

Symantec NetBackup™ Appliance Administrator's Guide

Release 2.6

NetBackup 52xx



Symantec NetBackup Appliance Administrator's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 2.6

Legal Notice

Copyright © 2013 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo and NetBackup 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, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. 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

Symantec 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 Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's 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 Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/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.symantec.com/business/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 Symantec
 - Recent software configuration changes and network changes

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/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
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

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

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Technical Support	4
Chapter 1	
Overview	12
About NetBackup appliances	12
About the Master Server role	15
About the Media Server role	16
About accessing the NetBackup Appliance Web Console	17
Web browsers supported by Appliance	17
Disabling the Untrusted Connection page in Mozilla Firefox	18
About the Symantec NetBackup Appliance Web Console menus	19
About Appliance console components	21
About using the links on the title bar	21
Accessing and using help	21
About using Web browser bookmarks	23
About the NetBackup Appliance Web Console login page	23
NetBackup Appliance home page	28
Common tasks in Appliance	29
About the NetBackup Appliance documentation	31
Chapter 2	
Understanding the NetBackup appliance settings	34
About modifying the appliance settings	34
Settings > Notification	36
Settings > Notification > Alert Configuration	37
Settings > Notification > Registration	46
Settings > Network	49
Settings > Network > Network Settings	49
Settings > Network > Fibre Transport	53
Settings > Network > Host	54
Settings > Network > WAN Optimization options	56
About IPv4-IPv6-based network support	61
Settings > Password Management	63
Settings > Date and Time	64
Settings > Authentication	65
Settings > Authentication > Server Configuration	65

	Settings > Authentication > User Management	76
Chapter 3	Monitoring the NetBackup appliance	81
	About monitoring the NetBackup Appliance	81
	About hardware monitoring and alerts	82
	Monitor > Hardware options	82
	Monitor > Hardware > Health details	87
	Acknowledging hardware errors	91
	About Email notification from a NetBackup appliance	92
	About Symantec Critical System Protection	94
	Monitor > SCSP Audit View	94
	Viewing SCSP audit log details	96
	Filtering SCSP audit logs	98
	Setting the audit log retention specification	100
	Connecting to the SCSP server	101
	About viewing SCSP-specific documentation	102
Chapter 4	Managing a NetBackup appliance from the NetBackup Appliance Web Console	103
	About the Manage views	103
	About appliance supported tape devices	106
	Adding external robots to the NetBackup appliance	107
	About configuring Host parameters for your appliance	107
	Manage > Host > Data Buffer options	108
	Configuring data buffer parameters	109
	Manage > Host > Lifecycle options	110
	Configuring lifecycle parameters	113
	About configuring deduplication solutions	113
	About BMR integration	116
	About storage configuration	117
	Manage > Storage > Partitions	120
	Resizing a partition	124
	Resize dialog	126
	Moving a partition	128
	Move <partition> dialog	129
	Manage > Storage > Disks	130
	Scanning storage devices from the NetBackup Appliance Web Console	133
	Adding a new disk	134
	Removing an existing storage disk	135
	Monitoring the progress of storage manipulation tasks	137

Scanning storage devices using the NetBackup Appliance Shell	
Menu	137
About viewing storage space information using the <code>Show</code> command	
.....	138
About storage email alerts	143
Manage > Appliance Restore	144
About creating an appliance checkpoint	146
About rollback to a checkpoint	154
Appliance factory reset	163
Manage > License	175
Managing license keys on the NetBackup appliance	176
Adding a permanent license key if an evaluation license key	
expires	177
About the Migration Utility	179
Selection Criteria	181
Migration Job Status	185
Policy Conversion	188
Best practices to run a migration job	191
About software release updates	192
Manage > Software Updates	194
Upgrading an appliance using the NetBackup Appliance Web	
Console	196
Upgrading an appliance using the NetBackup Appliance Shell	
Menu	200
Media servers to upgrade	208
Software Updates > Status	209
About installing an EEB	210
About installing NetBackup Administration Console and client	
software	211
Manage > Additional Servers	218
Adding additional servers to the appliance	218

Chapter 5	Managing NetBackup appliance using the	
	NetBackup Appliance Shell Menu	220
	Expanding the bandwidth on the NetBackup appliance	220
	About configuring the maximum transmission unit size	221
	About OpenStorage plugin installation	221
	Installing OpenStorage plugin	223
	Uninstalling OpenStorage plugin	224
	About mounting a remote NFS	225
	Mounting an NFS remote drive	226
	Unmounting an NFS drive	228

	About running NetBackup commands from the appliance	229
	About NetBackup administrator capabilities	230
	Creating NetBackup administrator user accounts	234
	Deleting NetBackup administrator user accounts	237
	Viewing NetBackup administrator user accounts	238
	About Auto Image Replication between appliances	239
	About Auto Image Replication between NetBackup appliances	239
	About Auto Image Replication between NetBackup appliances and deduplication appliances	244
Chapter 6	Decommissioning a NetBackup appliance	245
	About decommissioning a NetBackup 52xx appliance	245
	Decommissioning a NetBackup 52xx master appliance	246
	Decommissioning a NetBackup 52xx media appliance	246
Chapter 7	Troubleshooting	249
	Troubleshooting and tuning Appliance from the Appliance Diagnostics Center	249
	NetBackup Appliance log file location information	253
	About password recovery	254
	About disaster recovery	255
	Gathering device logs with the Datacollect command	256
Chapter 8	Reconfiguring a NetBackup appliance	258
	About reconfiguring a NetBackup appliance	258
	Reimaging a NetBackup appliance	260
	Reconfiguring a 52xx master server appliance from the USB drive using the NetBackup Appliance Shell Menu	268
	Configuring a master server to communicate with an appliance media server	273
	Reconfiguring a 52xx media server appliance from the USB drive using the NetBackup Appliance Shell Menu	275
Appendix A	Call Home upload information	284
	About the appliance hardware information that is uploaded	284
	About the storage shelf information that is uploaded	289

Appendix B	Fibre Channel and Fibre Transport connectivity	293
	About the card slots on NetBackup 52xx series appliances	293
	About Fibre Channel port configuration options for the NetBackup 52xx appliances	298
	About NetBackup SAN Client and Fibre Transport	304
	About the SAN Client license key	305
	About zoning the SAN for a NetBackup 5220 or 5230 appliance	305
	Guidelines for changing NetBackup appliance FT target ports to receive data streams from multiple SAN Client FC initiator ports	309
	About Fibre Transport paths for NetBackup appliances	310
	How to determine appliance HBA WWPNs	315
	About the NetBackup appliance as a VMware backup host	316
	Notes on the NetBackup appliance as a VMware backup host	316
	Appliance as backup host: component overview	317
	About backup to tape support for NetBackup appliances	317
Appendix C	IPMI Configuration	319
	About IPMI configuration	319
	Configuring IPMI using the BIOS setup	321
	Accessing and using the Symantec Remote Management interface	327
	About the Integrated Storage Manager interface for 5200 appliances	336
	Managing settings using the NetBackup Appliance Shell Menu	339
Index	341

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 Symantec NetBackup Appliance Web Console menus](#)
- [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 configurations, you get the added benefit of internal disk storage.

This appliance allows for easy expansion of existing NetBackup environments that have NetBackup 7.6 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 8.0 and later, and Mozilla Firefox versions 15.0 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
- MSDP is supported on all 52xx master and media appliances. MSDP offers up to the maximum available capacity on a 52xx appliance.
- Backup of VMware virtual machines. NetBackup appliance version 2.6 (NetBackup version 7.6) supports direct backup of VMware virtual machines. The appliance can back up virtual machines without a separate Windows system as backup host.
- Symantec Critical System Protection (SCSP) integration. The SCSP agent is installed and configured when you initially configure your appliance. This agent ensures that your appliance's audit logs are sent to the SCSP 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 52xx appliance. This feature enables the appliance

administrator to 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. Helps to simplify the deployment and can be easily integrated into an existing NetBackup environment.
- Tape out option. The appliance includes a gigabit, dual-port Fibre Channel host bus adapter (HBA).
- 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 *NetBackup server 7.x hardware compatibility list* on the Symantec Support website.
<http://www.symantec.com/docs/TECH59978>
- 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 1GB 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 and Initial Configuration Guide* and the *Symantec NetBackup 5030 and 5230 Appliance and Symantec Storage Shelf Product Description*.

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 7.6.
-----------------------------------	--

- Add deduplication capability
- Add the appliance to an existing NetBackup environment or replace an existing media server that does not support deduplication.
 - Add NetBackup AdvancedDisk support for faster backups.
 - Configure MSDP partition on the Appliance for deduplication capability.

Add more storage capability Add storage capability to existing NetBackup 7.6 and greater environments.

- Built-in appliance disk storage for 52xx appliances
The internal disks can be used for additional backup storage on a 52xx appliance.
- Additional external storage
The Symantec Storage Shelf is an external unit that provides additional disk storage space. You can add up to two of these units to a NetBackup 5220 or 5230 appliance.
When you purchase a 5220 appliance and a Symantec Storage Shelf together, the units are matched at the factory for optimum performance. 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.

This appliance contains everything you need to start using NetBackup. After you mount the appliance in a rack in your lab, you are ready to connect it and configure it to your network. After you have successfully configured your appliance, you can install and configure your media servers and clients. Once that is done, you are ready to run backups.

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.

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.

The master server can be a 52xx with appliance software version 2.6 or later, or a traditional NetBackup master server with NetBackup version 7.6 or later.

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

- **For use with a traditional NetBackup master server** (52xx series appliances only)
This appliance role must be used only with a standard NetBackup master server. The NetBackup master server must have NetBackup version 7.6 or later installed. Symantec recommends that you install the latest version of the NetBackup master server.
- **Specify master server**
The master server that you specified must be a NetBackup 52xx with appliance software version 2.6 or later, or a traditional NetBackup master server with version 7.6 or later

[Table 1-1](#) describes the supported deduplication configuration for each appliance media server:

Table 1-1 Supported deduplication configurations for NetBackup appliances

Appliance model	Deduplication support on media server
5220	Media server deduplication pool (MSDP) only

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: **http://host.domain**

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

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 8.0 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 1-2 lists the Web browsers that Appliance supports.

Table 1-2 Web browsers supported by Appliance

Web browser	Supported Versions	Notes
Microsoft Internet Explorer	8.0, 9.0 Note: Appliance is not supported specifically on IE 8.0 with Cipher strength 128-bit on Windows XP. To verify your IE version and Cipher strength, open Internet Explorer and click Help > About Internet Explorer .	IE 8.0 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 8 or 9 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	15.0 and higher	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 18.

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 Symantec NetBackup Appliance Web Console menus

The Symantec NetBackup Appliance v2.6 now comes with a new and improved NetBackup Appliance Web Console that ensures a better user experience. The menu structure has been improved to enable you to easily access the tasks that are associated with each other. The following diagram provides a brief overview of how the menu structures have evolved for v2.6:

Figure 1-1 NetBackup Appliance Web Console menu structure for 52xx appliance

Menus	Symantec NetBackup 52xx - v2.5.1	Symantec NetBackup Appliance 52xx – v2.6
Home		Symantec NetBackup Welcome Page ★
Manage	Storage	Storage
	NetBackup License	License
	Additional Servers*	Additional Servers*
	Appliance	Appliance Restore
	Add Media Appliance	Migration Utility ★
	Download Updates	Policy Conversion
	Browse for Updates	Selection Criteria
	Install Updates	Migration Job Status
		Software Updates
		Host
Monitor		Deduplication
		Data Buffer
		Lifecycle*
		Advance*
	Hardware	Hardware
	SCSP Audit Logs*	SCSP Audit View
	Hardware Monitoring	Notification
	Configuration	Alert Configuration
	SNMP	Registration ★
	SMTP	Network
Settings	WAN Optimization	WAN Optimization
	Appliance Reconfig.	Network
	Network Config.	Host
	DNS Configuration	Fiber Transport
	Fiber Transport	
	Security	Password
	Date and Time	Date and Time
		Authentication ★
	NetBackup	Server Configuration
	Deduplication	User Management
	Data Buffer	
	Lifecycle*	
	Advance*	

★ New ● Moved to **Manage** tab
● Removed * Master Servers

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 (or SymHelp) is available with the Appliance. SymHelp is a browser-based Help delivery system with advanced search, autosuggest, and filtering capabilities. SymHelp lets you search from a much larger Appliance content set. Additionally you can search from the NetBackup documentation from the same SymHelp window. More information about online Help is available. See [“Accessing and using help”](#) on page 21.
- 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 (or SymHelp) is shipped with the NetBackup Appliance. SymHelp is a browser-based Help delivery system with advanced search, autosuggest, and filtering capabilities.

SymHelp offers the following advantages over traditional Help systems:

- SymHelp lets you search from a much larger Appliance content set. SymHelp includes content from the *NetBackup Appliance Administrator's Guide*, the *Troubleshooting Guide*, and the *Commands Guide*. This means that you can search all of 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, SymHelp lets you search content from the *NetBackup Administrator's Guide*. By default, you can view and search the Appliance content.

Figure 1-2 shows a sample view of SymHelp and how you can search Appliance and NetBackup content from SymHelp.

Figure 1-2 Sample view of SymHelp

The screenshot shows the Symantec Help Center interface. On the left, there is a navigation pane with 'Product' (NetBackup Appliance, NetBackup Administrator's Guide) and 'Subject' (Configuring, Installing, Licensing, Overview, Recovering, Troubleshooting, Using, Backing Up, Maintaining, Managing Devices, Managing Media, Monitoring, Reporting). The 'Licensing' subject is selected. The main content area displays search results for 'license'. The first result is 'Manage > License', which is expanded to show details about reviewing, adding, and deleting license keys. Annotations with arrows point to specific parts of the interface: 'Select the product filters – Appliance and NetBackup' points to the Product section; 'Enter text in the Search box' points to the search bar; 'To get specific results, select a subject category that you want to search on' points to the Subject section; and 'Search results from Appliance and NetBackup content are displayed.' points to the search results list.

Select the product filters – Appliance and NetBackup

Enter text in the Search box

To get specific results, select a subject category that you want to search on

Search results from Appliance and NetBackup content are displayed.

To access and use SymHelp

- 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 SymHelp is a search-based Help system. 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.

You can view and search the Appliance content by default. To be able to search NetBackup content, select *NetBackup (Administrator's Guide)* from the **Product Filters** section. You can then type in your NetBackup related search query in the search toolbar.
- 3 Click **Search**. To view the updated documentation content that is posted online, you must be connected to the Internet and check **Include online KB search**.

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.

About the NetBackup Appliance Web Console login page

The section describes the procedure to log into your Symantec NetBackup Appliance Web Console. The login page provides the fields to enter your login credentials and also displays the following sections:

Section	Description
Product Information	- This section provides links to the latest documentation like What's New in this release or the Release Notes . It also provides links to the Compatibility Lists and Symantec Operational Readiness Tools (SORT) .

