDAP user authentication, the server configuration parameters that you added or imported are displayed in the **Configuration Parameters** table on the **Authentication Server Configuration** tab. The following procedure describes the steps to delete LDAP configuration parameters.

To delete a configuration parameter

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication**.

The appliance displays the **Authentication Server Configuration** tab with the details of the configured LDAP server in the **Configuration Parameters** table.

- 3 Select the configuration parameter you want to delete.
- 4 Click the **Delete** option that is displayed at the top of the **Configuration Parameters** table.

The appliance displays the following message:

```
Are you sure you want to delete the configuration parameter?
```

- 5 Click **Yes** to proceed.

The deleted configuration parameter is removed from the **Configuration Parameters** table.

Adding LDAP configuration parameters

When you configure LDAP user authentication, the server configuration parameters that you added or imported are displayed in the **Configuration Parameters** table on the **Authentication Server Configuration** tab. The following procedure describes the steps to delete LDAP configuration parameters.

To add a configuration parameter

- 1 Log on to the NetBackup Appliance Web Console
- 2 Click **Settings > Authentication**.

The appliance displays the **Authentication Server Configuration** tab with the details of the configured LDAP server in the **Configuration Parameters** table.

- 3 Click the **Add** option that is displayed at the top of the **Configuration Parameters** table.

The appliance displays a new row in the **Configuration Parameters** table with the **Update** and **Cancel** options.

- 4 Enter the name of the new configuration parameter in the **Name** field.
- 5 Enter the value of the configuration parameter in the **Value** field.
- 6 Click **Update**.

The new configuration parameter is added to the **Configuration Parameters** table.

Adding an LDAP attribute mapping

When you add a new LDAP configuration, its attribute mappings are added or imported and displayed in the **Attribute Mappings** table on the **Authentication Server Configuration** tab. 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 Appliance Web Console.
- 2 Click **Settings > Authentication**.

The appliance displays the **Authentication Server Configuration** tab with the details of the configured LDAP server in the **Attribute Mappings** table.

- 3 Click the **Add** option that is displayed at the top of the **Attribute Mappings** table.

The appliance displays a new row in the **Attribute Mappings** table with the **Update** and **Cancel** options.

- 4 Enter the mapping type in the **Map Type** field.
- 5 Enter the NSS value in the **NSS Value** field.

- 6 Enter the LDAP value for the attribute in the **LDAP Value** field.
- 7 Click **Update**.

The new attribute mapping is added to the **Attribute Mappings** table.

Deleting an LDAP attribute mapping

When you add a new LDAP configuration, its attribute mappings are added or imported and displayed in the **Attribute Mappings** table on the **Authentication Server Configuration** tab. 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 Appliance Web Console.
- 2 Click **Settings > Authentication**.

The appliance displays the **Authentication Server Configuration** tab with the details of the configured LDAP server in the **Attribute Mappings** table.
- 3 Select the attribute mapping you want to delete in the **Attribute Mappings** table.
- 4 Click the **Delete** option that is displayed at the top of the **Attribute Mappings** table.

The appliance displays the following message:

Are you sure you want to delete the configuration parameter?

- 5 Click **Yes** to proceed.

The deleted attribute mapping is removed from the **Attribute Mappings** table.

Settings > Authentication > Active Directory

You can use the **Settings > Authentication** page of the NetBackup Appliance Web Console to configure the appliance to use Active Directory (AD) server as a directory source to access user information and authenticate the users and user groups to access the appliance. But, only one authentication type can be configured in this appliance at one time.

Prerequisites

- You must have NetBackup Appliance 2.6.0.3 or higher installed to configure AD user authentication.
- 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.

- Ensure that the authorized domain user credentials are used to configure the AD server with the appliance.
- Configure the NetBackup 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.

Adding an Active Directory server configuration

You can use the **Authentication** tab 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 procedure describes the steps to configure Active Directory user authentication.

To configure an Active Directory server

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication**.

Three types of authentication server appear.

- 3 Click **Active Directory** to expand the Active Directory configuration list.

Note: Before you configure a new Active Directory authentication, verify the DNS of appliance directs to the Active Directory server or Active Directory DNS server.

- 4 Enter the following parameters:

Field	Description	Example
Server Name or IP	Enter the Active Directory server name or IP address. The recommended method is to use the Fully Qualified Domain Name (FQDN) for the Active Directory server.	10.200.210.229
Username	Enter the username of the AD server Administrator.	admin
Password	Enter the password of the AD server Administrator..	P@ssw0rd

- 5 Click **Configure** to apply the Active Directory authentication parameters to the appliance.

You can check the authentication status when the configuration process is complete.

Unconfiguring the Active Directory user authentication

You can stop authenticating the AD user from the appliance. The following procedure describes the steps to unconfigure the Active Directory server configuration.

Note: To unconfigure the Active Directory authentication from the appliance, you must have the Administrator authority on the AD server.

Note: You must remove the roles of all Active Directory users and user groups before the unconfigure process begins.

To unconfigure an Active Directory server

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication**.
The details of the configured Active Directory server are displayed.
- 3 Enter the **Username** and **Password** of an administrator on Active Directory server.

- 4 Click **Unconfigure**.
A warning dialog box pops up.
- 5 Click **Yes** to continue with the unconfigure process.
Click **No** to cancel the unconfigure process.

Settings > Authentication > Kerberos-NIS

You can use the **Settings > Authentication** page of the NetBackup Appliance Web Console to configure the appliance to use NIS server as a directory source for users and user groups to access the appliance. The appliance requires that NIS users authenticate using Kerberos.

Prerequisites

- You must have NetBackup Appliance 2.6.1.1 or higher installed to configure Kerberos-NIS user authentication.
- 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.
- Ensure that the Kerberos server is available and properly configured to communicate with the NIS domain.
- Due to the strict time requirements of Kerberos, Symantec strongly recommends that you use an NTP server to synchronize time between the appliance, the NIS server, and the Kerberos server.

Adding a Kerberos-NIS authentication configuration

You can use the **Authentication** tab to add the details of a NIS server with Kerberos authentication and configure it with your appliance. The Kerberos and NIS servers enable you to access the directory information services for your appliance. The following procedure describes the steps to configure Kerberos-NIS user authentication.

To configure a Kerberos-NIS authentication

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication**.
Three types of authentication server appear.
- 3 Click **Kerberos-NIS** to expand the Kerberos-NIS configuration list.