Section	Description
Download Client Packages	<p>This section enables you to select and download the client packages available for the current release.</p> <p>Note the following important pointers while downloading client packages:</p> <ul style="list-style-type: none"> ■ If you have opted to install the 10GB package, the client packages are not installed on the appliance. In such cases the Download Client Packages section displays the following message: <p style="margin-left: 40px;">No packages found.</p> <p>For more information about the installation process, refer to the <i>Symantec NetBackup Appliance Hardware Installation and Initial Configuration Guide</i>.</p> ■ You need to download the Windows client package to install the NetBackup Administration Console client. 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.
Browser Recommendation	<p>This section verifies and displays a confirmation if the Symantec NetBackup Appliance Web Console supports your browser.</p> <p>Note: The Symantec NetBackup Appliance Web Console cannot be viewed on the Microsoft Internet Explorer 8 or Microsoft Internet Explorer 9 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 and is used to identify the device in your network.

Note: If you use Internet Explorer 8.0 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**.
- 3 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.

- 4 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

Log on to the shell menu and run `Settings> SystemLocale List language_code`.

Example: Run `Settings> SystemLocale List ja` to browse the available locales in Japanese language.

The following locales can be displayed:

- `ja_JP.UTF-8`
- `ja_JP.eucJP`
- `ja_JP.eucjp`
- `ja_JP.shiftjisx0213`
- `ja_JP.sjis`
- `ja_JP.utf8`

2. Set the preferred locale along with its format

Run `Settings > SystemLocale Set language_code` command.

Example: Run `Settings> SystemLocale Set ja_JP.UTF-8` to set the `ja_JP.UTF-8` locale to the Appliance.

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 setup your appliance. For more information, refer to the *Symantec NetBackup Hardware Installation and 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 will be valid for 30 days. Symantec recommends that you add a permanent license key before the temporary license key has expired.

- Symantec NetBackup Appliance home page - When you have successfully configured your appliance the **Home** page is displayed. For more information about the **Home** page, See [“NetBackup Appliance home page”](#) on page 28.

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.

Along with the process to log into the appliance, let us see some of the reasons due to which login failure can occur. [Table 1-3](#) lists the reasons due to which login failure can occur:

Table 1-3 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.
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 instance 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: /opt/SYMCnbappws/webserver/logs
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:

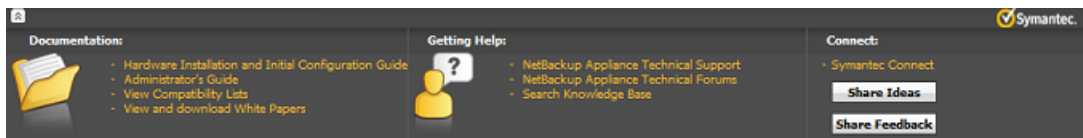
Table 1-4 Home page description

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 52xx 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 > Partitions” on page 120.</p>
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 “About software release updates” on page 192.</p>

Table 1-4 Home page description (*continued*)

Element	Displays	Helps to	Links to the page
Hardware	Displays the performance of all the monitored hardware devices.	Determine if the hardware is running and a failure has been detected. An error message is displayed, in case a hardware component malfunctions.	Monitor > Hardware For more information See “Monitor > Hardware > Health details” on page 87.
Deduplication Summary	Displays the current deduplication ratio pertaining to all the backups taken so far across all the media servers.	Determine the quality of the data backed-up using deduplication. Lower the ratio, lower is the amount of data being stored using Deduplication. Deduplication ratio = total number of bytes backed up (without Deduplication) / number of bytes changed and backed up (with Deduplication)	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 113.

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 1-5 Quick links for common Appliance tasks

Appliance functions	Tasks	Go to this topic
Monitoring	Monitor hardware, services, and Symantec Critical System Protection Agent (SCSP)	See “Monitor > Hardware options” on page 82. See “About hardware monitoring and alerts” on page 82. See “About Symantec Critical System Protection” on page 94.
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 113. See “Configuring data buffer parameters” on page 109. See “About the Migration Utility” on page 179. See “Manage > Software Updates” on page 194.
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 117. See “Manage > Storage > Partitions” on page 120. See “Manage > Storage > Disks” on page 130.
Restoring an Appliance	Create a checkpoint Rollback to a checkpoint Perform Factory Reset	See “Manage > Appliance Restore” on page 144.
Configuring Appliance settings	Alert and Call Home Network Date and Time Configure LDAP server Password management	See “About modifying the appliance settings” on page 34.
Troubleshooting	Troubleshoot Appliance issues	See “Troubleshooting and tuning Appliance from the Appliance Diagnostics Center” on page 249.

About the NetBackup Appliance documentation

Included with your NetBackup appliance are the following documents to ensure you can successfully install, configure, and use your appliance. You can find these documents on the Symantec Support web site at the following URL:

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

Table 1-6 NetBackup Appliance documentation

Guide	Description
<i>Symantec NetBackup™ Appliance Hardware Installation and Initial Configuration 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> ■ Software configuration steps <p>This section guides you through the configuration process from the NetBackup Appliance Web Console or from the NetBackup Appliance Shell Menu.</p>
<i>Symantec NetBackup™ Appliance Administrator's Guide</i>	<p>The <i>Symantec NetBackup™ Appliance Administrator's Guide</i> is provided as part of the NetBackup appliance software package. This guide may contain updates that have occurred since the initial release of the document. For the latest administration information always refer to this version of the guide.</p> <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

Table 1-6 NetBackup Appliance documentation (*continued*)

Guide	Description
<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. This document is provided as a part of the product software that is installed on the appliance, and in electronic form on the Symantec Support Web site:</p> <p>http://www.symantec.com/docs/DOC2792</p>
<i>Symantec NetBackup Appliance Release Notes</i>	<p>This document contains information about NetBackup appliance, version 2.6 release. It contains brief descriptions of new features within the release, operational notes that apply to the release update, and any known issues.</p> <p>This document is available on the Symantec Support Web site at the following location.</p> <p>http://www.symantec.com/docs/DOC2792</p>
<i>Symantec NetBackup Appliance Troubleshooting Guide</i>	<p>This document contains the latest troubleshooting information for the NetBackup appliances. It is available on the Symantec Support Web site at the following location.</p> <p>http://www.symantec.com/docs/DOC2792</p>
<i>Symantec NetBackup Product Family Third-party Legal Notices</i>	<p>The <i>NetBackup Product Family 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. This document is available from the following Web site:</p> <p>http://www.symantec.com/docs/DOC3775</p>

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

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

- *Symantec NetBackup 5230 Appliance and Symantec Storage Shelf Product Description*

Understanding the NetBackup appliance settings

This chapter includes the following topics:

- [About modifying the appliance settings](#)
- [Settings > Notification](#)
- [Settings > Network](#)
- [Settings > Password Management](#)
- [Settings > Date and Time](#)
- [Settings > Authentication](#)

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 2-1](#) describes the settings that are available from **Settings > Configuration** menu:

Table 2-1 Settings > Notification

Sub Menu	Lets you...	Topic
Alert configuration	Configure the SNMP, SMTP, and Call Home settings.	See “Settings > Notification > Alert Configuration” on page 37.
Registration	Register the details of your appliance and your contact information.	See “Settings > Notification > Registration” on page 46.

[Table 2-2](#) describes the settings that are available from **Settings > Network** menu:

Table 2-2 Settings > Network

Sub Menu	Lets you...	Topic
Network	View and change network configuration settings.	See “Settings > Network > Network Settings” on page 49. See “Changing Network Configuration settings” on page 50.
Host	Configure the host name, for either DNS or non-DNS systems	See “Settings > Network > Host” on page 54. See “Changing DNS and host name Configuration settings” on page 55.
Fibre Transport Configuration	Configure fibre transport settings for your appliance.	See “Settings > Network > Fibre Transport” on page 53. See “Changing the Fibre Transport settings” on page 54.
WAN Optimization	Improve the outbound network traffic.	See “Settings > Network > WAN Optimization options” on page 56. See “Disabling, enabling, and viewing the WAN optimization settings” on page 58.

[Table 2-3](#) describes the settings that are available from the **Settings > Password** menu:

Table 2-3 Settings > Password

Sub Menu	Lets you...	Topic
Password	Change the admin password for your appliance.	See " Settings > Password Management " on page 63.

[Table 2-4](#) describes the settings that are available from the **Settings > Date and Time** menu:

Table 2-4 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 64.

[Table 2-5](#) describes the settings that are available from **Settings > Authentication** menu:

Table 2-5 Settings > Authentication

Sub Menu	Lets you...	Topic
Server Configuration	Configure your LDAP (Lightweight Directory Access Protocol) server. The LDAP server enables you to access and maintain distributed directory information services for your appliance.	See " Settings > Authentication > Server Configuration " on page 65.
User Management	Add new users and create user groups for accessing your appliance.	See " Settings > Authentication > User Management " on page 76.

Settings > Notification

The **Settings > Notification** menu displays the following tabs:

- **Alert Configuration** - enables you to provide the SMTP, SNMP and Call Home settings. See "[Settings > Notification > Alert Configuration](#)" on page 37.
- **Registration** - enables you to register the appliance and your contact information. See "[Settings > Notification > Registration](#)" on page 46.

Settings > Notification > Alert Configuration

The **Settings > Notification > 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.

[Table 2-6](#) lists the fields from the **SNMP** (Simple Network Management Protocol) section.

Table 2-6 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 sever 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 61.</p>
SNMP Port	Enter the SNMP Server port number. If you do not enter anything for this variable, then the default port is 162.
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>

You can check the details of the SNMP 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. The MIB file serves as a data dictionary that is used to assemble and interpret SNMP messages.

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 use the following command to configure the SMTP server and add a new Email account.

Main_Menu > Settings > Alerts > Email SMTP Add

[Table 2-7](#) lists the fields from the **SMTP** section.

Table 2-7 SMTP Server Configuration settings

Fields	Description
SMTP Server	<p>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.</p> <p>See “About IPv4-IPv6-based network support” on page 61.</p>
Software Administrator Email	<p>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:</p> <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	<p>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</p> <p>See “About Email notification from a NetBackup appliance” on page 92. for more information about potential hardware alerts.</p>
Sender Email	<p>Enter the Email ID to receive any replies to the alerts or the reports that are sent by the Appliance.</p>
SMTP Account	<p>Enter the user name to access the SMTP account.</p> <p>Note: You maybe asked to enter a user name as some SMTP servers may require user name and password credentials to send an email.</p>

Table 2-7 SMTP Server Configuration settings (*continued*)

Fields	Description
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.

[Table 2-8](#) lists the fields from the **Call Home Configuration** section.

Table 2-8 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 server settings using the **Settings > Notification > Alert Configuration** page.

To configure the SNMP 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 2-6](#)
- 5 Enter the SMTP settings in the provided fields. A description of the SMTP parameters is available in [Table 2-7](#)
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 2-8](#)
- 7 Click **Save**, to save the SNMP 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 is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. 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.

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. An 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 **Setting > Notifications > Alert Configuration** page. To configure the appliance SNMP manager to receive hardware monitoring related traps, click **View SNMP MIB file** in the **SNMP Server Configuration** pane.

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 15 minutes.

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 > Media Server** 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** menu to configure Call Home from the NetBackup Appliance Web Console. Click **Alert Configuration** and enter the details in the **Call Home Configuration** pane.

[Table 2-9](#) describes how a hardware failure is reported when the feature is enabled or disabled.

Table 2-9 What happens when Call Home is enabled or disabled

Monitoring enabled or disabled	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 the following hardware and software information to a Symantec AutoSupport server.<ul style="list-style-type: none">■ Power supply■ CPU■ Fan■ Disk■ Fibre Channel■ Temperatures■ RAID group■ RAID adapter■ Network card■ Storage Shelf status <p>See the following for an example of the hardware information that is uploaded for an appliance or a storage device:</p> <p>See “About the appliance hardware information that is uploaded” on page 284.</p> <p>The following software information is uploaded:</p> <ul style="list-style-type: none">■ The backup jobs that failed in the last 12 hours.■ Total available deduplicated space.■ Used deduplicated space. ■ The appliance generates a local alert by email to notify you of the hardware failure. The appliance also generates an SNMP trap.
Call Home disabled	<p>The appliance generates a local alert by email notifying you of the hardware failure.</p>

Your NetBackup Appliance environment determines which appliance sends the hardware failure report. [Table 2-10](#) describes the Call Home behavior for various appliance environments.

Table 2-10 Call Home feature behavior

Appliance environment	Call Home routine
<ul style="list-style-type: none">■ Standalone appliance master server	If the master server hardware fails, the master server sends the email message that reports the failure.
<ul style="list-style-type: none">■ Appliance master server■ Media server appliance	<p>If the master server hardware fails, the backup media server sends the email message that reports the failure.</p> <p>If the backup media server hardware fails, the master server sends the email message that reports the failure.</p>
<ul style="list-style-type: none">■ Appliance master server■ Media server appliance■ Replication media server	<p>If the master server hardware fails, the backup media server or the replication media server sends the email message that reports the failure.</p> <p>If the media server hardware fails, the master server or the replication media server sends the email message reporting the failure.</p> <p>If the replication media server hardware fails, the master server or the backup media server sends an email message reporting the failure.</p>

See [“Settings > Notification > Alert Configuration”](#) on page 37.

See [“Configuring Call Home from the NetBackup Appliance Shell Menu”](#) on page 43.

See [“About AutoSupport”](#) on page 48.

See [“Monitor > Hardware options”](#) on page 82.

See [“Monitor > Hardware > Health details”](#) on page 87.

Configuring Call Home from the NetBackup Appliance Shell Menu

You can configure the Call Home details from the **Settings > Notification** page.

[Table 2-8](#) provides the settings required to configure Call Home from the NetBackup Appliance Web Console

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 82.

See [“About Call Home”](#) on page 41.

See [“About Email notification from a NetBackup appliance”](#) on page 92.

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.

The transmission of the Call Home data is done using the NetBackup Product Improvement Program Agent. The agent communicates using Secure Socket Layer (SSL) over port 443. All communications are initiated by the appliance. Your appliance needs access to both, <https://telemetrics.symantec.com> and <https://www.symappmon.com>.

The appliance Call Home feature uses the following workflow to communicate with AutoSupport servers:

- Access a port to <https://www.symappmon.com> every 15 minutes.
- Perform a self-test operation to <https://www.symappmon.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 41.

See “[About AutoSupport](#)” on page 48.

Settings > Notification > Registration

You can register the appliance and your contact information from the **Registration** tab that is available under the **Settings > Notification** menu. You may also complete the registration while configuring your appliance. This page provides the necessary data entry fields to register this appliance with Symantec over the Internet.

Registration of your NetBackup appliance helps to make sure that you are alerted to product updates and other important information about your appliance.

[Table 2-11](#) describes the data entry fields that are related to specific information sections and the type of information to enter in the fields.

Table 2-11 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.

Table 2-11 Data entry fields for the appliance registration (*continued*)

Section and related field name	Description
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.
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*.

See [“About AutoSupport”](#) on page 48.

See [“Settings > Notification > Alert Configuration”](#) on page 37.

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 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 46.

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 49.
- **Host** - enables you to reconfigure your appliance's host settings. See “Settings > Network > Host” on page 54.
- **Fibre Transport** - enables you to reconfigure the Fibre Transport settings. See “Settings > Network > Fibre Transport” on page 53.
- **WAN Optimization** - enables you to disable or enable WAN Optimization settings. See “Settings > Network > WAN Optimization options” on page 56.

You can also configure the Network settings using the `Main > Network` commands under the shell menu. For more information refer to the *Symantec NetBackup Appliance Command Reference Guide*.

Settings > Network > Network Settings

The **Settings > Network > Network Settings** tab enables you to update or add the network configuration settings for your appliance. These settings have been applied at the time of initial configuration. The **Network Settings** tab is divided into the following sections:

- **Properties** - This section displays the current configuration settings as described below:

Network Interface	Displays the NIC (network interface card) number. For example, eth1.
IPv4 Address	Displays the IPv4 address of the network connection.
IPv6 Address	Displays the IPv6 address of the network connection.
MAC Address	Displays the Media Access Control address of the configured network. For example, 00:1E:67:08:23:6C
Port Type	Displays the port type of the network connection. For example, Twisted pair.

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 Bonding	Displays if the link is bonded or not.
Reserved	Displays if the network is reserved or not.
MTU	Displays the Maximum Transmission Unit of the configured network in bytes.

- **Network Configuration** - You can use this section to add a new network connection for your appliance.

Warning: NetBackup appliances do not support configuring two IP addresses that belong to the same subnet. The appliance runs on the Linux operating system and this type of networking is a current limitation. Each bond that you create must use an IP address that belongs to a different subnet.

Note: You cannot remove an IP address if the appliance host name resolves to that IP address.

- **Routing Configuration** - You can use this section add the routing information for your appliance.

Changing Network Configuration settings

Use the following procedure to change or add to the **Network Configuration** settings.

Note: If you remove or change the primary IP address configuration, the result may cause a loss of the network connections. If the connection is lost, you need to reconnect and log in to the appliance.

Warning: NetBackup appliances do not support configuring two IP addresses that belong to the same subnet. The appliance runs on the Linux operating system and this type of networking is a current limitation. Each bond that you create must use an IP address that belongs to a different subnet.

Note: You cannot remove an IP address if the appliance host name resolves to that IP address.

To change the network configuration settings

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Network > Network Settings** tab.
The appliance displays the **Network Settings** page.
- 3 In the **Network Configuration** section, enter the network interface information using the following fields:

Fields	Description
Network Interface	<p>Enter the device name of the new network connection to be configured on your appliance.</p> <p>Use the following guidelines to bond multiple NICs:</p> <ul style="list-style-type: none">■ The NIC drop-down list shows the supported combination of appliance Ethernet ports that can be bonded. The list is compiled automatically and is based on the link types and the link speeds of the ports. Ports do not require connection to the network to appear in the list.■ 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. If you try to add an IPv4 address to a NIC that already has an IPv4 address configured, the new address replaces the old address.■ Select Auto to have the NICs selected automatically. This mode selects the best possible set of NICs to plumb the IP address on. The selection is based on the available NICs, the link type (copper or FC), and the link speed. If multiple NICs have the same properties, then a bond (link aggregation) is created and the IP address is plumbed on the bond.■ Only NICs of the same type and speed can be bonded.■ Once a NIC is bonded, it cannot be bonded to another NIC. To reassign a bond, you must first remove the NIC from its current bond.
IP address	<p>Enter the IPv4 or 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>

Fields	Description
Bond Mode	<p>This field lets you combine (aggregate) multiple network interfaces into a single logical "bonded" interface. The behavior of the bonded interfaces depends upon the mode. The default bond mode is balance-alb.</p> <p>The available bonding modes are as follows:</p> <ul style="list-style-type: none">■ balance-rr■ active-backup■ balance-xor■ broadcast■ 802.3ad■ balance-tlb■ balance-alb <p>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>

- 4 Click on the green + button to add the new network configuration.

- 5 Enter the kernel routing information in the **Routing Configuration** section using the following fields:

Fields	Description
Destination IP	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.
Destination Subnet Mask	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.
Default Gateway	Enter the address of the network point that acts as an entrance to another network.
NIC	The appliance can use multiple network interface cards (NICs). This column displays the network device name. Refer to the Linux <code>route</code> command for more information about how to add routing entries.

- 6 Click on the green + button to add the kernel routing information .

The new entries are configured on the appliance and appear automatically in the read-only fields of the **Network Properties** table.

Settings > Network > Fibre Transport

You can change the Fibre Transport (FT) settings from **Settings > Network > Fibre Transport** tab. By default, these features are disabled.

Note: If Fibre Transport is not used currently and you want to use the SAN Client feature, you must first obtain a SAN Client license key. Then, add the key to your master server.

The ports on all FC HBA cards default to the initiator mode. When you select the **Enable SAN Client Fibre Transport on the Media Server (use FT for backups to this appliance)** option, Port 1 on the installed FC HBA cards is configured for the target mode. This feature requires a SAN Client license on the NetBackup master server, contact Symantec Support to obtain the appropriate license.

When you select the **Enable Fibre Transport for duplication and backups on a Deduplication Appliance** option Fibre transport is used to perform deduplication based backups using the Netbackup Appliance.

Changing the Fibre Transport settings

Use the following procedure to change the Fibre Transport settings.

To change the Fibre Transport settings

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click the **Settings > Network > Fibre Transport** tab.
- 3 Click to enable the **Enable SAN Client Fibre Transport on the Media Server (use FT for backups to this appliance)**
- 4 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".

- 5 Click **Save** to apply the changed settings.

See ["Settings > Network > Fibre Transport"](#) on page 53.

See ["About Fibre Channel port configuration options for the NetBackup 52xx appliances"](#) on page 298.

See ["About the card slots on NetBackup 52xx series appliances"](#) on page 293.

Settings > Network > Host

The **Settings > Network > Host Configuration** tab enables you to configure the host name, for either DNS or non-DNS systems. The **Host Configuration** tab displays the **Host name** of your appliance and the remaining page 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 using the host name details.

Changing DNS and host name Configuration settings

Use the following procedure to change or add the **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 61.</p>
Domain Name Suffix	<p>Enter the suffix name of the DNS server.</p>
Search Domain(s)	<p>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.</p>

- 4 Click **Save**.

To change the non-DNS configuration settings:

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Settings > Network > Host** tab.

3 Enter the non-DNS configuration information using the following fields:

Fields	Description
IP Address	<p>Enter the IP address of the appliance.</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 61.</p>
Fully-Qualified-Hostname	Enter the Fully Qualified Host Name (FQHN) of the appliance.
Short-Hostname	<p>Enter the short name of the appliance.</p> <p>After you enter all of the necessary information in these fields, you must click Add.</p>

4 Click **Save**.

Settings > Network > WAN Optimization options

The WAN Optimization feature applies various techniques to improve outbound network traffic from your appliance. This feature includes benefits such as:

- Beneficial for 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.
- WAN optimization is non-intrusive, it does not impose any overhead in situations where the overall network traffic is already high. In some scenarios, when the overall network traffic is higher, the connection speed may not be optimized despite of this feature being enabled. In such situations the WAN Optimization is bypassed and it is not recorded in the traffic command optimized data per second report.

From **Settings > Network > WAN Optimization** tab, you can enable or disable WAN Optimization.

Table 2-12 lists the operations that you can perform under the WAN optimization using the NetBackup Appliance Shell Menu and the NetBackup Appliance Web Console.

Table 2-12 WAN Optimization operations

Operation	Description	NetBackup Appliance Shell Menu	NetBackup Appliance Web Console
Enable	The <code>Enable</code> command is used to enable the network optimization settings. The WAN optimization feature is enabled by default. See “Disabling, enabling, and viewing the WAN optimization settings” on page 58.	Yes	Yes
Disable	The <code>Disable</code> command is used to disable the network optimization settings. You can disable this setting using the NetBackup Appliance Web Console or the NetBackup Appliance Shell Menu. See “Disabling, enabling, and viewing the WAN optimization settings” on page 58.	Yes	Yes
Status	The <code>Status</code> command is used to view network optimization reports. See “Viewing the WAN optimization status” on page 60.	Yes	Not Applicable
Traffic	The <code>Traffic</code> command is used to view network throughput. It displays the amount of optimized and non-optimized traffic for a specific time period. See “Viewing the network connection traffic” on page 59.	Yes	No
Parameter	The <code>Parameter</code> command is used to view WAN optimization Parameter Information. It displays a list of internal values useful to the Symantec Support and Engineering. See “Disabling, enabling, and viewing the WAN optimization settings” on page 58.	Yes	No

For more information about `Main > Network > WANOptimization` commands refer to *Symantec NetBackup™ Appliance Command Reference Guide*.

Disabling, enabling, and viewing the WAN optimization settings

This section describes the operations you can perform to optimize your network connections.

To disable the WAN optimization settings

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Settings > Network > WAN Optimization**.
The **WAN Optimization** tab appears.
- 3 Select the **Enable Network Optimization** check-box to disable the WAN optimization setting.

The appliance disables the WAN Optimization settings and displays the following message:

```
Network Optimization Status Updated Successfully.
```

To enable the WAN optimization settings

- 1 Log in to the administrative NetBackup Appliance Web Console.
- 2 Click **Settings > Network > WAN Optimization**.
The **WAN Optimization** tab appears.
- 3 Select the **Enable Network Optimization** check-box to enable the WAN optimization setting.
- 4 The appliance enables the WAN Optimization settings and displays the following message:

```
Network Optimization Status Updated Successfully.
```

To view the WAN optimization setting parameters

- 1 Log in to the administrative appliance shell menu.
- 2 To view the WAN Optimization option, use the following command:

```
Main > Network > WANOptimization
```

The appliance displays all the options under WANOptimization.

- 3 To view the optimization setting Parameters, use the following command:

```
Parameters
```

- 4 The appliance displays a list of values. The second value is the WAN Optimization version number. The other values are for debugging purposes and can help the Symantec Support and Engineering teams to troubleshoot any optimization-related issues.

Viewing the network connection traffic

The `traffic` command does the following:

- Displays the amount of optimized and non-optimized traffic for a specific time period.
- Displays the output in MBytes/sec, Mbits/sec, and Kbits/sec to help minimize confusion between bit and byte measurements.
- Provides a high level view of the benefit of WAN Optimization. The output should not be used to account for every last byte of traffic.
- Measures the total traffic from a connection, before and after the connection is optimized.
- Computes the traffic from a non-optimized connection, using the following equation:

```
Total traffic - Optimized traffic = non-optimized traffic
```

Note: Due to measurement limitations and rounding errors, the non-optimized traffic value can be slightly inaccurate as a percentage of total traffic.

To view the network connection traffic

- 1 Log in to the administrative appliance shell menu.
- 2 To view the WAN Optimization option, use the following command:

```
Main > Network > WANOptimization
```

The appliance displays all the options under WANOptimization.

- 3 To view the network connection traffic, use the following command:

```
Traffic period_length periods
```

Note: In the command `period_length` is considered in seconds. `Periods` is the number of periods reported. For example, `Traffic 10 3` lists traffic for the periods [0 to 10], [10 to 20], and [20 to 30] seconds. The period lengths must be 10secs or more.

- 4 The appliance displays the amount of optimized and non-optimized traffic for a specific time period. This information is displayed in MBytes/sec, Mbits/sec, and Kbits/sec.

Note: Specifying 0 as the `period` allows the traffic command to run indefinitely

The following example displays the generated output after the `Traffic 10 5` command is executed.

	OPTIMIZED				NON-OPTIMIZED		
Time offset	MB/sec	MB/Sec	KB/sec		MB/sec	MB/Sec	KB/sec
(sec)	(sec)	(sec)	(sec)		(sec)	(sec)	(sec)
-----	-----	-----	-----		-----	-----	-----
10	0.00	0	8		0.00	0	17
20	0.00	0	14		0.00	0	11
30	0.00	0	21		0.00	0	15
40	0.01	0	102		0.00	0	0
50	0.00	0	8		0.00	0	17

Note: If **WAN Optimization** is enabled and the performance for a TCP connection is still not improved. Then the traffic bypasses the WAN Optimization settings and is considered as `NON-OPTIMIZED` traffic.

Viewing the WAN optimization status

The `Status` command displays the number of optimized and non-optimized connections. This classification is set when the TCP connection is established.

- If WAN Optimization is enabled and performance can be improved, the connection is optimized.

- If WAN Optimization is enabled and performance cannot be improved, the connection is not optimized.
- If WAN Optimization is disabled, the connection is not optimized in any scenario.
- If the WAN Optimization status is changed (from disabled to enabled or vice versa), the status of existing connections is not reset. Only new connections follow the new rules.

To view the WAN optimization status

- 1 Log in to the administrative NetBackup Appliance Shell Menu.
- 2 To view the WAN Optimization option, use the following command:

```
Main > Network > WANOptimization
```

The appliance displays all the options under WAN Optimization.

- 3 To view the optimization status, use the following command:

```
Status
```

- 4 The appliance displays the number of optimized and non-optimized connections, and the current enabled /disabled settings. The following example displays the generated output after the `Status` command is executed:

```
Network Optimization Report
-----
TCP connections optimized   = 53
TCP connections not optimized
(or not appropriate for optimization) = 0
Network Optimization = ENABLED
```

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 SUSE.

Global-scope IP addresses refer to the addresses that are globally routable. Unique-local addresses are treated as global on SUSE.

- 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 > 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 2-13](#) describes the data entry fields on the **Password Management** page.

Table 2-13 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 <code>P@ssw0rd</code> .
New Password	Enter the new password. Passwords with seven characters must include all of the following requirements while longer passwords must include at least three: <ul style="list-style-type: none">■ One uppercase letter.■ One lowercase letter.■ One number (0-9)■ One special character (<code>@#\$%^&*(){}[].</code>) Passwords may begin with an uppercase letter or they may end with a number. However, when these characters appear in those positions, the password is not considered to meet the minimum requirements.
Confirm New Password	Re-enter the new password for confirmation.

Table 2-13 Data entry fields for administrator password change (continued)

Field	Description
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 34.

Settings > Date and Time

On the **Settings > Date and Time** page, you can change the date, the time, and the time zone parameters 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 on the appliance.
- 2 Click **Settings > Date and Time**.
- 3 Enter the appropriate information in the fields:

Time Zone	To assign a time zone to the appliance, click on the Time zone drop-down box and select the appropriate time zone.
Specify date & time	<div>To enter the date and the time manually, select this option and enter the following information:<ul style="list-style-type: none">■ In the first field, enter the date by using the mm/dd/yyyy format.■ In the second field, enter the time by using the hh:mm:ss format. Entries must be in the 24 hour format (00:00:00 - 23:59:59).</div>

NTP

To synchronize the appliance with an NTP server, select this option and enter the NTP Server IP address.

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 `Date` command refer to the *Symantec NetBackup Appliance Command Reference Guide*.

Settings > Authentication

The **Settings > Authentication** menu is used to display the following tabs:

- **Server Configuration** - enables you to add or import LDAP server configuration settings. See “[Settings > Authentication > Server Configuration](#)” on page 65. You can also configure the LDAP server settings using the `Main > Settings > Security > Authentication` commands under the shell menu.
- **User Configuration** - enables you to manage users, manage user groups, and grant permissions to these users and user groups. See “[Settings > Authentication > User Management](#)” on page 76. You can also configure the users using the `Main > Settings > Security > Authorization` commands under the shell menu.

For more information about the `Authentication` and `Authorization` commands refer to the *Symantec NetBackup Appliance Command Reference Guide*.