- 4 Enter the following parameters:

Field	Description	Example
NIS Server Name or IP	Enter the NIS server name or IP address. We recommend that you use the Fully Qualified Domain Name(FQDN) for the NIS server.	BCFTNIS or 10.200.38.222
NIS Domain	Enter the domain for the NIS server.	BCFTNIS
Kerberos Server Name or IP	Enter the Kerberos server name or IP address. We recommend that you use the Fully Qualified Domain Name(FQDN) for the NIS server.	BCFTKBR or 10.200.38.225
Kerberos Realm	Enter the realm for the Kerberos server.	BCFTKBR
Kerberos Domain	Enter the domain for the Kerberos server.	BCFT

- 5 Click **Configure** to apply the Kerberos-NIS authentication using the entered parameters.

The configured parameters display in the **Configuration Parameters** when the authentication configuration process is completed successfully.

Unconfiguring the Kerberos-NIS user authentication

You can stop authenticating the Kerberos-NIS users from the appliance. The following procedure describes the steps to unconfigure the Kerberos-NIS server authentication.

Note: Make sure that you have deleted all Kerberos-NIS users and user groups before the unconfigure process starts.

To unconfigure a Kerberos-NIS authentication

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication**.

The **Configuration Parameters** table with the details of the configured Kerberos-NIS authentication shows in the **Authentication Server Configuration** tab.

- 3 Click **Unconfigure**.
A warning dialog box pops up.
- 4 Click **Yes** to apply the unconfigure process.
Click **No** to cancel the unconfigure process.

Settings > Authentication > User Management

You can use the **Settings > Authentication > User Management** page of the NetBackup Appliance Web Console to do the following tasks:

- View all of the users that have been added to the appliance.
- Expand and view all of the users belonging to a single user group.
- Add and delete local users.
- Add and delete LDAP users and user groups.
- Grant Administrator user permissions to local, LDAP, AD, and Kerberos-NIS users.
- Grant Administrator user permissions to LDAP, AD, and Kerberos-NIS user groups.
- Grant NetBackupCLI user permissions to LDAP, AD, and Kerberos-NIS users.
- Grant NetBackupCLI user permissions to LDAP, AD, and Kerberos-NIS user groups.
- Revoke Administrator user permissions from local, LDAP, AD, and Kerberos-NIS users.
- Revoke Administrator user permissions from LDAP, AD, and Kerberos-NIS user groups.
- Revoke NetBackupCLI user permissions from LDAP, AD, and Kerberos-NIS users.
- Revoke NetBackupCLI user permissions from LDAP, AD, and Kerberos-NIS user groups.
- Sync group members with the Administrator role.

Note: Kerberos-NIS users and user groups are displayed as **Kerberos** in the **Type** column.

Adding appliance users

You can use the **User Management** tab to add new users to the NetBackup appliance. The following procedure describes how to add new users.

To add new users

- 1 Log on to the NetBackup Appliance Web Console
- 2 Click the **Settings > Authentication > User Management** tab.
The appliance displays the **User Management** tab.
- 3 Click on the **Add User** option that is displayed at the end of the **User Management** tab.
The appliance displays the **Add User** pop-up dialog box.
- 4 Select the type of user from the **User Type** drop-down list. The drop-down list displays the following options depending on your configuration:
 - **Local** - Select this option to add a local user to the appliance database.
 - **LDAP** - Select this option to register a user that is already present on the LDAP server that you have configured with your appliance.

Note: If you do not register (add) a remote (LDAP, etc.) user with the appliance, that user cannot access the appliance.

- 5 Enter the name of the user in the **User Name** field.
- 6 If you selected a **Local** user type from the **User Type** drop-down list, enter a password for the new user in the **Password** field. Valid passwords must include the following:
 - Eight or more characters
 - At least one lowercase letter
 - At least one number (0-9)

Uppercase letters and special characters can be included, but they are not required.

The following describes password restrictions:

- 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.

You or the new user can change their password at a later time on the **Settings > Password > Password Management** page.

- 7 Reenter the password in the **Confirm Password** field.

- 8 Click **Save**.

The appliance adds the new user and displays the following message:

```
User added successfully.
```

- 9 Click **OK** to continue.

The new user is added to the list of users on the **User Management** tab.

Deleting appliance users

As a matter of best practice, you should delete a registered user or user group from the NetBackup 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.

You can use the **User Management** tab to delete users from the NetBackup appliance. The following procedure describes how to delete existing users.

To delete existing users

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click the **Settings > Authentication > User Management** tab.

The appliance displays the **User Management** tab.

- 3 Select the user that you want to delete.
- 4 Click on the **Delete User** option that is displayed at the end of the **User Management** tab.

The appliance displays the following message:

```
User Deleted Successfully
```

- 5 Click **OK** to continue.

The selected user is deleted from the appliance and removed from the **User Management** tab.

Adding appliance user groups

You can use the **User Management** tab to add new user groups to the NetBackup appliance from a registered directory service, such as LDAP. The following procedure describes how to add new user groups.

To add user group

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click the **Settings > Authentication > User Management** tab.
The appliance displays the **User Management** tab.
- 3 Click on the **Add Group** option that is displayed at the end of the **User Management** tab.
The appliance displays the **Add Group** pop-up dialog box.
- 4 Enter the name of the user group in the **Group Name** field.

Note: If you do not register (add) a remote (LDAP, etc.) user group with the appliance, the users belonging to that user group cannot access the appliance.

- 5 Click **Save**.
The appliance adds the new user group and displays the following message:

Group Added Successfully

- 6 Click **OK** to continue.
The user group is added to the list of users and user groups on the **User Management** tab.

Deleting appliance user groups

As a matter of best practice, you should delete a registered user or user group from the NetBackup 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.

You can use the **User Management** tab to delete user groups from the NetBackup appliance. The following procedure describes how to delete existing user groups.

To delete user groups:

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click the **Settings > Authentication > User Management** tab.
The appliance displays the **User Management** tab.
- 3 Select the user group that you want to delete.

- 4 Click on the **Delete Group** option that is displayed at the end of the **User Management** tab.
- 5 Click **OK** to continue.

The appliance displays the following message:

```
Group Deleted Successfully
```

The selected user group is deleted from the appliance and removed from the **User Management** tab.

Granting roles to users and user groups

You can use the **User Management** tab to grant roles to appliance users and user groups that grant them different types of permissions to access the appliance. The following procedure describes how to grant roles to existing users and user groups.

To grant administrative roles to users and user groups

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click the **Settings > Authentication > User Management** tab.
The appliance displays the **User Management** tab.
- 3 Select a user or user group that has **NoRole** displayed in the **Role** column.
- 4 Click on the **Grant Permission** option that is displayed at the end of the **User Management** tab.