Settings > Authentication > Server Configuration

This section describes how to use the PAM (Pluggable Authentication Module) plug-in from your appliance operating system to configure and work with an LDAP (Lightweight Directory Access Protocol) server. The PAM plug-in enables you to use the LDAP directory to provide user credentials and maintain distributed directory information service for your appliance.

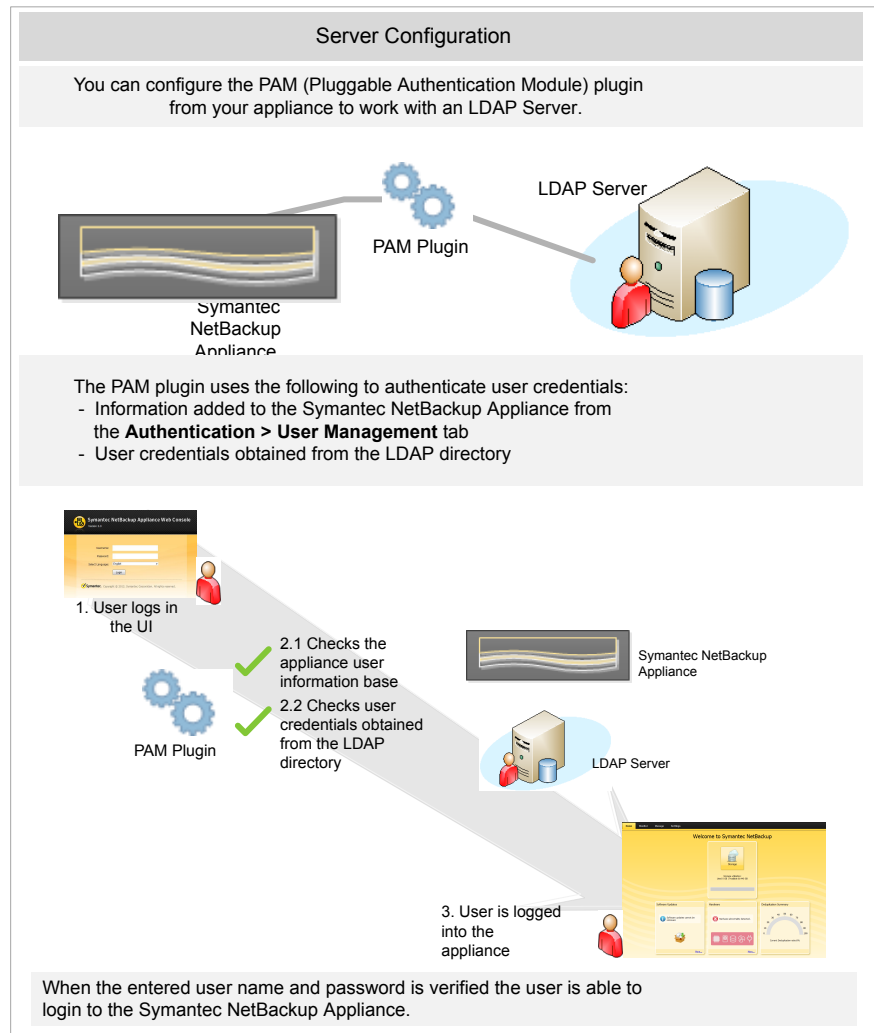
Using the Server Configuration feature to use your LDAP directory as a single directory source to access user information and authenticate the users across all your appliances. It also enables you to import and export LDAP server configuration settings to apply them for multiple appliances.

You can also set the SSL certificates for an LDAP PAM Authentication module that enables you to establish a secure connection, between the NetBackup Appliance LDAP PAM module and the LDAP server. [Figure 2-1](#) provides a brief overview of

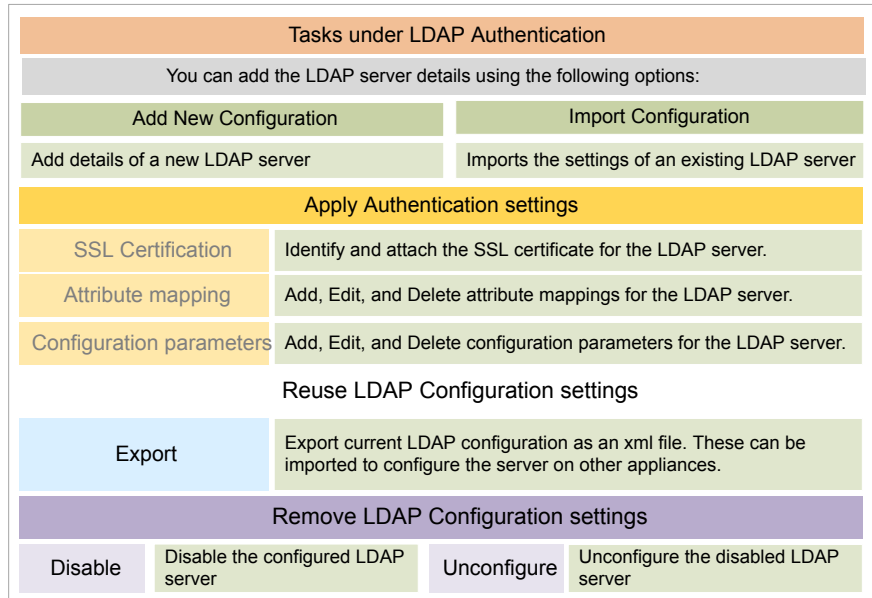
how the PAM plug-in enables you to use the LDAP server for authenticating user credentials.

Note: Ensure that the Unix services for Active Directory are installed and configured. It is important that the Unix attributes `uidNumber`, `gidNumber`, `homeDirectory` are configured:

Figure 2-1 LDAP Authentication



This following diagram illustrates the tasks you can perform relating to your LDAP authentication settings:



You can use the **Settings > Authentication > Server Configuration** tab on the NetBackup Appliance Web Console, to use the PAM plug-in for configuring the LDAP server.

Adding an LDAP server configuration

You can use the **Server Configuration** tab to add the details of an LDAP server and configure it with your appliance. The LDAP server enables you to access and maintain distributed directory information services for your appliance. The following procedure describes the steps to configure your LDAP server using NetBackup Appliance Web Console.

To configure an LDAP server

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication > Server Configuration**.
The appliance displays the **Server Configuration** tab with two radio buttons.
- 3 Select the **Add new configuration** radio button.
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 IP address of your LDAP Server.	
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.	
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, while configuring the LDAP or Active Directory Authentication server, 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 SSL channel established doesn't do the server side certificate validation. This validation starts after the server's root certificate is explicitly set using Set Certificate option. For more information, refer to See "Setting the SSL Certification" on page 70.</p>	

Field	Description	Example
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 or Active Directory.	

- 5 Click **Configure**, configure the LDAP server using the entered parameters.
The appliance configures and enables the new LDAP server and displays the **Attribute Mapping** and **Configuration Parameters** table.

Importing an LDAP server configuration

You can use the **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 Symantec NetBackup appliance configures and connects to the LDAP server using these details.

Note: Save the `.xml` file in the base directory or a directory underneath the base directory.

To import an LDAP server configuration:

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication > Server Configuration**.
The appliance displays the **Server Configuration** tab with two radio buttons.
- 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.

Note: Ensure that the `.xml` file is in the base directory or a directory underneath the base directory. `:/inst/patch/incoming/`

- 5 Click **Import**.
The appliance imports the `.xml` and configures the LDAP server using the details provided in the `.xml`.

See [“Settings > Authentication > Server Configuration”](#) on page 65.

See [“Adding an LDAP server configuration”](#) on page 67.

See [“Importing an LDAP server configuration”](#) on page 69.

Setting the SSL Certification

You can use the **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** link is enabled only after the LDAP server is configured. Save the SSL certificate file in the folders of the appliance, to which you are configuring the LDAP server.

To set the SSL certificate:

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication > Server Configuration**.
The appliance displays the **Server Configuration** tab with the details of configured LDAP Server.
- 3 Click on the **Set Certificate** link displayed at the end of the tab.
The appliance displays a pop box to enter the path to the SSL certificate.

Note: The LDAP and AD validation starts only after the server's root certificate is explicitly set using **Set Certificate** option.

- 4 Enter the absolute path to the SSL certificate file in the **File Path** field.

Note: Ensure that the file is in the base directory or a directory underneath the base directory. `:/inst/patch/incoming/`

- 5 Click **OK**.
The appliance imports the SSL certificate and is used to authenticate the LDAP Server.

See [“Settings > Authentication > Server Configuration”](#) on page 65.

Exporting the configuration file

You can use the **Server Configuration** tab to export LDAP configuration file. This file can be used to save the details of the configured LDAP server and imported for other appliances. The following procedure describes the steps to export the configuration details of your LDAP server into an `.xml` file.

Note: The **Export** link is enabled only after the LDAP server is configured.

To export the configuration file:

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication > Server Configuration**.
The appliance displays the **Server Configuration** tab with the details of configured LDAP Server.
- 3 Click on the **Export** link displayed at the end of the tab.
The appliance displays a pop box to enter the path for exporting the `.xml` file.
- 4 Enter the location within your appliance to export the configuration details.

Note: Ensure that you save the file in the base directory or a directory underneath the base directory. `:/inst/patch/incoming/`

- 5 Click **OK**.
The appliance converts the configuration details in an `.xml` file and exports it to the specified location.

See [“Settings > Authentication > Server Configuration”](#) on page 65.

Unconfiguring the LDAP server

You can use the **Server Configuration** tab to unconfigure an LDAP server. The following procedure describes the steps to unconfigure the LDAP server.

Warning: Unconfiguring the LDAP server will delete the current settings and the authentication provided through the LDAP server.

To unconfigure an LDAP server:

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication > Server Configuration**.
The appliance displays the **Server Configuration** tab with the details of configured LDAP Server.

- 3 Click on the **Unconfigure** link 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.

See [“Settings > Authentication > Server Configuration”](#) on page 65.

Enabling the LDAP server

You can use the **Server Configuration** tab to enable the disabled LDAP server. The following procedure describes the options to enable the configured LDAP server.

Note: When you configure the LDAP server it is set as enabled, by default.

To enable the configured server:

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication > Server Configuration**.
The appliance displays the **Server Configuration** tab with the details of configured LDAP Server.

If the configured LDAP server is disabled the following messages is displayed on the **Server Configuration** tab next to the **Enable** link.

```
LDAP authentication is disabled.
```


- 3 Click on the **Enable** link.

The appliance displays the following messages:

```
Are you sure you want to enable the configuration?
```

- 4 Click **OK** to enable the LDAP server.

The appliance enables the LDAP Server.

See [“Settings > Authentication > Server Configuration”](#) on page 65.

Disabling the LDAP server

The following procedure describes the options to disable the configured LDAP server.

To disable the configured server:

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication > Server Configuration**.

The appliance displays the **Server Configuration** tab with the details of configured LDAP Server.

If the configured LDAP server is enabled the following messages is displayed on the **Server Configuration** tab next to the **Disable** link.

```
LDAP authentication is enabled.
```

- 3 Click on the **Disable** link.

The appliance displays the following message:

```
Are you sure you want to disable the LDAP server?
```

- 4 Click **OK** to enable the LDAP server.

The appliance enables the LDAP Server.

See [“Settings > Authentication > Server Configuration”](#) on page 65.

Deleting LDAP configuration parameters

When you configure a new LDAP server the configuration parameters added or imported are displayed in the **Configuration Parameter** table on the **LDAPAuthentication** tab. The following procedure describes the steps to add LDAP configuration parameters.

To delete a configuration parameter:

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Settings > LDAP > Server Configuration**.
The appliance displays the **LDAP Authentication** tab with the details of configured LDAP Server in the **Configuration Parameter** table.
- 3 Select the configuration parameter you want to delete.
- 4 Click the **Delete** button displayed at the top of the **Configuration Parameter** 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 Parameter** table.

See [“Settings > Authentication > Server Configuration”](#) on page 65.

Adding LDAP configuration parameters

When you configure a new LDAP server the configuration parameters added or imported are displayed in the **Configuration Parameter** table on the **Server Configuration** tab. The following procedure describes the steps to add LDAP configuration parameters.

To add a configuration parameter:

- 1 Log in to the NetBackup Appliance Web Console
- 2 Click **Settings > Authentication > Server Configuration**.
The appliance displays the **Server Configuration** tab with the details of configured LDAP Server in the **Configuration Parameter** table.
- 3 Click the **Add** button displayed at the top of the **Configuration Parameter** table.
The appliance displays a new row in the **Configuration Parameter** table with the **Update** and **Cancel** buttons.
- 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 Parameter** table.

See [“Settings > Authentication > Server Configuration”](#) on page 65.

Adding an LDAP attribute mapping

When you configure a new LDAP server its attribute mappings are added or imported and displayed in the **Attribute Mapping** table on the **Server Configuration** tab. The following procedure describes the steps to add a new attribute mapping for the LDAP server.

To add an attribute mapping:

1 Log in to the NetBackup Appliance Web Console.

2 Click **Settings > Authentication > Server Configuration**.

The appliance displays the **Server Configuration** tab with the details of configured LDAP Server in the **Attribute Mapping** table.

3 Click the **Add** button displayed at the top of the **Attribute Mapping** table.

The appliance displays a new row in the **Attribute Mapping** table with the **Update** and **Cancel** buttons.

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 Mapping** table.

See [“Settings > Authentication > Server Configuration”](#) on page 65.

Deleting an LDAP attribute mappings

When you configure a new LDAP server its attribute mappings are added or imported and displayed in the **Attribute Mapping** table on the **Server Configuration** tab. The following procedure describes the steps to delete an attribute mapping for the LDAP server.

To delete an attribute mapping:

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication > Server Configuration**.
The appliance displays the **Server Configuration** tab with the details of configured LDAP Server in the **Attribute Mapping** table.
- 3 Select the attribute mapping you want to delete in the **Attribute Mapping** table.
- 4 Click the **Delete** button displayed at the top of the **Attribute Mapping** 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 Mapping** table.

See [“Settings > Authentication > Server Configuration”](#) on page 65.

Settings > Authentication > User Management

The Symantec NetBackup Appliance enables you to add new users and create user groups for accessing your appliance.

The user management feature enables you to:

- Add users and user groups on the local appliance
- Add users and user roles present in your LDAP server and allow them to access the NetBackup Appliance
- Grant administrative permissions
- Revoke administrative permissions
- Delete existing users and user groups

One of the primary reasons for configuring the PAM plug-in to work with an LDAP server, is to enable the user base from the LDAP server to access the Symantec NetBackup Appliance. You need to register the LDAP users with the appliance, so as to map them to the appliance user base. If you do not register the LDAP users, they cannot log onto the appliance.

You can access the **User Management** tab using the **Settings > Authentication > User Management** menu. This section provides an overview of the tasks you can perform using the **User Management** tab.

Adding users using the User Management tab

The following procedure describes how to add new users.

To add new users:

- 1 Log in to the NetBackup Appliance Web Console
- 2 Click **Settings > Authentication > User Management** tab.
The appliance displays the **User Management** tab.
- 3 Click on the **Add User** link, displayed at the end of the **User Management** tab.
The appliance displays the **Add User** pop-up box.
- 4 Select the type of user from the **User Type** drop-down list. The drop-down list displays the following options:
 - **Local** - Select this option to add a user to the appliance database.
 - **LDAP** - Select this option to register a user that is already present on the LDAP server that is configured with your appliance.