Depending on your configuration, the appliance displays the **Grant Permissions** pop-up dialog box:

- Select the **Administrator** option to grant the Administrator user role to the selected user or user group.
- Select the **NetBackupCLI** option to grant the NetBackupCLI user role to the selected user or user group.

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 from the NetBackup Appliance Shell Menu.

- 5 Click **OK** to continue.

The term **Administrator** or **NetBackupCLI** is displayed in the **Role** column for the selected user.

Revoking roles from users and user groups

You can use the **User Management** tab to revoke roles from appliance users and user groups to limit their permissions to access the appliance. The following procedure describes how to revoke roles from existing users and user groups.

To revoke roles

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click the **Settings > Authentication > User Management** tab.
The appliance displays the **User Management** tab.
- 3 Select a user or user group that has the **Administrator** or **NetBackupCLI** role displayed in the **Role** column.
- 4 Click on the **Revoke Permission** option that is displayed at the end of the **User Management** tab.
- 5 Click **OK** to continue.

The appliance displays the following message:

```
User Un-authorized Successfully
```

The term **NoRole** is displayed in the **Role** column for the selected user or user group.

Synchronizing the user groups

You can use the **User Management** tab to synchronize the user group members. The following procedure describes how to synchronize the user groups between the appliance and the servers for LDAP, AD, and NIS.

Also you can schedule a sync start time by using the `Settings > Security > Authorization > SyncGroupMembers` command in the NetBackup Appliance Shell Menu. For more information, refer to the *NetBackup Appliance Command Reference Guide*.

To sync the user groups

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click the **Settings > Authentication > User Management** tab.
The appliance displays the **User Management** tab.
- 3 Select a user group from the list.
- 4 Click on the **Sync Group Members** option that is displayed on the right top corner of the **User Management** tab.
- 5 Click **Sync** to sync user group members immediately.

Settings > Password Management

After the initial configuration, you can change the appliance user password from the **Settings > Password > Password Management** page.

Note: For maximum security, Symantec recommends that you set a regular schedule for password changes and keep a record of all passwords in a secure location.

When the password is changed here, it is also updated for use with the command-line interface. If you change this password from the command-line interface, the new password is also used to log on to the appliance user interface.

[Table 5-20](#) describes the data entry fields on the **Password Management** page.

Table 5-20 Data entry fields for administrator password change

Field	Description
User Name	Enter your current user name.
Old Password	Enter the current password. If the current password is the factory default password, enter P@ssw0rd .
New Password	Enter the new password. Valid passwords must include the following: <ul style="list-style-type: none">■ Eight or more characters■ At least one lowercase letter■ At least one number (0-9) Uppercase letters and special characters can be included, but they are not required. The following describes password restrictions: <ul style="list-style-type: none">■ 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.
Confirm New Password	Re-enter the new password for confirmation.
Reset Password	Click this item to commit the password change.
Clear Fields	Click this item to remove the data from all fields and start over.

You can also configure the Password settings using the `Main > Settings > Password` commands under the shell menu. For more information refer to the *Symantec NetBackup Appliance Command Reference Guide*.

See [“About modifying the appliance settings”](#) on page 225.

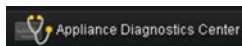
Troubleshooting

This chapter includes the following topics:

- [Troubleshooting and tuning appliance from the Appliance Diagnostics Center](#)
- [Viewing log files using the Support command](#)
- [Where to find NetBackup appliance log files using the Browse command](#)
- [About password recovery](#)
- [About disaster recovery](#)
- [Gathering device logs with the DataCollect command](#)
- [Setting a NetBackup 5330 storage shelf component to the Service Allowed mode](#)

Troubleshooting and tuning appliance from the Appliance Diagnostics Center

You can troubleshoot multiple failures and resolve issues in the NetBackup appliance by using some interactive self-repair wizards in the Appliance Diagnostics Center. Each wizard helps you perform specific diagnostic tasks. Some of the wizards also guide you through system optimization and tuning. These wizards can be accessed by clicking the Appliance Diagnostics Center icon on the NetBackup Appliance Web Console. The icon is located on the upper-right corner of the NetBackup Appliance Web Console and looks like the following:

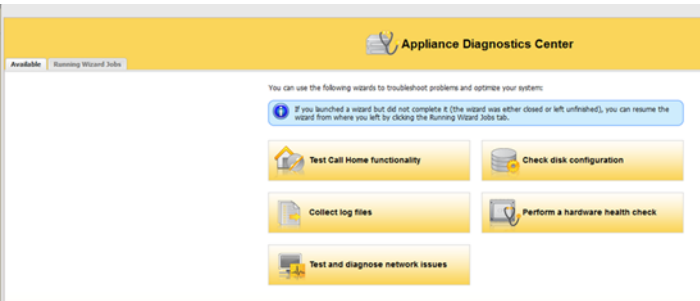


When you click this icon, the Appliance Diagnostics Center page appears where you can see the **Available** and the **Running Wizard Jobs** tab. You can return to the NetBackup Appliance Web Console by closing this page.

All the troubleshooting wizards are listed under the **Available** tab.

Figure 6-1 shows a sample view of the **Available** tab.

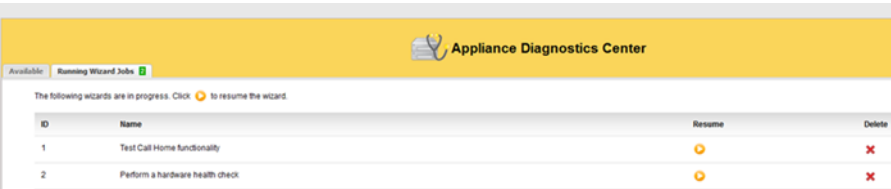
Figure 6-1 Available tab



The **Running Wizard Jobs** tab lists the wizards that were started but are not complete yet. If you close a wizard without completing it (using the cross icon) or leave it unfinished, it is listed under the **Running Wizard Jobs** tab. You can resume or delete these active wizards by clicking the respective icons from the **Resume** or **Delete** columns.

Figure 6-2 shows a sample view of the **Running Wizard Jobs** tab.

Figure 6-2 Running Wizard Jobs tab



You can do the following to run the wizards from the **Available** tab:

- Click **Test Call Home functionality**
- Use this wizard to troubleshoot Call Home failures. The wizard checks if Call Home is enabled, the Call Home proxy server (or proxy server) is enabled, and if Appliance, proxy server, and the Symantec Call Home server can communicate.