Note: If you do not register an LDAP user with the appliance, the user cannot access the appliance.

- 5 Enter the name of the user in the **User Name** field.
- 6 Click **Save**.
The appliance adds the new user and displays the following message:

User added successfully.

- 7 Click **OK** to continue.
The new user is added to the list of users on the **User Management** tab.

See [“Settings > Authentication > User Management”](#) on page 76.

Deleting users using the User Management tab

Always ensure that you delete the user from the NetBackup Appliance prior to deleting it from the LDAP or Active Directory. If the user is removed from the LDAP directory (and not removed from appliance allowed to login list), though the user is listed as LDAP authorized user, the user won't be able to login. So, this users poses no security threat.

This following procedure describes how to delete existing users.

To delete existing users:

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication > User Management** tab.
The appliance displays the **User Management** tab.
- 3 Select the user you want to remove.
- 4 Click on the **Delete User** link, 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 and removed from the **User Management** tab.

See [“Settings > Authentication > User Management”](#) on page 76.

Adding user groups using the User Management tab

This following procedure describes how to add new user groups.

To add user group:

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication > User Management** tab.
The appliance displays the **User Management** tab.
- 3 Click on the **Add Group** link, displayed at the end of the **User Management** tab.
The appliance displays the **Add Group** pop-up box.
- 4 Enter the name of the user group in the **Group Name** field.

Note: If you do not register an LDAP user group with the appliance, the users belonging to the 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.

See [“Settings > Authentication > User Management”](#) on page 76.

Deleting user groups using the User Management tab

This following procedure describes how to delete existing user groups.

To delete user groups:

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication > User Management** tab.
The appliance displays the **User Management** tab.
- 3 Select the user group you want to delete.
- 4 Click on the **Delete User** link, displayed at the end of the **User Management** tab.

The appliance displays the following message:

```
Group Deleted Successfully
```

- 5 Click **Ok** to delete the selected user group.

The selected user group is deleted and removed from the **User Management** tab.

See [“Settings > Authentication > User Management”](#) on page 76.

Granting permissions to users and user groups

This following procedure describes how to grant administrative permissions to users and user groups.

To grant administrative permission:

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication > User Management** tab.

The appliance displays the **User Management** tab.

- 3 Select the user or user group which has **NoRole** displayed in the **Role** column.
- 4 Click on the **Grant Permission** link, displayed at the end of the **User Management** tab.

The appliance displays the following message:

```
User Authorized Successfully
```

- 5 Click **OK** to continue.

The term **Administrator** is displayed in the **Role** column for the selected user. This user can now log into the appliance as an Admin user.

See [“Settings > Authentication > User Management”](#) on page 76.

Revoking permissions from users and user groups

This following procedure describes how to revoke administrative permissions assigned to users and user groups.

To revoke administrative permissions:

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Settings > Authentication > User Management** tab.
The appliance displays the **User Management** tab.
- 3 Select the user or user group which has **Administrator** displayed in the **Role** column.
- 4 Click on the **Revoke Permission** link, displayed at the end of the **User Management** tab.

The appliance displays the following message:

```
User Un-authorized Successfully
```

- 5 Click **OK** to continue.

The term **NoRole** is displayed in the **Role** column for the selected user. This user can no longer log into the appliance as an Admin user.

See [“Settings > Authentication > User Management”](#) on page 76.

Monitoring the NetBackup appliance

This chapter includes the following topics:

- [About monitoring the NetBackup Appliance](#)
- [About hardware monitoring and alerts](#)
- [About Symantec Critical System Protection](#)

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.

[About monitoring the NetBackup Appliance](#) describes the components that you can monitor using the **Monitor** menu:

Table 3-1 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 82.

Table 3-1 Monitor tab (continued)

Monitor	Lets you...	Topic
SCSP Audit View	Monitor the Symantec Critical System Protection (SCSP) agent. The SCSP agent is installed and configured when you initially configure your appliance. This agent ensures that your appliance's audit logs are sent to the SCSP server to be validated and verified.	See “About Symantec Critical System Protection” on page 94.

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 82.
- Sending an email to the local administrator. See [“About Email notification from a NetBackup appliance”](#) on page 92.
- Sending an alert to the SNMP manager. See [“About SNMP”](#) on page 40.
- Sending a notification to Symantec using Call Home. See [“About Call Home”](#) on page 41.

Symantec recommends that you check for hardware alert messages daily.

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

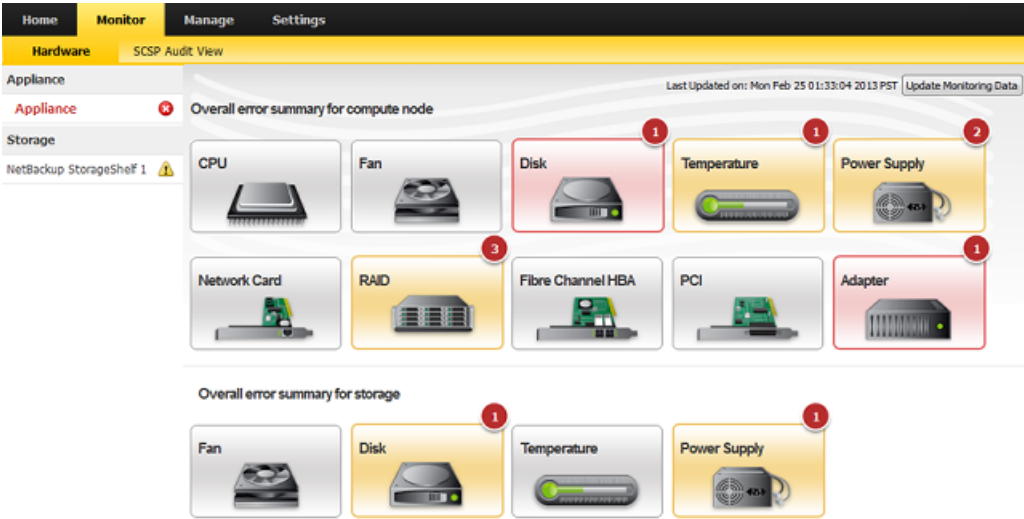
Monitoring the hardware components of your appliance is important for correct functioning of the appliance.

The **Monitor > Hardware** page on the NetBackup Appliance Web Console lets you monitor the hardware, the storage devices, and all the components that are associated with them. Using hardware monitoring, you can monitor the appliance hardware and storage components that are listed in the following table:

Table 3-2 Hardware components monitored in 52xx appliances

Appliance	CPU, Fan, Disk, Temperature, Power Supply, Network Card, RAID, Fibre Channel HBA, PCI, Adapter
Storage	Fan, Disk, Temperature, Power Supply

Figure 3-1 Hardware components monitored in 52xx series appliances



The **Monitor > Hardware** page of the NetBackup Appliance Web Console lets you monitor the appliance hardware through the following ways:

- Displaying the overall hardware error summary
The left pane of [Figure 3-1](#) displays the **Appliance** and the **Storage** components. The right pane displays the **Overall error summary for compute node** and **Overall error summary for storage** for the appliance and the storage respectively. The information that is displayed is generated from the last Call Home heartbeat. You can click **Update Monitoring Data** to get the latest information for the overall hardware error summary.
- 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 warning 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.

- **Acknowledging errors or warnings**
When a hardware component displays error or warning messages for hardware status, the appliance sends error notifications at regular intervals. These error notifications can be suppressed by acknowledging the errors or warning until the issue is resolved. After the issue has been resolved, the errors or warnings are automatically cleared.

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

Table 3-3 Appliance hardware that is monitored

Hardware monitored	Sample of the data collected
CPU	<ul style="list-style-type: none">■ ID - 2■ Status - OK■ Voltage - 0.78 Volts■ Low watermark - 0.55 V■ High watermark - 1.51 V
Disk	<ul style="list-style-type: none">■ ID - 3■ Slot number - 0■ Status - Online, Spun up■ Foreign State - None■ Firmware version - 0002■ Serial number - Z1N2BM45■ Capacity - 930.390GB■ Type - SAS■ Enclosure ID - 252
Fan	<ul style="list-style-type: none">■ ID - 3■ Name - System Fan 3■ Status - OK■ Speed - 9653.00 RPM■ Low watermark - 1715.00 RPM
Power Supply	<ul style="list-style-type: none">■ ID - 1■ Status - Power Supply AC lost■ Wattage - 0.00 Watts■ High watermark - 920.00 Watts

Table 3-3 Appliance hardware that is monitored (*continued*)

Hardware monitored	Sample of the data collected
RAID	<ul style="list-style-type: none"> ■ ID - 2 ■ Name - VD-0 ■ Status - Optimal ■ Capacity - 35.469TB ■ Type - RAID-6 ■ Disks - 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16 ■ Write policy - Writeback ■ Enclosure ID - 24 ■ All hostspares available - yes
Temperature	<ul style="list-style-type: none"> ■ ID - 2 ■ Type - Outtake Vent Temperature Types of temperature can be Intake Vent Temperature, Outtake Vent Temperature, <i>P1 Therm Margin</i> , and <i>P2 Therm Margin</i>. These are the temperature sensors that monitor the temperature of the appliance. Note: The reading for <i>P1 Therm Margin</i> , and <i>P2 Therm Margin</i> 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. ■ Value - 44.00 degrees C ■ Low watermark - 0.00 degrees C ■ High watermark - 85.00 degrees C
Adapter	<ul style="list-style-type: none"> ■ ID - 2 ■ Adapter model - Intel®) Integrated RAID Module RMS25CB080 ■ Adapter Status - OK ■ BBU Status - OK ■ BBU Learn Cycle active - N/A ■ Charge - 65% ■ Charging status - None ■ Voltage - OK ■ Temperature- OK ■ Manufacturing date - Mar 27, 2013

Table 3-3 Appliance hardware that is monitored (*continued*)

Hardware monitored	Sample of the data collected
PCI	<ul style="list-style-type: none"> ■ ID - This is an ID of the hardware for the purpose of acknowledging errors. ■ Slot - 1 ■ Details - RAID bus controller
Fibre Channel HBA	<ul style="list-style-type: none"> ■ ID - 2 ■ Status - Online ■ Mode - Initiator <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> <ul style="list-style-type: none"> ■ PCI Slot - Slot2 ■ World wide port name - 21:00:00:24:FF:44:11:8E ■ Speed - 8 Gbit/s ■ Remote Port - 0x21000024ff3b0618
Network card	<ul style="list-style-type: none"> ■ ID - 3 ■ Port name - eth2 ■ Card model - BaseBoard ■ Serial number -8e-22-59-ff-ff-67-1e-00 ■ Speed - 1 Gb/s ■ MAC address -00:1E:67:59:22:90 ■ Link state - PLUGGED
Partition information	<ul style="list-style-type: none"> ■ ID - 4 ■ Partition - AdvancedDisk ■ Total - 1TB ■ Used - 1% ■ Status - Optimal
MSDP	<ul style="list-style-type: none"> ■ ID - 1 ■ Queue Size - 6785 ■ Oldest TLog Creation Date - Thu Aug 22 01:03:38 2013

Table 3-4 Storage shelf hardware that is monitored

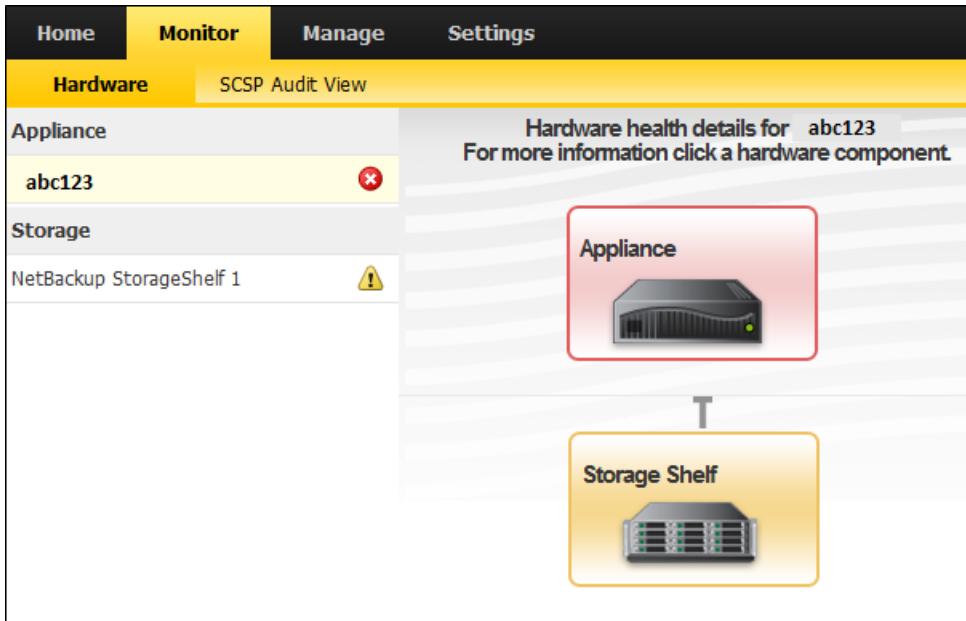
Hardware monitored	Sample of the data collected
Disk	<ul style="list-style-type: none">■ ID - 1■ Beacon - Green■ Slot No - 1■ Status - Unconfigured(good), Spun down■ Capacity - 2.727TB■ Firmware version - A222■ Serial number - YVHAGBAD■ Foreign state - None■ Type - SAS■ Storage shelf ID - 24
Fan	<ul style="list-style-type: none">■ ID - 2■ Status - Device Present■ Speed - 3360 RPM■ Low watermark - 2000 RPM
Power Supply	<ul style="list-style-type: none">■ ID - 2■ Status - Presence detected
Temperature	<ul style="list-style-type: none">■ ID - 2■ Type - Backplane Temperature 2■ Value - 27 degrees C■ High watermark - 51 degrees C

Monitor > Hardware > Health details

You can get a detailed health status of the appliance hardware from the **Monitor > Hardware Health details** page of the NetBackup Appliance Web Console.

The left pane of the **Monitor > Hardware** page lists **Appliance** and **Storage**. The right pane displays the overall error summary for the hardware components.

Figure 3-2 Hardware health details in 52xx appliances



When you click the appliance that is listed under **Appliance** on the left pane, a **Hardware health details** page opens as shown in Figure 3-2. The **Hardware health details** page displays health details for the appliance and the storage shelf that is attached to it. To get detailed information on the hardware health of a component, click the **Appliance** icon or the **Storage Shelf** icon. Clicking the icons opens a pop-up window that displays the detailed information for the selected device.

The **Storage Shelf details** pop-up lists information for disks, fan, power supply, and temperature.

The disks in the storage shelf have a beacon to flash light. The beacon helps to locate a disk within the storage shelf and it can be used to identify a disk that requires replacement.

- When you click the **Beacon** icon against a disk drive, the following message is displayed at the top of the disk information table.