Click Check Disk Configuration	<p>Use this wizard to troubleshoot disk storage issues, tuning, and availability. The wizard checks the storage partitions like AdvancedDisk, etc., and does the following:</p> <ul style="list-style-type: none">■ Checks if the storage paths are mounted. If they are not mounted, it provides an option for you to mount them.■ Checks if the disk pool and disk volumes are up and running. If they are not running, the wizard provides an option for you to reset them.■ Checks if PureDisk services are up and running. If they are not running, the wizard helps to start these services.
Click Collect Log files	<p>Use this wizard to collect log files from an Appliance.</p> <p>The wizard lets you collect different types of log files like NetBackup, Appliance, operating system, PureDisk, GUI, NBSU (NetBackup Support Utility), DataCollect etc. Note that it may take several minutes to collect the NetBackup logs.</p> <p>Table 6-1 lists details about the log files that are collected by the wizard.</p> <p>You can choose to email the log files to recipients, download to your computer, or upload them to Symantec Support.</p> <p>Review the following points if you want to email the log files:</p> <ul style="list-style-type: none">■ SMTP must be configured for emailing the logs. You can configure SMTP from Settings > Notification > Alert Configuration in the NetBackup Appliance Web Console.■ To email the logs, the collected log size must be 10 MB or less.
Click Perform a hardware health check	<p>Use this wizard to perform a hardware health check of your environment. The wizard helps you determine if hardware components like CPU, Disk, Fan, RAID, are working fine.</p>
Click Test and diagnose network issues	<p>Use this wizard to check the network connectivity of your Appliance with the master server, media servers, storage servers, and clients. The wizard helps you to quickly test and diagnose network-related issues.</p>

[Table 6-1](#) lists the log files that are collected by the Collect Log Files Wizard. The logs are collected based on the log type that you specify. If you are collecting NetBackup logs, you can also specify the time frame for which you want to collect the logs.

Table 6-1 Log files collected by the Collect Logs Wizard

Log Type	What is collected?
NetBackup	<p>Logs created by the NetBackup Copy Logs tool (<code>nbcplogs</code>). These include the following:</p> <ul style="list-style-type: none">■ NetBackup legacy logs■ NetBackup VxUL (Unified) logs■ NetBackup OpsCenter logs■ NetBackup PureDisk logs■ Windows Event logs (Application, System, Security)■ PBX logs■ NetBackup database logs■ NetBackup database error logs■ NetBackup database trylogs■ Vault session logs■ Volume Manager debug logs■ VxMS logs, if enabled <p>Note: The legacy logs and the VXlogs are collected based on the time frame that you specify.</p>

Table 6-1 Log files collected by the Collect Logs Wizard (*continued*)

Log Type	What is collected?
Appliance	<p>Appliance logs including upgrade, hardware, event logs and so on. The following Appliance logs are collected:</p> <ul style="list-style-type: none"> ■ <code>hostchange.log</code>, <code>selftest_report*</code> ■ Logs created by the <code>CallhomeDataGather</code> utility. ■ <code>config_nb_factory.log</code>, <code>iso_postinstall.log</code>, <code>sf.log</code> ■ <code>patch_*</code>, <code>upgrade_*</code> logs ■ NetBackup Appliance VxUL (Unified) logs, which include: <ul style="list-style-type: none"> ■ All ■ CallHome ■ Checkpoint ■ Common ■ Config ■ Database ■ Hardware ■ HWMonitor ■ Network ■ RAID ■ Seeding ■ SelfTest ■ Storage ■ SWUpdate ■ Commands ■ CrossHost ■ Trace <p>Note: The NetBackup Appliance unified logs are not the same as the NetBackup unified logs, such as <code>nbpem</code> or <code>nbjm</code>. NetBackup Appliance has its own set of unified logs. To collect the NetBackup unified logs, select NetBackup in the Collect Logs Wizard.</p>
Operating system	<p>Operating system logs that include the following:</p> <ul style="list-style-type: none"> ■ <code>boot.log</code> ■ <code>boot.msg</code> ■ <code>boot.omsg</code> ■ <code>messages</code>

Table 6-1 Log files collected by the Collect Logs Wizard (*continued*)

Log Type	What is collected?
Deduplication (Media Server Deduplication Pool or PureDisk)	All logs related to Media Server Deduplication Pool (MSDP) are collected under the following directories: <DIR> PD <ul style="list-style-type: none"> ■ /var/log/puredisk ■ /msdp/data/dpl/pdvol/log
NetBackup Appliance Web Console	All logs related to NetBackup Appliance Web Console logs are collected under the following directories: /log/webgui
NetBackup support utility (nbsu)	Diagnostic information about NetBackup and the operating system.
DataCollect	Hardware and storage device logs. The logs created by the DataCollect utility are collected.

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 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 `GUI` directory, the prompt appears as `LOGROOT/GUI/>`. From that prompt you can use the `ls` command to display the available log files in the `GUI` 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 appliance log files using the Browse command”](#) on page 302.

To view NetBackup Appliance unified (VxUL) logs using the `Support > Logs` command:

- 1 You can view the NetBackup 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.
 - `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. The available module names are: All, CallHome, Checkpoint, Common, Config, Database, Hardware, HWMonitor, Network, RAID, Seeding, SelfTest, Storage, SWUpdate, Commands, CrossHost, and Trace.
Use to display debug information for a specific module. The available module names are: All, CallHome, Checkpoint, Common, Config, Database, FTMS, Hardware, HWMonitor, Network, RAID, Seeding, SelfTest, Storage, SWUpdate, Commands, CrossHost, and Trace.
- 2 If you want, you can copy the unified logs with the `Main > Support > Share Open` command. Use the desktop to map, share, and copy the logs.

Note: The NetBackup Appliance unified logs are not the same as the NetBackup unified logs, such as `nbpem` or `nbjm`. NetBackup Appliance has its own set of unified logs. To collect the NetBackup unified logs, use the Collect Logs Wizard and select **NetBackup**.

See [“Troubleshooting and tuning appliance from the Appliance Diagnostics Center”](#) on page 295.

You can also use the `Main_Menu > Support > Logs` commands to do the following:

- Upload the log files to Symantec Technical Support.
- Set log levels.
- Export or remove CIFS and NFS shares.

Note: The NetBackup Appliance VxUL logs are no longer archived by a cron job, or a scheduled task. In addition, log recycling has been enabled, and the default number of log files has been set to 50.

Refer to the *NetBackup Appliance Command Reference Guide* for more information on the above commands.

Where to find NetBackup appliance log files using the Browse command

Table 6-2 provides the location of the logs and the log directories that are accessible with the `Support > Logs > Browse` command.