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

- You must provide the duration for which you want the disk to flash the beacon light. After you have entered the duration (in minutes), click **Start Beacon**.
- This action lights-up the beacon for the selected disk in the storage shelf. When the **Beacon** icon on the NetBackup Appliance Web Console flashes green light,

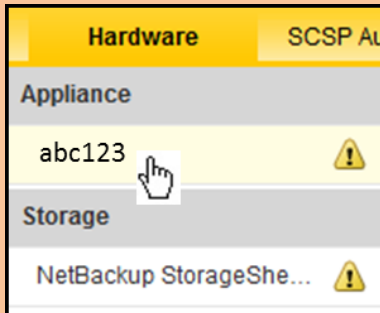
it indicates that the action is completed. When the beacon flashes red light, it indicates failure to complete the action.

- Hovering over the beacon icon, displays its status.

The **Appliance details** pop-up helps you to determine the serial number of your appliance along with details for various hardware components. When you report an issue to Symantec support, the Technical Support engineer requests for your appliance serial number.

[Figure 3-3](#) illustrates locating the serial number of your appliance.

Figure 3-3 Appliance serial number



From the left-pane of the **Monitor > Hardware** page, click an appliance. This action opens the hardware health details page.



On the hardware health details page, click the **Appliance** icon to open the **Appliance Details** pop-up box.

The **Appliance Details** pop-up box displays the serial number of the appliance.



Acknowledging hardware errors

You can use the acknowledge function of hardware monitoring to acknowledge errors or warnings that are related to the appliance hardware. Acknowledging errors suppresses the error notifications (that the appliance sends in case of a hardware failure) until the issue is resolved. You can acknowledge errors through the NetBackup Appliance Web Console and the NetBackup Appliance Shell Menu.

To acknowledge errors from the NetBackup Appliance Web Console

- 1 Log on to the NetBackup Appliance Web Console. The **Home** tab opens.
- 2 From the **Home** tab, click **Monitor > Hardware**.
- 3 On the **Monitor > Hardware** menu, click the highlighted hardware icon that displays the error state. A pop-up window opens, which displays error information in a tabular format.
- 4 To acknowledge errors or warnings, select the **Acknowledge** check-box that is against the error state that you want to acknowledge.
- 5 Click **Update acknowledgment** and close the pop-up window.
- 6 To start receiving error notifications for the acknowledged error state, clear the **Acknowledge** check-box against the error.
- 7 Click **Update acknowledgment** and close the pop-up window.

To acknowledge errors from the NetBackup Appliance Shell Menu

- 1 Log on to NetBackup Appliance Shell Menu.
- 2 To acknowledge errors or warnings for any hardware component, run the `Main > Settings > Alerts > AcknowledgeErrors` command. A table with an error ID and error status is displayed.
- 3 Enter the ID of the error that you want to acknowledge. You can enter *all* to acknowledge all the errors or warnings. On entering the error ID, the following message is displayed:

```
- [Info] Successfully acknowledged alerts.
```

- 4 To start receiving error notifications for the acknowledged error state, run the `Main > Settings > Alerts > ClearAcknowledgedErrors` command.
- 5 Enter the ID of the error for which you want to receive notifications. You can enter *all* to clear all the acknowledged errors or warnings. On entering the error ID, the following message is displayed:

```
- [Info] Successfully removed acknowledged alerts.
```

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 command from the NetBackup Appliance Shell Menu to configure the email address that you want to use to receive the hardware failure notification. 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 *Symantec NetBackup™ Appliance Command Reference Guide*.

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

Compute Node abc123

Time Monitoring Ran: Thu Sep 5 2013 23:24:04 UTC

```
+-----+
|                                     Disk Information                                     |
+-----+
||ID| Slot | Status | Foreign|Firmware| Serial |Capacity |Type|Enclosure| State |Acknowled-|
|| |Number|      | State |Version | Number |         |   |   ID    |      |-ge       ||
||-+-+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
||1 |0      |Online, |None   |0002   |Z1N1PWYR|930.390GB|SAS |99      |OK     |N/A      ||
|| |      |Spun Up |       |       |         |         |         |    |        |       |         ||
||-+-+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
||2 |1      |Rebuild |None   |0002   |Z1N1Q05F|930.390GB|SAS |99      |OK     |N/A      ||
|| |      |(15%)  |       |       |         |         |         |    |        |       |         ||
||-+-+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     RAID Information                                     |
+-----+
|| |      |      |      |      |      |      |      |      |Enclo-| All |      |      |
||ID|Name|Status |Capacity | Type |Disks|Write Policy|-sure |hotspares|State|Acknow-|
|| |      |      |      |      |      |      |      | ID |available|     |-ledge ||
||-+-+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|| |      |      |      |      |      |1 2 3|      |      |      |      |      |      ||
|| |      |      |      |      |      |4 5 6|      |      |      |      |      |      ||
||3 |VD-1|Optimal |35.469TB |RAID-6|7 8 9|WriteBack |41 |yes   |OK   |N/A   ||
|| |      |      |      |      |      |10 11|      |      |      |      |      |      ||
|| |      |      |      |      |      |12 13|      |      |      |      |      |      ||
|| |      |      |      |      |      |14 15|      |      |      |      |      |      ||
||-+-+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
||4 |VD-0|Degraded |930.390GB |RAID-1|0 1 |WriteThrough|99 |no    |OK   |N/A   ||
```

		(Rebuilding..)					
+-----+							
Power Supply Information							
+-----+							
ID	Status	Wattage	HighWaterMark	State	Acknowledge		
+-----+							
1	Power Supply AC lost	0.00 Watts	920.00 Watts	Warning	No		
+-----+							
Temperature Information							
+-----+							
ID	Type	Temperature	LowWaterMark	HighWaterMark	State	Acknowledge	
+-----+							
3	P1 Therm	-12 degree	-128.00	-15.00	Warning	No	
	Margin	C	degrees C	degrees C			
+-----+							
Partition Information							
+-----+							
ID	Partition	Total	Used	Status	State	Acknowledge	
+-----+							
4	AdvancedDisk	744 GB	98 %	Optimal	Warning	No	
+-----+							
+-----+							

Power Supply Information

ID	Status	Wattage	HighWaterMark	State	Acknowledge
1	Power Supply AC lost	0.00 Watts	920.00 Watts	Warning	No

Temperature Information

ID	Type	Temperature	LowWaterMark	HighWaterMark	State	Acknowledge
3	P1 Therm	-12 degree	-128.00	-15.00	Warning	No
	Margin	C	degrees C	degrees C		

Partition Information

ID	Partition	Total	Used	Status	State	Acknowledge
4	AdvancedDisk	744 GB	98 %	Optimal	Warning	No

Note: If the email notification is not readable on your email client, change the font of the email to a fixed-width font. The font settings might be different for different email clients. The following procedure lets you change an existing email font to a fixed-width font for Microsoft Outlook 2010.

To improve the readability of the email notification for Microsoft Outlook 2010, change the font by following the steps below:

- 1 Go to the **File** menu and select **Options**. The Outlook Options window opens.
- 2 From the left pane of the Outlook Options window, select **Mail**.
- 3 Under the **Compose messages** section, click **Stationery and Fonts**. The Signatures and Stationery window opens.
- 4 On the **Personal Stationery** tab, under **Composing and reading text messages**, click **Font**. The Font window opens.
- 5 From the **Font** list, select **Courier New**.

About Symantec Critical System Protection

The Symantec Critical System Protection (SCSP) secures physical and virtual servers that use flexible, policy-based monitoring, and protection. It provides policy-based monitoring, protection, and helps to comply with security requirements.

It enables you to do the following:

- Ensures applying the host integrity and compliance settings. With host intrusion and detection-based system monitoring, notification, and auditing.
- Provides intrusion detection and intrusion prevention for the appliance, based on the backup policy selected.
- Leverages the Symantec Protection Center for advanced security management only if the appliance is integrated with SCSP server.
- Address the compliance requirements across heterogeneous environments.
- Monitors and records all the security relevant information like:
 - User logins, logouts, and failed login
 - Sudo commands
 - User addition, deletion, password changes
 - Group addition, deletion, member modifications
 - System auto start change options
 - Modifications to all system directories and files (which includes Core system files, core system configuration files, installation programs, common daemon files)
 - Changes to Appliance scripts in `/opt/NBAppliance/scripts` directories
 - USB device connection and disconnection
 - Detected system attacks from UNIX Rootkit File / Directory Detection, UNIX Worm File/Directory Detection, Malicious Module Detection, Suspicious Permission Change Detection, and so on
 - Shell menu operations

Monitor > SCSP Audit View

You can use the **Monitor > SCSP Audit View** menu to monitor the Symantec Critical System Protection (SCSP) agent.

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

For more information about SCSP, refer to the following section:

See [“About Symantec Critical System Protection”](#) on page 94.

You can use the **SCSP Audit View** page, to perform the following tasks:

- **SCSP Documentation** - Enables you to view documentation about the Symantec Critical System Protection.
See [“About viewing SCSP-specific documentation”](#) on page 102.
- **Connect** - Enables you to connect to the SCSP server from the **SCSP Audit View** page.
See [“Connecting to the SCSP server”](#) on page 101.
- **Set Log Retention** - Enables you to set the period or log files size for retaining audit logs from the **SCSP Audit View** page.
See [“Setting the audit log retention specification”](#) on page 100.
- **Filter logs** - Enables you to filter the SCSP audit logs displayed on the **SCSP Audit View** page.
See [“Filtering SCSP audit logs”](#) on page 98.

The **SCSP Audit View** page displays the following columns are used to display the event log information:

Table 3-5 Columns used to display the event logs

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

Table 3-5 Columns used to display the event logs (*continued*)

Columns	Description
Severity	<p>Displays the severity of each event in the log. For example, an event like the Sever Error would be of Critical severity.</p> <p>The following Severity types are displayed:</p> <ul style="list-style-type: none">■ Info - Events with a severity of Info contain information about normal system operation.■ Notice - Events with a severity of Notice contain information about normal system operation.■ Warning - Events with a severity of Warning indicate unexpected activity or problems that have already been handled by Symantec Critical System Protection. These Warning messages 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 to the specific resources if necessary.■ Major - Events with a severity of Major imply more affect than Warning and less affect than Critical.■ Critical - Events with a severity of Critical indicate activity or problems that might require administrator intervention to correct.
Message	Displays the message describing the logged event.
Details	<p>Enables you to view the details of each logged event. For example, if you want to view the details of the event displaying event type as Server Error, click on the drop-down arrow. It displays the Log Details pop-up window with the details of the logged event.</p> <p>See “Viewing SCSP audit log details” on page 96.</p>

Viewing SCSP audit log details

You can view the detailed information for each logged event using the **SCSP Audit View** page. To view the log details, click on the drop-down arrow in the **Details** column. The following information is displayed in the **Log Details** pop window:

Table 3-6 SCSP audit log details

Detail	Description
Event Severity	<p>Displays the severity of the logged event.</p> <p>The following Severity types are displayed:</p> <ul style="list-style-type: none">■ Info - Events with a severity of Info contain information about normal system operation.■ Notice - Events with a severity of Notice contain information about normal system operation.■ Warning - Events with a severity of Warning indicate unexpected activity or problems that have already been handled by Symantec Critical System Protection. These Warning messages 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 to the specific resources if necessary.■ Major - Events with a severity of Major imply more affect than Warning and less affect than Critical.■ Critical - Events with a severity of Critical indicate activity or problems that might require administrator intervention to correct.
Process ID	Displays the ID assigned to the process.
Rule Name	Displays the name of the policy rule that generated the event.
Process	Displays the name of the policy applied to the agent that triggered this event.
Event Date	Displays the date (YYYY-MM-DD HH:MM:SS) that the event occurred.
Event Type	Displays the event type for the logged event. For a detailed list of all the event types and their description refer to the SCSP documentation.
Sequence number	Displays the sequence number of the logged event.
Event Priority	Displays the priority (0-100) assigned to the event.
Facility	Displays the facility in which the appliance is located.
Description	Displays the detailed description of the event.
User name	Displays the name of the user logged in, when the event took place.

See [“About Symantec Critical System Protection”](#) on page 94.

See [“Monitor > SCSP Audit View”](#) on page 94.

See [“Filtering SCSP audit logs”](#) on page 98.

Filtering SCSP audit logs

The following procedure describes how to filter the SCSP audit logs displayed on the **SCSP Audit View** screen.

To filter SCSP audit logs

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Monitor > SCSP Audit View**.
The appliance displays the **SCSP Audit View** page. It displays the audit logs for the last 24 hours.
- 3 Click on the **Filter logs** button, to filter and view the SCSP audit logs.
The appliance displays the **Filters** dialog box.

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 using their Event Ids.	1375524
From Date From Time	Select the From and To date and time. The appliance displays the SCSP audit logs for the selected time period.	03/10/2011, 14.19.01 to 04/10/2011, 14.19.01
To DateTo Time		
Events	Select the event type from the drop-down list. The list displays the events using which the audit logs are maintained.	IDS Audit
Severities	Select the severity type of the logs to be filtered and displayed.	Critical

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

The appliance applies the filter and displays the relevant logs on the **SCSP Audit View** page. You can view the following audit log details:

Field	Description	Example
Event ID	Displays the ID for event logged.	1375524
Date and Time	Displays the date and time at which the event was logged.	03/10/2011, 14.19.01
Event Type	Displays the event type under which the event was logged.	IDS Audit
Severity	Displays the severity of the event.	Critical
Message	Displays the message to describe the event.	Process Assignment for /opt/NBUAppliance/scripts/storage_management.pl to int_rootpriv_ps. Arguments are /opt/NBUAppliance/bin/perl
Details	Displays the log details.	

Setting the audit log retention specification

When your appliance is not connected to the SCSP server, you can retain your appliance's log. The following procedure describes how to set the audit log retention on the **SCSP Audit View** page.

Note: The **Set Log Retention** button is active only if the connection to the SCSP server is inactive.

To set the audit log retention

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Monitor > SCSP Audit View**.
- 3 The appliance displays the **SCSP Audit View** page. It displays the audit logs for the last 24 hours.

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

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

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

Field	Description
Period	Select this radio button to set the log retention in number of days. 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.
Days	Enter the number of days. The appliance stores the SCSP audit logs for the specified number of days. This field is enabled, when you select the Period radio button.
Number of Logs	Select this radio button to enter the number of log files to be retained.
Size	Enter the size in Bytes up to which the audit logs are retained.

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

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

Connecting to the SCSP server

The following procedure describes how to connect to the SCSP server from the **SCSP Audit View** page.

To connect to the SCSP server

- 1 Log in to the NetBackup Appliance Web Console.
- 2 Click **Monitor > SCSP Audit View**.

The appliance displays the **SCSP Audit View** page. It displays the audit logs for the last 24 hours.

- 3 Click on the **Connect** button, to connect to the SCSP server.

The appliance displays the **Connect to SCSP Server** dialog box.

- 4 Enter a complete and valid host name / IP address of the SCSP server in the **Host Name / IP** field.
- 5 Enter the port number of the SCSP server in the **Port** field.

Note: You cannot add an SCSP 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.

- 6 Select the **Download authentication certificate from the site** radio button to download the authentication certificate from the SCSP server site.
The appliance displays certificate details.
- 7 Click on the **Accept Certificate** button, to accept the certificate.
The appliance displays the **Certificate issued** message.
OR
- 8 Select the **Provide location of an existing certificated** radio button, to enter the location of the certificate from your local folders.
- 9 Click on the **Connect** button to connect to the SCSP server.
The appliance connects to the SCSP Server and displays the following message:
Connected successfully to SCSP server.