Table 6-2 NetBackup appliance log file locations

Appliance log	Log file location
Configuration log	<DIR> APPLIANCE config_nb_factory.log
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 <ul style="list-style-type: none"> <DIR> netbackup <DIR> openv <DIR> volmgr
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
NetBackup Administrative web user interface log and the NetBackup web server log	<DIR> WEBGUI <ul style="list-style-type: none"> <DIR> gui <DIR> webserver

Table 6-2 NetBackup appliance log file locations (*continued*)

Appliance log	Log file location
Device logs	/tmp/DataCollect.zip You can copy the DataCollect.zip to your local folders using the Main > Support > Logs > Share Open command.

About password recovery

Symantec understands that there may be situations where you need to recover your administrator (admin) password. For example, an employee that maintains the password may leave the company, or you may lose or forget the password.

If any of these situations occur, refer to the following tech note on the Symantec Support website:

<http://www.symantec.com/docs/TECH189518>

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 Symantec 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 primary (master server) appliance offers the least amount of recovery solutions. A failure that is severe enough to bring your appliance down, may mean that it is impossible to recover the data on the system. Symantec's support engineers work with you to determine whether they can recover your appliance. If your appliance is not recoverable, then Support may suggest that you rebuild your appliance. If that option is not feasible, then you may need to replace your appliance completely.

However, an appliance that is configured with one or more secondary appliances, or configured with a tape storage unit, there is a much better chance that its data can be recovered.

You can also configure Auto Image Replication between appliances.

See [“About Auto Image Replication between appliances”](#) on page 219.

Symantec 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.symantec.com/docs/DOC5332>

Gathering device logs with the DataCollect command

You can use the `DataCollect` command from the `Main > Support` shell menu to gather device logs. You can share these device logs with the Symantec Support team to resolve device-related issues.

Along with the operating system, IPMI, and storage logs, the `DataCollect` command now collects the following logs as well:

- Patch logs
- File System logs
- Test hardware logs
- CPU information
- Disk performance logs
- Memory information
- Hardware information

To gather device logs with the `DataCollect` command

- 1 Log on to the administrative NetBackup Appliance Shell Menu.
- 2 Open the Support menu. To open the support menu, use the following command:

```
Main > Support
```

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

3 Enter the `DataCollect` command to gather storage device logs.

The appliance initiates the following procedure:

```

appliancel23.Support > DataCollect
Gathering release information
Gathering dmidecode logs
Gathering ipmitool sel list logs
Gathering fwtermlog logs
Gathering AdpEventLog logs
Gathering smartctl logs
Gathering disk performance logs
Gathering ipmiutil command output
Gathering cpu information
Gathering memory information
Gathering sdr logs
Gathering adpallinfo logs
Gathering encinfo logs
Gathering cfgdsply logs
Gathering ldpdinfo logs
Gathering pdlist logs
Gathering fru logs
Gathering adpbucmd logs
Gathering os logs
Gathering adpalilog logs
Gathering dfinfo logs
Gathering vxprint logs
Gathering Test Hardware logs
Gathering patch logs

```

```

All logs have been collected in /tmp/DataCollect.zip
Log file can be collected from the appliance shared folder
- \\appliancel23\logs\APPLIANCE
Share can be opened using Main->Support->Logs->Share Open

```

```

=====End of DataCollect=====
All logs have been collected in /tmp/DataCollect.zip

```

The appliance generates the device log in the `/tmp/DataCollect.zip` file.

- 4 Copy the `DataCollect.zip` to your local folders using the `Main > Support > Logs > Share Open` command.
- 5 You can send the `DataCollect.zip` file to the Symantec Support team to resolve your issues.

Setting a NetBackup 5330 storage shelf component to the Service Allowed mode

Before service or replacement can be performed on a Primary Storage Shelf or an Expansion Storage Shelf, the specific component of the unit must be set to the Service Allowed mode.

Typically, a failure automatically sets the component of the affected unit to the Service Allowed mode. When a warning of an impending failure occurs, the component is not automatically set to the Service Allowed mode. For this situation, you must set the component to the Service Allowed mode manually, by using the NetBackup Appliance Shell Menu.

In the `Main_Menu > Support` view, two main commands are available:

- `ServiceAllowed Set PrimaryShelf`
This command is used with options to set the appropriate Primary Storage Shelf component to the Service Allowed mode.
- `ServiceAllowed Set ExpansionShelf`
This command is used with options to set the appropriate Expansion Storage Shelf component to the Service Allowed mode.

The following describes the available command options for setting a Primary Storage Shelf component or an Expansion Storage Shelf component to the Service Allowed mode.

Table 6-3 Service Allowed command options

Storage unit	Command options
Primary Storage Shelf	<ul style="list-style-type: none"> Controller Set the Service Allowed flag for a Primary Shelf Controller. When you enter this option, you must also identify the controller location (A/B). The following shows the complete command: ServiceAllowed Set PrimaryShelf Controller A/B On/Off FanCanister Set the Service Allowed flag for a Primary Shelf fan canister. When you enter this option, you must also identify the fan canister location (Left/Right).The following shows the complete command: ServiceAllowed Set PrimaryShelf FanCanister Left/Right On/Off HDD Set the Service Allowed flag for a Primary Shelf hard disk drive. When you enter this option, you must also identify the drawer location (DrawerID) and the disk drive location (SlotNo). The following shows the complete command: ServiceAllowed Set PrimaryShelf HDD DrawerID SlotNo On/Off <p>Note: Before you run this command, first run the Monitor > Hardware ShowHealth PrimaryShelf RAID command. Refer to the "Precautions and guidelines" section for more information.</p> PowerCanister Set the Service Allowed flag for a Primary Shelf power canister. When you enter this option, you must also identify the power canister location (Top/Bottom). The following shows the complete command: ServiceAllowed Set PrimaryShelf PowerCanister Top/Bottom On/Off

Table 6-3 Service Allowed command options (*continued*)

Storage unit	Command options
Expansion Storage Shelf	<ul style="list-style-type: none"> ExpansionCanister Set the Service Allowed flag for an Expansion Shelf canister. When you enter this option, you must also identify the canister location (<i>Top/Bottom</i>). The following shows the complete command: <pre>ServiceAllowed Set ExpansionShelf ExpansionCanister Top/Bottom On/Off</pre> FanCanister Set the Service Allowed flag for a Primary Shelf fan canister. When you enter this option, you must also identify the fan canister location (<i>Left/Right</i>). The following shows the complete command: <pre>ServiceAllowed Set ExpansionShelf FanCanister Left/Right On/Off</pre> HDD Set the Service Allowed flag for an Expansion Shelf hard disk drive. When you enter this option, you must also identify the expansion shelf ID (<i>ExpansionShelfID</i>), the drawer location (<i>DrawerID</i>), and the disk drive location (<i>SlotNo</i>). The following shows the complete command: <pre>ServiceAllowed Set ExpansionShelf HDD ExpansionShelfID DrawerID SlotNo On/Off</pre> <p>Note: Before you run this command, first run the <code>Monitor > Hardware ShowHealth PrimaryShelf RAID</code> command. Refer to the "Precautions and guidelines" section for more information.</p> PowerCanister Set the Service Allowed flag for a Primary Shelf power canister. When you enter this option, you must also identify the power canister location (<i>Top/Bottom</i>). The following shows the complete command: <pre>ServiceAllowed Set ExpansionShelf PowerCanister Top/Bottom On/Off</pre>

Precautions and guidelines

Symantec requires that you perform this procedure only with assistance from Symantec Technical Support. It is important to understand that certain situations can adversely affect system operation. Care must be taken when you run the Service Allowed command options.

To keep your system at peak performance, fix each problem as it occurs and do not let problems accumulate. Multiple problems can degrade system performance and make servicing the system more difficult. Multiple problems can also increase the potential for a situation that may cause data loss.

The following describes how the Service Allowed mode may affect the system:

- Degraded performance

In some situations, setting a component to the Service Allowed mode can cause degraded performance. A message appears to alert you of this possibility before you proceed. For example, when you use the `Controller` option for the Primary Shelf, the following message appears:

```
Support> ServiceAllowed Set PrimaryShelf Controller A on
Service allowed flag is used for component replacement. Setting
this flag may cause performance degradation due to write cache
being turned off.
>> Do you want to continue? (yes, no):
```

- RAID volume status in Degraded state

When you use the `HDD` option to set a hard disk drive to the Service Allowed mode, the following message appears:

```
Support> ServiceAllowed Set PrimaryShelf HDD 1 2 on
Service allowed flag is used for component replacement. Before
you set this flag, run the
'Monitor->Hardware ShowHealth PrimaryShelf RAID' command to
make sure that this Hard Disk Drive (HDD) is in a RAID volume
with a status of Optimal. If the RAID volume status is not Optimal,
executing this command creates a RISK OF POTENTIAL DATA LOSS.
>> Do you want to continue? (yes, no): no
```

In this situation, the best practice is to enter `no`. Then you must resolve the current RAID volume issue to return it to Optimal status. Only then can you proceed with setting the affected hard disk drive to the Service Allowed mode. Symantec recommends that before you attempt to set any hard disk drive to the Service Allowed mode, first run the `Monitor > Hardware ShowHealth PrimaryShelf RAID` command. Check to make sure that the hard disk drive that you want to set to the Service Allowed mode is in a RAID volume with Optimal status.

Warning: Make sure that you contact and work with Symantec Technical Support for guidance to avoid any situation that may cause the potential for data loss.

The following procedure describes how to set a Primary Storage Shelf or an Expansion Storage Shelf component to the Service Allowed mode.

To set a Primary Storage Shelf or an Expansion Storage Shelf component to the Service Allowed mode

- 1 Contact Symantec Technical Support and inform the representative that you need to set a storage shelf component to the Service Allowed mode.
Allow the representative to assist you with the remaining steps that follow.
- 2 Log in to the NetBackup Appliance Shell Menu.
- 3 Enter `Main_Menu > Support`.
- 4 From the list of commands in [Table 6-3](#), enter the appropriate command.

Note: Before you attempt to set a hard disk drive to the Service Allowed mode, first run the `Monitor > Hardware ShowHealth PrimaryShelf RAID` command. Refer to the "Precautions and guidelines" section for more information.

- 5 Verify that the component is in the Service Allowed mode by checking that the blue Service Action Allowed LED on the affected storage shelf is on.
- 6 Perform the necessary work on the affected unit.
After the work has been completed and the unit has been restored to normal operation, the Service Allowed mode is cleared automatically.

Deduplication pool catalog backup and recovery

This chapter includes the following topics:

- [Deduplication pool catalog backup policy](#)
- [Automatic configuration of the deduplication pool catalog backup policy](#)
- [Manually configuring the deduplication pool catalog backup policy](#)
- [Manually updating the deduplication pool catalog backup policy](#)
- [Recovering the deduplication pool catalog](#)

Deduplication pool catalog backup policy

Creating a backup of the deduplication pool catalog is a very important step in protecting your data in the event of a disaster. The NetBackup Appliance automatically creates a policy to backup the deduplication pool catalog. In rare cases where a policy cannot be created, manual intervention may be necessary.

Caution: Symantec recommends that you contact your Symantec 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 deduplication pool catalog backup policy”](#) on page 312.

See [“Manually configuring the deduplication pool catalog backup policy”](#) on page 315.

See [“Manually updating the deduplication pool catalog backup policy”](#) on page 316.

See [“Recovering the deduplication pool catalog”](#) on page 317.

Automatic configuration of the 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 in the following scenarios:

- When a deduplication storage pool is created during the initial configuration of the appliance.
- When `Manage>Storage>Resize MSDP` is run when a deduplication storage pool did not exist.
- When upgrading an appliance that had a deduplication storage pool already configured.

The deduplication pool catalog backup policy can be viewed once it is created by one of the above scenarios. Symantec 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.

If a policy to backup the deduplication storage pool catalog already exists, the configuration of this policy is updated.

When configuring the deduplication storage pool backup policy, take the following into consideration:

- The residence must be set and should not be local to the appliance.
- 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.

Note: If MSDP storage is not configured during initial configuration, the policy is not created.

The creation of the policy is automatic so be sure to check the output messages to make sure that the policy has been successfully created.

Email notifications are sent to the email addresses that have been configured to receive software alerts. These email addresses are configured through the NetBackup Appliance Web Console or by running the following command:

```
Settings>Alerts>Email Software Add.
```

Table 7-1 Deduplication storage pool catalog backup policy success messages

Message	Definition
A backup policy, <policy-name>, has been configured to protect the deduplication pool catalog. Review the policy configuration and make changes to its schedules, backup window, and residence as required. Make sure to activate the policy to protect the catalog. For more information, refer to the <i>NetBackup Appliance Administrator's Guide</i> .	This message is displayed in the following scenarios: <ul style="list-style-type: none"> ■ The deduplication pool catalog backup policy did not exist and was created successfully. ■ The deduplication pool catalog backup policy has existed and was updated successfully.
An existing backup policy, <policy-name>, has been found that conflicts with the required deduplication pool backup policy. The policy type has been updated to 'Standard' to protect the deduplication pool catalog. The policy type was set to <previous-policy-type> before this update.	The policy type of the pre-existing deduplication pool policy has been updated to standard. The policy type was set to <previous policy type>. Review the policy configuration and make sure that the previous backup configuration is not affected.