About viewing SCSP-specific documentation

The **SCSP Audit View** page provide a link to the [SCSP documentation page](#) for additional information on SCSP features and user documentation. You can click on the **SCSP Documentation** button to view the SCSP documentation on the Symantec support website.

<http://www.symantec.com/business/support>

Managing a NetBackup appliance from the NetBackup Appliance Web Console

This chapter includes the following topics:

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

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.

[About the Manage views](#) describes the tabs included in the **Manage > Host** menu:

Table 4-1 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 108.
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 110.
Deduplication	View and change the deduplication parameters using this tab.	See "About configuring deduplication solutions" on page 113.
Advanced	Enable Bare Metal Restore (BMR) from this tab when the appliance is configured as a master server.	See "About BMR integration" on page 116.

[About the Manage views](#) describes the tabs included in the **Manage > Storage** menu:

Table 4-2 Manage > Storage

Manage	Lets you...	Topic
Partitions	View a graphical and tabular representation of the storage partitions within your appliance. You can use this tab to manage the storage partitions.	See "Manage > Storage > Partitions" on page 120.
Disks	View a tabular representation of the storage disks that comprise your appliance and the storage shelves that are attached to it. You can use this tab to manage the storage disks.	See "Manage > Storage > Disks" on page 130.

[About the Manage views](#) describes the tabs included in the **Manage > Migration Utility** menu:

Table 4-3 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 188.
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 181.
Migration Job Status	View the status and the result of all the scheduled migration jobs.	See “Migration Job Status” on page 185.

[About the Manage views](#) describes the individual following sub-menus under the **Manage** menu:

Table 4-4 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 144.
NetBackup License	Review, add, and delete license keys through the administrative Web UI.	See “Manage > License ” on page 175.
Software Updates	View and initiate an install of a software upgrade 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.	See “About software release updates” on page 192.

Table 4-4 Manage > Appliance Restore, License, Software Updates, Additional Servers *(continued)*

Manage	Lets you...	Topic
Additional Servers	<p>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.</p> <p>Note: This tab is specifically displayed for an appliance configured as a master server.</p>	See “Manage > Additional Servers” on page 218.

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 NetBackup hardware compatibility list at the following URL:</p> <p>http://symantec.com/docs/TECH76495</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 the NetBackup Key Management Service (KMS) feature.</p> <p>Note: The KMS feature is supported when the appliance is configured as a media server only in a NetBackup domain. A NetBackup master server appliance cannot administrate KMS. A non-appliance master server is required to administrate KMS with the devices that are connected to a NetBackup appliance.</p> <p>For a list of the tape drives supported with KMS, see the NetBackup hardware compatibility list at the following URL:</p> <p>http://symantec.com/docs/TECH76495</p> <p>Note: WORM tape is not currently supported.</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 Starting with appliance version 2.5, NetBackup appliances support the NetBackup type ACS libraries and the configuration of NetBackup ACS robotics on the NetBackup 52xx appliance. Appliance administrators can change the ACS entries in the `vm.conf` file on the local appliance.

For complete details about the ACS commands that can be used to modify the `vm.conf` file, see the *Symantec NetBackup Appliance Command Reference Guide*.

See [“How to determine appliance HBA WWPNs”](#) on page 315.

See [“Adding external robots to the NetBackup appliance”](#) on page 107.

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 *NetBackup Administrator's Guide, Volume I*.

See [“About appliance supported tape devices”](#) on page 106.

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 109.
- Specify Lifecycle parameters
See [“Configuring lifecycle parameters”](#) on page 113.
- Specify Deduplication parameters
See [“Configuring deduplication parameters”](#) on page 115.
- Enable or disable BMR as a server recovery option
See [“About BMR integration”](#) on page 116.

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 4-5 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.

Table 4-5 Data Buffer parameters (*continued*)

Fields	Description for the Count field
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 108.
- 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 4-6](#) describes the lifecycle parameters that are displayed.

Table 4-6 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 4-6 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 4-6 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

- Log on to the NetBackup Appliance Web Console.
- 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 110.
- 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 4-7 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 124.

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 4-8 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.
Maximum bandwidth	Enter the maximum bandwidth that is allowed for optimized duplication. The value is specified in KBytes/second.
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.

Table 4-8 Deduplication parameters (*continued*)

Fields	Description
Maximum image fragment size	Enter the maximum backup image fragment size in megabytes. Note: Change this value only when directed to do so by a Symantec representative.
Web services retry count	Enter the number of retries that can be attempted in case the Web service fails out or times out. Note: This parameter applies to the PureDisk Deduplication Option only. It does not affect NetBackup deduplication.
Web service call timeout	Enter the parameter to increase or decrease the timeout value for Web service calls made from NetBackup media servers to PureDisk storage units. Note: This parameter applies to the PureDisk Deduplication Option only. It does not affect NetBackup deduplication.
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.
Segment size	Enter the file segment size in kilobytes. The value must be a multiple of 32.
File segment exceptions	Enter the suffixes for log files. The files with these suffices 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 114.
- 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.

See [“Enabling BMR from the NetBackup Appliance Web Console”](#) on page 117.

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 117.

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**.

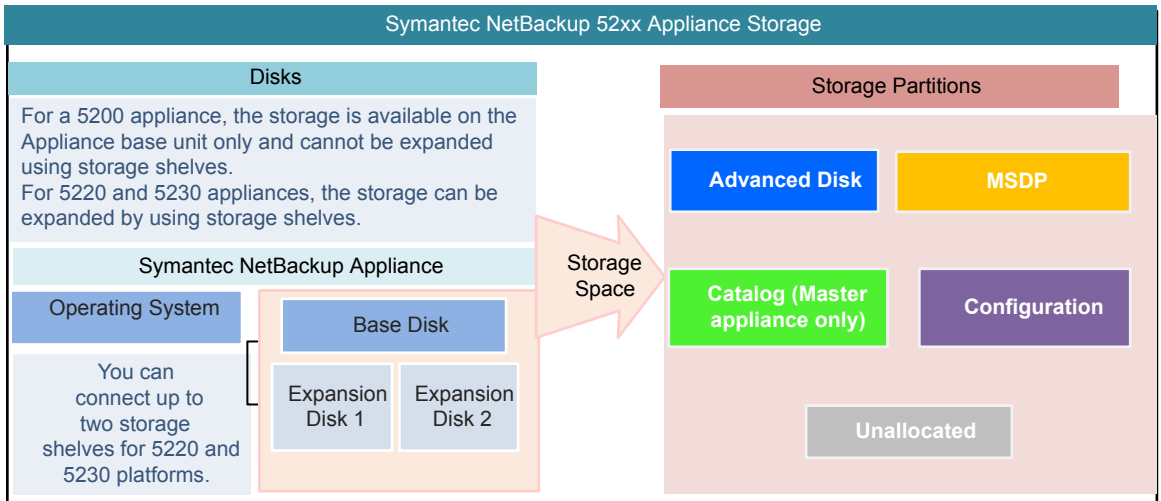
About storage configuration

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

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

[Figure 4-1](#) provides a bird's-eye view of how storage space is configured within your 52xx appliance.

Figure 4-1 NetBackup 52xx Appliance storage space



[Figure 4-2](#) lists the tasks that you can perform on the appliance storage space.

Figure 4-2 Storage operations

Storage Operations	
Tasks performed on Storage Disks	Tasks performed on Storage Partitions
<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>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>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>Move</p> <p>Moves the partition from one disk to another.</p> <p>Command - Move <Partition> <SourceDisk> <TargetDisk> [Size] [Unit]</p>
<p>Remove</p> <p>Removes disk space from the unallocated space.</p> <p>Command - Remove <Disk ID></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>Scan</p> <p>Refreshes the storage disks and devices information.</p> <p>Command - Scan</p>	<p>Show Partition</p> <p>Shows the partition's total, available, and used storage capacity.</p> <p>Command - Show Partition</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>

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

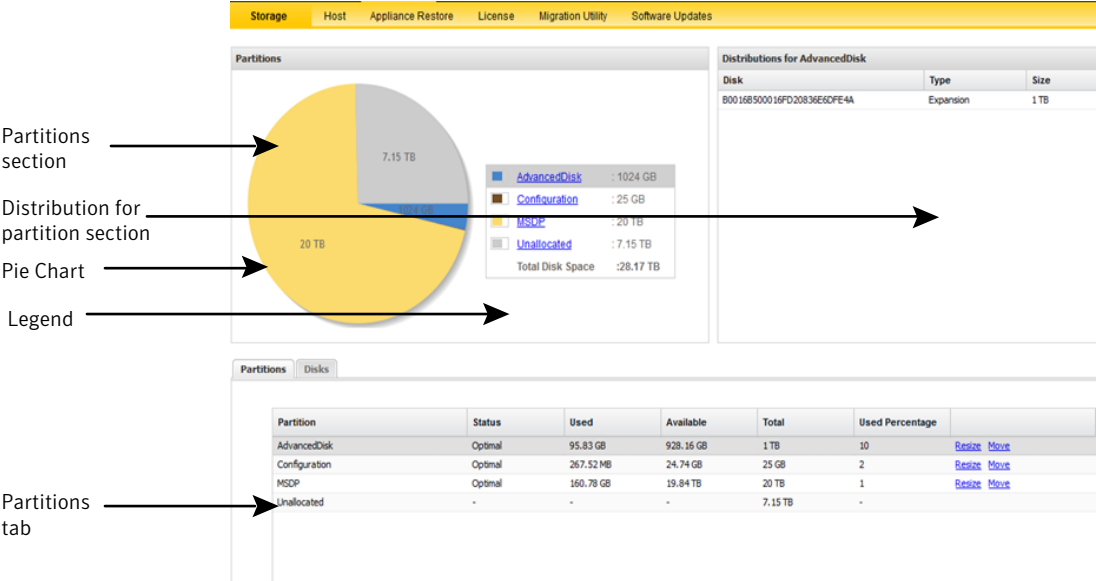
For more information about `Main > Manage > Storage` commands, refer to *NetBackup™ Appliance Command Reference Guide*.

Manage > Storage > Partitions

The Manage > Storage menu enables you to manage the storage configuration. Use the **Partition** and **Distribution for <partition>** sections to quickly view the storage configuration. You can use the **Partitions** and **Disks** tabs to manage this storage space.

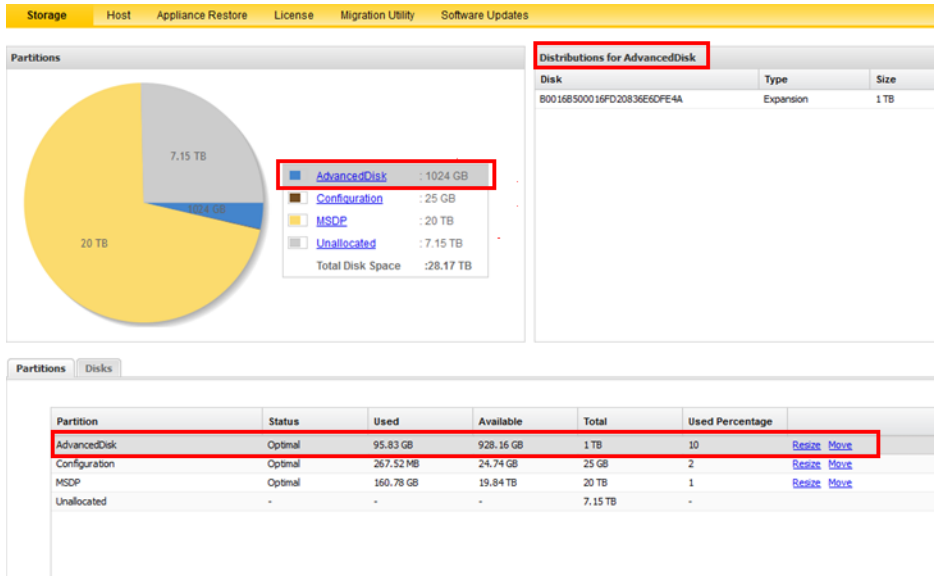
Figure 4-3 shows a sample view of **Partitions** tab for a 5230 appliance.

Figure 4-3 Partitions view for a 52xx appliance



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

When you click a partition from the legend, the specific partition is highlighted in the **Partitions** tab. Also, the **Distributions for *partition*** section displays the disks where the specific partition resides. The following figure depicts this behavior:



The **Distributions for partition** section shows the disks where a specific partition resides. It also shows the disk type and size.

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.

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

Configuration A storage partition that stores configuration information.

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

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 Catalog, AdvancedDisk, it is used from the Unallocated space.

When you add a disk, the size of the Unallocated space increases. The size of the Catalog, AdvancedDisk, and any other partition remains the same.

See the NetBackup documentation for more information on partitions.

[Table 4-9](#) lists the supported sizes and platforms for each partition.

Table 4-9 Appliance storage partitions

Partition Name	Minimum supported size	Maximum supported size	Supported Platforms
AdvancedDisk	1 GB	Maximum available capacity	5200, 5220, 5230
Catalog	250 GB (Master server)	4 TB (Master server)	5200, 5220, 5230 (master server only)
Configuration	25 GB for a 52xx appliance	500 GB	5200, 5220, 5230
MSDP	5 GB	Maximum available capacity	5200, 5220, 5230

The **Partitions** tab 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	Displays the name of the partition. Example: AdvancedDisk Table 4-9 describes each partition.
Status	Displays the status of the partition. Example: Optimal Table 4-10 describes each partition status.
Used	Displays the used space within a partition. Example: 13.70 GB
Available	Displays the free space within a partition. Example: 1.62 TB
Total	Displays the total space within the partition. Example: 1.63 TB
Used Percentage	Displays the percentage of used space in the partition. Example: 2%

Column Name	Description
Operations	Displays the applicable operations you can perform for a partition. You can resize or move a partition. Table 4-11 lists details about the resize and move operations.

[Table 4-10](#) describes the various partition status that is displayed next to the partition name.

Table 4-10 Partition Status

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

[Table 4-11](#) lists the operations that can be performed, on a partition, using the NetBackup Appliance Shell Menu and the NetBackup Appliance Web Console.

Table 4-11 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 124.</p> <p>See "Resize dialog" on page 126.</p>	<ul style="list-style-type: none"> MSDP AdvancedDisk Catalog Configuration
Move	<p>Moves the selected partition from a source disk to the destination disk.</p> <p>See "Moving a partition" on page 128.</p>	<ul style="list-style-type: none"> MSDP AdvancedDisk Configuration <p>Note: The Catalog partition cannot be moved.</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.

Note that 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. Also, 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 Catalog partitions even if the Appliance is in a factory state.

Review the following points before you resize a storage partition:

- The AdvancedDisk, Configuration, MSDP, and 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.
 See [Table 4-9](#) on page 122.

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 > Partitions**.
- 3 Go to the partition that you want to resize and click **Resize** next to it.

- 4 Enter appropriate values for the parameters on the **Resize <partition>** dialog. Click **OK** to resize the partition.

The following topic describes the parameters on Resize dialog and how you can resize each partition.

See [“Resize dialog”](#) on page 126.