Table 7-2 Deduplication storage pool catalog backup policy failure messages

Message	Definition
Failed to create a deduplication pool catalog backup policy. The policy is required to protect the deduplication pool catalog and recover it in case of disaster. Refer to the <i>NetBackup Appliance Administrator's Guide</i> for how to configure the policy manually.	The deduplication pool catalog backup policy did not exist and the policy creation has failed. To protect the deduplication pool catalog, you need to configure the backup policy manually. See "Manually configuring the deduplication pool catalog backup policy" on page 315.

Table 7-2 Deduplication storage pool catalog backup policy failure messages (*continued*)

Message	Definition
Failed to update deduplication pool catalog backup policy, '<policy-name>', type to 'Standard.' An existing backup policy has been found that conflicts with the required deduplication pool catalog backup policy. Make sure to update the policy type to 'Standard' manually to protect the deduplication pool catalog. Refer to the <i>NetBackup Appliance Administrator's Guide</i> for how to configure the policy manually.	<p>This message is displayed in the following scenarios:</p> <ul style="list-style-type: none"> ■ The policy already exists and the policy type is not set to Standard. ■ The operation has failed to update the policy type to Standard. <p>To protect the deduplication pool catalog, you need to change the policy type manually.</p> <p>See "Manually updating the deduplication pool catalog backup policy" on page 316.</p>
Failed to update the client and the backup selection properties of the deduplication pool catalog backup policy <policy-name>. Refer to the <i>NetBackup Appliance Administrator's Guide</i> for how to configure the policy manually.	<p>The deduplication pool catalog backup policy pre-exists but the operation has failed to update the policy properties, which include Client and Backup Selection.</p> <p>To protect the deduplication pool catalog, you need to update the Client and Backup selection manually.</p> <p>See "Manually updating the deduplication pool catalog backup policy" on page 316.</p>

Caution: Symantec recommends that you contact your Symantec 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 deduplication pool catalog backup policy"](#) on page 315.

See ["Manually updating the deduplication pool catalog backup policy"](#) on page 316.

See ["Recovering the deduplication pool catalog"](#) on page 317.

Manually configuring the 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 in to the Appliance with a NetBackupCLI user account.

See [“Creating NetBackup administrator user accounts”](#) on page 214.

- 2 Enter the following command to create the deduplication pool catalog backup policy:

```
# drcontrol --new_policy --policy <policy-name> --hardware  
<appliance model> --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 *<appliance model>* with the model of the Appliance. For example,
5220, 5230 or 5330.
- 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 deduplication pool catalog backup policy”](#) on page 312.

See [“Manually updating the deduplication pool catalog backup policy”](#) on page 316.

See [“Recovering the deduplication pool catalog”](#) on page 317.

Manually updating the 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 in to the Appliance with a NetBackupCLI user account.

See [“Creating NetBackup administrator user accounts”](#) on page 214.

- 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> --hardware <appliance model> --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 *<appliance model>* with the model of the Appliance. For example, 5220, 5230 or 5330.
- 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 deduplication pool catalog backup policy”](#) on page 312.

See [“Manually configuring the deduplication pool catalog backup policy”](#) on page 315.

See [“Recovering the deduplication pool catalog”](#) on page 317.

Recovering the deduplication pool catalog

This section outlines how to recover the deduplication pool catalog in the event of a disaster.

Caution: Symantec recommends that you contact your Symantec 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 in to the Appliance with a NetBackupCLI user account
See [“Creating NetBackup administrator user accounts”](#) on page 214.

- 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 in to the Appliance as an Appliance Administrator.
- 4 Run hardware monitoring commands to make sure that there are no errors.

- 5 Run hardware self-test to make sure that all hardware components are in place and functioning correctly.
- 6 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.
- 7 If the size requirement is not met, run `Manage > Storage Resize MSDPCatalog` to expand the partition.
- 8 Log in to the Appliance with a NetBackupCLI user account.
- 9 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 [“Automatic configuration of the deduplication pool catalog backup policy”](#) on page 312.

See [“Manually configuring the deduplication pool catalog backup policy”](#) on page 315.

See [“Manually updating the deduplication pool catalog backup policy”](#) on page 316.

Index

Symbols

- 5330 storage shelf component
 - set to Service Allowed mode 306

A

- about
 - appliance restore 127
 - checkpoint creation status 133
 - creating appliance checkpoint 128, 131
 - Email notification from NetBackup appliance 45
 - factory reset 141
 - license key management 153
 - master server role 17
 - media server role 17
 - NetBackup appliances 12
 - NetBackup documentation 32
 - rollback to checkpoint 134
 - supported tape devices and tapes 115
- About BMR 125
- Active Directory
 - authentication 282
 - user management 287
- Active Directory user
 - configure authentication 269
- add external robots 115
- add user
 - Active Directory 288
 - LDAP 288
 - local 288
 - NIS 288
- add user group
 - Active Directory 289
 - LDAP 289
 - NIS 289
- alert notification
 - call home 227
 - SMTP 227
 - SNMP 227
- Appliance console
 - description 21
- Appliance Diagnostics Center 295

- appliance log files
 - Browse command 302
- appliance password
 - change after initial configuration 293
- appliance registration
 - initial configuration for 238
- Appliance Restore
 - management on the NetBackup appliance 127
- Appliance Web Console
 - enable BMR 126
- Auto Image Replication 219
 - between appliances and deduplication appliances 224
- AutoSupport
 - customer registration 240

B

- bandwidth
 - expanding on NetBackup appliance 199
- BMR
 - enable 126
 - option 126
- bond
 - create 255
- bookmarks
 - using with Appliance 23
- Browse command
 - appliance log files 302

C

- Call Home
 - alerts 233
 - workflow 237
- Call Home proxy server
 - configuring 236
- change
 - Date and Time Configuration 265
- change appliance password 293
- change FT settings 260
- change settings
 - for DNS Configuration 263

- changing host configuration 262
- Check Disk Configuration wizard 295
- clients used with appliances
 - install client software on 190
- Collect Log files wizard 295
- collect logs
 - commands 300
 - datacollect 304
 - log file location 300
 - types of logs 300
- common tasks
 - Appliance 31
- configuration
 - of maximum transmission unit size 200

D

- dashboard 29
- data buffer
 - parameters 118
- datacollect
 - device logs 304
- Date and Time Configuration
 - change 265
- deduplication
 - parameters 124
 - solutions 122
- deduplications 5230 122
- delete user
 - Active Directory 289
 - LDAP 289
 - local 289
 - NIS 289
- delete user group
 - Active Directory 290
 - LDAP 290
 - NIS 290
- disable security warnings
 - on Mozilla 19
- disk information
 - viewing 106
- disks
 - storage 67
- DNS Configuration
 - change settings 263
- documentation 32
- download NetBackup client packages from NetBackup
 - appliance 192
- download software updates
 - Manage > Software Updates tab 173

E

- Email notification
 - from NetBackup appliance 45
- Ethernet ports
 - NetBackup 5330 configurations 247
- expand bandwidth
 - on NetBackup appliance 199
- external robots
 - adding to the NetBackup 5200 115

F

- Fibre Transport
 - option descriptions 259
- FT settings
 - change 260

G

- grant permissions 291
- guidelines
 - VLAN configuration 253

H

- hardware
 - monitoring 40
 - monitoring and alerts on the appliance 36
- hardware monitoring and alerts 36
- home page 29
- host
 - IPMI 126
- host reconfiguration 262

I

- initial configuration
 - for appliance registration 238
- install
 - openstorage plugin 202
- install client software
 - on clients used with appliances 190
- install software updates
 - Manage > Software Updates tab 173
- IPv4 and IPv6 support 264

L

- LDAP
 - authentication 273
 - user management 287

- LDAP user
 - configure authentication 268
- license key
 - management on the NetBackup appliance 153
- lifecycle
 - parameters 118, 122
- local user
 - configure authentication 267
 - user management 287
- login page
 - NetBackup Appliance Web Console 24

M

- Manage
 - license keys 155
- manage
 - appliance restore 128, 131, 133–137, 139–141, 145, 149
 - license keys 154
- Management Information Base (MIB) 232
- master server
 - about role 17
- maximum transmission unit size
 - about configuration for 200
- media server role 17
- menu
 - settings 225
- Microsoft Internet Explorer 18
- migration
 - check job status 163
 - Policy Conversion tab 166
 - Selection Criteria tab 159
- Migration Job Status tab 163
- Migration Utility
 - about 157
- monitor
 - hardware summary 36
 - NetBackup 52XX configuration 35
- monitor storage tasks 88
- move dialog
 - storage 80
- Mozilla Firefox 18

N

- NetBackup
 - about documentation for 32
- NetBackup 5200
 - adding external robots 115

- NetBackup Administration Console
 - download to Windows computer from NetBackup appliance 194
- NetBackup appliance
 - about appliance restore 127
 - about Email notification 45
 - about license key management 153
 - appliance factory reset 145, 149
 - appliance rollback validation 136
 - checkpoint rollback status 139
 - expanding bandwidth on 199
 - factory reset status 149
 - managing appliance restore 128
 - managing license keys 154
 - monitoring and alerts 36
 - rollback appliance 135, 137, 140
- NetBackup Appliance Web Console
 - login page 24
- NetBackup Appliance Web Console login page 24
- NetBackup client packages
 - download from NetBackup appliance 192
- NetBackup commands
 - Auditing accounts 217
 - Best practices 213
 - Creating touch files 211
 - creating users 214
 - deleting users 217
 - Known limitations 214
 - Logging in as administrator 215
 - manage users 208
 - Managing passwords 216
 - OS commands 213
 - Running commands 210
 - viewing current users 218
- NetBackup parameters 116
- network
 - VLAN 243
- NFS mount
 - mount a remote NFS drive 205
 - mount list 204
 - unmount 204
 - Unmount a remote NFS drive 207
- NIS
 - authentication 285
 - user management 287
- NIS user
 - configure authentication 269
- notifications 233

O

- openstorage plugin 200
 - installing plugins 202
 - uninstalling plugins 203
- option descriptions
 - for Fibre Transport 259
- OST plugin
 - installing plugins 202
 - uninstalling plugins 203

P

- parameters
 - data buffer 118
 - deduplication 124
 - lifecycle 122
- partition distribution
 - on disks 111
- partitions
 - details 74
 - storage 67
- Perform a hardware health check wizard 295
- Policy Conversion
 - change policy for migration 166
- privileges
 - user role 272

R

- remove
 - storage disk 86
- resize dialog
 - storage 78
- revoke permissions 292
- role
 - about master server 17
 - about media server 17

S

- scan
 - storage device 88
- Selection Criteria tab
 - migration 159
- self-repair wizards 295
- Service Allowed mode
 - 5330 storage shelf component 306
- settings
 - network 243
 - sub menus 225

share

- creating 92
 - deleting 101
 - editing 96
 - moving 100
 - resizing 99
- ## show
- disks 102
 - distribution 102
 - partitions 102
- Simple Network Management Protocol (SNMP) 232
 - SNMP server options 231
 - options 231
 - software updates
 - Manage > Software Updates tab 173
 - storage 36
 - viewing 103
 - storage configuration
 - about 63
 - storage device
 - scan 88
 - storage disk
 - removing 86
 - storage partition
 - moving 80
 - resizing 76
 - storage partitions
 - viewing 110
 - Symantec Data Center Security
 - about 46
 - administration 48
 - connecting to server 57
 - filtering audit logs 52
 - log retention 52
 - managed mode 46, 54–57
 - policy downloads 54, 56
 - server and console downloads 54–55
 - unmanaged mode 46, 57
 - view log details 50
 - Symantec NetBackup Appliance
 - settings menu 225
 - Sync member groups 292
- ## T
- tag
 - VLAN 256
 - tape devices and tapes
 - about appliance supported 115
 - Test and diagnose network issues wizard 295

- Test Call Home functionality wizard 295
- third party SSL certificates 58
- trusted master servers
 - adding 220

U

- uninstall
 - openstorage plugin 203
- user
 - Active Directory 269
 - add 270
 - authorize 270
 - Kerberos-NIS 269
 - LDAP 268
 - local 267
 - manage role
 - permissions 271
- user authentication
 - configure 267
 - guidelines 270
- user group
 - add 270
 - manage role
 - permissions 271
- user role privileges
 - NetBackup appliance 272

V

- vCenter
 - credentials 197
- VLAN
 - tagging 242

W

- WAN optimization
 - about 248
 - disable 248, 251
 - enable 248, 250
 - status 248, 252
- web browser
 - book marks 23
 - support 18