An informational message like the following is also displayed when you resize an MSDP partition on master and media appliances:

Master server appliance	<p>The NetBackup processes are stopped before this operation begins, and are restarted automatically after this operation has completed.</p> <p>The NetBackup domain does not run any jobs during this time, and jobs that are currently in progress fail.</p>
Media server appliance	<p>The NetBackup processes are stopped before this operation begins, and are restarted automatically after this operation has completed.</p> <p>The media server does not run any backup jobs during this time, and jobs that are currently in progress fail.</p>

When you resize the MSDP partition to a higher or lower value, the NetBackup processes are stopped before the resize operation begins, and are restarted automatically after this operation has completed. If you resize the MSDP partition on a media server appliance, the appliance does not run any backup jobs during this time and the jobs that are currently in progress fail. If you resize the MSDP partition on a master server appliance, the NetBackup domain (all the media servers that are connected to the master server) do not perform any NetBackup operations, and any running operations fail

- 5 The progress details are displayed when you resize a partition:
Click **OK** once the operation is complete. The Manage > Storage > Partitions page is automatically refreshed.

Resize dialog

Review the following points before you resize a storage partition:

- The AdvancedDisk, Configuration, Catalog, and MSDP 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.

See [Table 4-9](#) on page 122.

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

Parameter	Description
Used Size	The Used Size is displayed when you resize AdvancedDisk, Configuration, MSDP, and 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>
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>

Parameter	Description
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 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>See Table 4-9 on page 122.</p> <p>For example, consider a Catalog partition with a Current size of 300 GB and an Unallocated Size of 6 GB. The maximum supported size for a Catalog partition is 4 TB. Since the maximum supported size for 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>

Moving a partition

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

Note: The Catalog partition cannot be moved. The Catalog partition must always be present on the base unit.

To move a partition

- 1 Log on to the NetBackup Appliance Web Console.
- 2 Click **Manage > Storage > Partitions**.
- 3 Go to the partition that you want to move and click **Move** next to it.
- 4 Enter the details on the **Move** dialog.

See [“Move <partition> dialog”](#) on page 129.

- Click **OK** to move the partition.

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

- The Move dialog displays the progress details and status of the move operation.
Click **OK** once the operation is complete. The Manage > Storage > Partitions page is automatically refreshed.

Move <partition> dialog

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

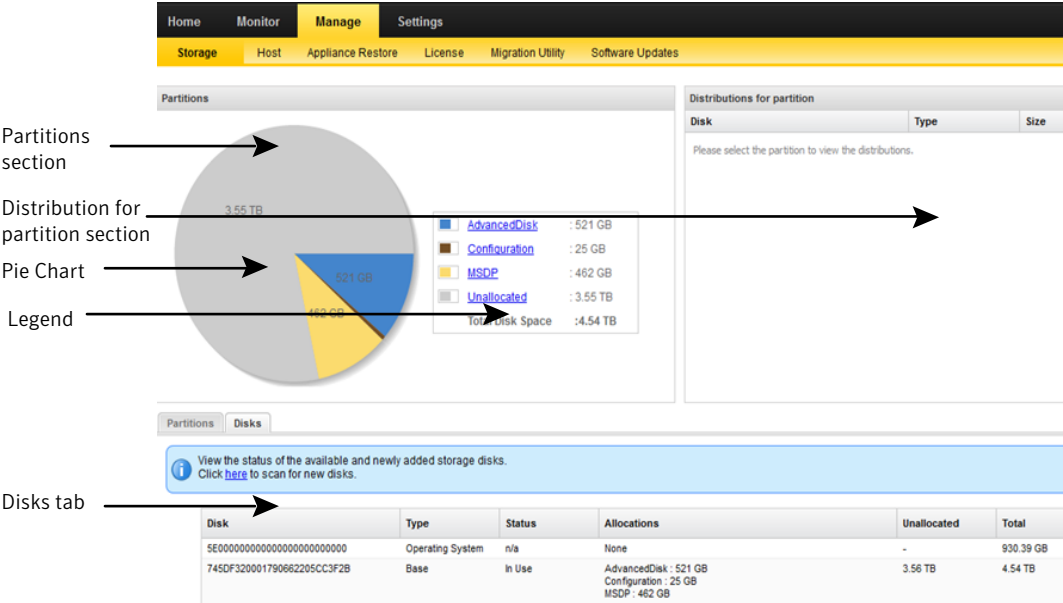
Parameter	Description	Example
Source Disk	Displays the name of disk that currently holds the selected partition.	76YTG2BA7CBACB4F416D631CE (Base)
Partition Size	Displays the selected partition's size on the source disk.	300 GB
Target Disk	Click the drop-down list and select the target disk to which you want to move the partition. Note: The Target disk must be different from the Source disk.	9DB0FD2BA7CBACB4F416D631CE(Base)
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

Manage > Storage > Disks

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

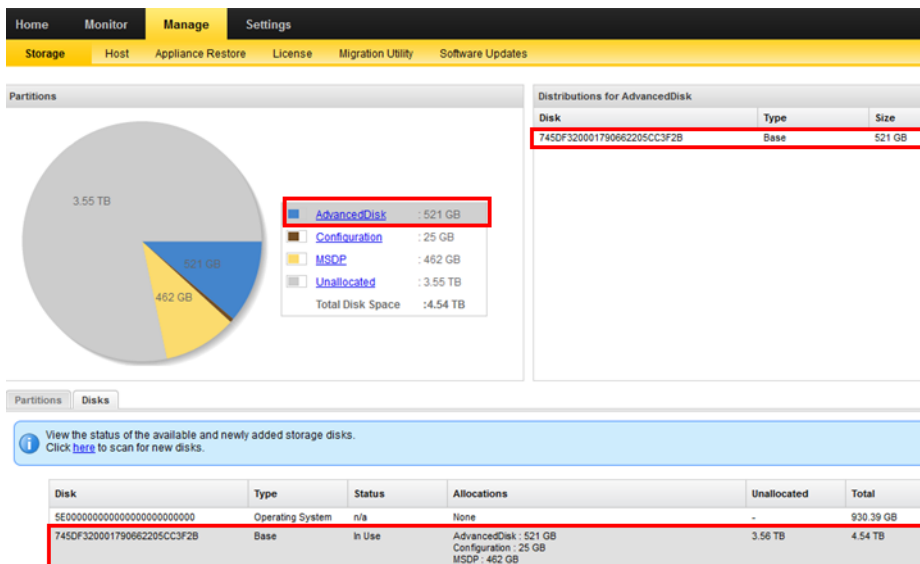
Figure 4-3 shows a sample view of **Disks** tab for a 52xx appliance.

Figure 4-4 Disks view for a 52xx appliance



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

When you click a partition from the legend, the **Distributions for partition** section displays the disks where the specific partition resides. If you do a mouseover on the disk in the **Distributions for partition** section, the corresponding disks are highlighted in the **Disks** tab. The following figure depicts this behavior:



The following text appears on **Disks** tab:

View status of the available and newly added storage disks.
 Click **here** to scan for new disks.

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

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.

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 and Initial Configuration 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** tab. 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 a new disk” on page 134.

The following columns are displayed in the table:

Column names	Description
Disk	Displays the ID that is associated with the disk. Example: 50001FAFA000000F5B0519CB4

Column names	Description
Type	<p>Displays the type of disk.</p> <p>Example: Base</p> <p>Table 4-12 describes each disk type.</p>
Status	<p>Displays the status of the disk.</p> <p>Example: In Use</p> <p>Table 4-13 describes each status.</p>
Allocations	<p>Lists the partitions that exist on each disk. Also lists the size of each partition.</p> <p>Example: AdvancedDisk: 18 TB</p>
Unallocated	<p>Displays the available space within the disks that has not been allocated.</p> <p>Example: 1.9172 GB</p>
Total	<p>Displays the total storage space within the disk.</p> <p>Example: 4.5429 TB</p>

[Table 4-12](#) lists the disk types that can appear depending on your Appliance platform.

Table 4-12 Disk Type

Type	Description	Supported Platforms
Operating system	This category tells you the storage that is occupied by the Appliance operating system.	5200, 5220, 5230
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
Unknown	This category appears when appliance cannot determine the disk type like when the disk is not accessible.	Not Applicable

[Table 4-13](#) describes the various status that is displayed in the **Status** field.

Table 4-13 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	Denotes that no commands or operations can be performed on disks with this status. An example of a disk that has n/a status is operating system
New Available	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.
Not Accessible	Storage disk that was In Use is not accessible any more.

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.

See [“Gathering device logs with the Datacollect command”](#) on page 256.

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 and Initial Configuration 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** tab. 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 the **Click here to scan for new disks** link.
- 4 You are prompted for confirmation. Click **Yes** to confirm. The scan starts.
- 5 When the scan is complete, click **OK**. The **Disks** tab refreshes automatically. If a new storage shelf is detected, a new disk ID appears in the **Disks** tab.

The new entry should have the following attributes:

- Type = Expansion
- Status = New Available

You can now add this disk to the Unallocated space.

See [“Adding a new disk”](#) on page 134.

Adding a new disk

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

If you want to attach a Storage Shelf or an expansion system to an appliance, see the *Symantec NetBackup Appliance Hardware Installation and Initial Configuration 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** tab. 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 a new disk

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

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.

The appliance scans all the connected devices and displays the following output:

```
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.

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

- `Show [ALL]` - to view Disk, Partition, and Distribution information together. See [“Viewing all storage information”](#) on page 139.
- `Show [Disk]` - to view total capacity, unallocated storage capacity, and current status of a disk. See [“Viewing disk information”](#) on page 140.
- `Show [Partition]` - to view total, available, and used storage capacity of a partition. See [“Viewing partition information”](#) on page 142.

- `Show [Distribution]` - to view the distribution of partitions on a disk.
See [“Viewing the partition distribution on disks”](#) on page 142.

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 5230 platform, the appliance displays the storage information as shown in the following example.

```
Storage> Show All
```

Disk ID	Type	Total	Unallocated	Status
SE000000000000000000se	Operating System	150 GB	-	n/a
S0001FB3BC00A00000009se	Base	550 GB	33.968 GB	In Use

```
S0001FB3BC00A00000009se (Base)
```

AdvancedDisk	: 20 GB
Catalog	: 350 GB
Configuration	: 50 GB

Partition	Total	Available	Used	%Used	Status
AdvancedDisk	20 GB	19.778 GB	227.31 MB	2	Optimal
Catalog	350 GB	49.196 GB	822.58 GB	2	Optimal
Configuration	50 GB	25 GB	25 GB	50	Optimal
MSDP	0 GB	0 GB	0 GB	0	Not Configured
Unallocated	130 GB	-	-	-	-

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

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
```

```
-----
Disk ID          |      Type          |   Total   | Unallocated | Status
-----
SE000000000000se | Operating System | 930.39 TB |      -      | n/a
S0001FB35CC3F2B | Base              |   2.24 TB |   300 GB    | In Use
S00ABDD0000001s  | Expansion         | 4.5421 TB | 840.92 GB   | In Use
```

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

[Table 4-14](#) lists the disk types that can appear depending on your Appliance platform.

Table 4-14 Disk Type

Type	Description	Supported Platforms
Operating system	This category tells you the storage that is occupied by the Appliance operating system.	5200, 5220, 5230
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
Unknown	This category appears when appliance cannot determine the disk type like when the disk is not accessible.	Not Applicable

Viewing partition information

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

To view partition information

- Log on to the NetBackup Appliance Shell Menu.
- 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.

- Enter the `Show Partition` command to view partition information.

For 52xx platforms, the appliance displays the partition information as shown in the following example:

```
Storage> Show Partition
```

Partition	Total	Available	Used	%Used	Status
AdvancedDisk	1 TB	1001.1 GB	22.876 GB	3	Optimal
MSDP	3.6343 TB	3.4868 TB	151.04 GB	4	Optimal
Configuration	150 GB	25 GB	125 GB	83.3%	Optimal
Unallocated	53.683 TB	-	-	-	-

Note that the partition information that is displayed depends on the hardware platform.

The Catalog partition is not supported if Appliance is configured in a media server role.

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

```
Storage> Show Distribution
```

```
S0001FB3BC00000A62501ABDA0000009se (Base)
```

```
-----
```

```
AdvancedDisk : 744 GB
```

```
Catalog : 930.38 GB
```

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:

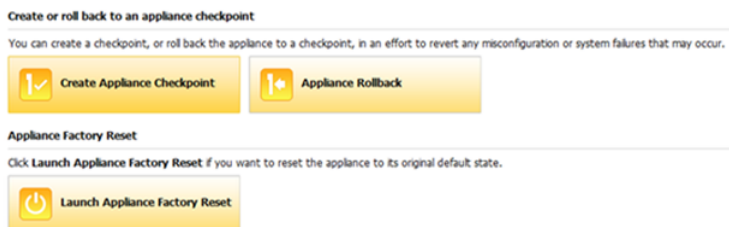
Alerts from NetBackup Appliance

```
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

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.


Create appliance checkpoint

Existing appliance restore checkpoints







Pre-upgrade checkpoint
Wed Mar 20 11:27:32 2013

Post-upgrade checkpoint
Wed Mar 20 11:27:32 2013

User-directed checkpoint
Wed Mar 20 11:27:32 2013

 Creating a user-directed checkpoint will replace this checkpoint.

The following components of the appliance will be included in the checkpoint

-  The appliance operating system
-  The appliance software
-  The NetBackup software
-  The network configuration
-  Any previously applied software updates
-  The backup data is **not** included in the checkpoint

Create appliance checkpoint

Provide a description for the new appliance checkpoint you are about to create.

See [“About creating an appliance checkpoint”](#) on page 146.

See [“Creating an appliance checkpoint”](#) on page 149.

See [“Rollback an appliance ”](#) on page 155.


See [“Appliance factory reset”](#) on page 163.

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.


Create appliance checkpoint

Existing appliance restore checkpoints




No appliance restore checkpoint currently exists. Create an appliance checkpoint to revert to the current state of the appliance.


The following components of the appliance will be included in the checkpoint




The appliance operating system




The appliance software




The NetBackup software



The network configuration



Any previously applied software updates



The backup data is **not** included in the checkpoint

Create appliance checkpoint

Provide a description for the new appliance checkpoint you are about to create.

Validate

Create

Cancel

[Table 4-15](#) contains the following fields and functions that you use to create a checkpoint.

Table 4-15 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 NetBackup catalog on the master server appliance is not included. ■ The backup data is not included.

Table 4-15 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 <i>Create</i> 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 <i>here</i> 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 149.

See [“Checkpoint creation status”](#) on page 152.

See [“Creating an appliance checkpoint from the appliance shell menu”](#) on page 153.

See [“Manage > Appliance Restore”](#) on page 144.

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.

Create appliance checkpoint

Existing appliance restore checkpoints

Pre-upgrade checkpoint


Wed Mar 20 11:27:32 2013

Post-upgrade checkpoint


Wed Mar 20 11:27:32 2013


User-directed checkpoint


Wed Mar 20 11:27:32 2013



 Creating a user-directed checkpoint will replace this checkpoint.


The following components of the appliance will be included in the checkpoint


 The appliance operating system

 The appliance software

 The NetBackup software

 The network configuration

 Any previously applied software updates

 The backup data is **not** included in the checkpoint

Create appliance checkpoint

Provide a description for the new appliance checkpoint you are about to create.

Validate

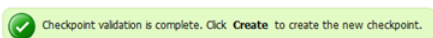
Create

Cancel

- 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**.

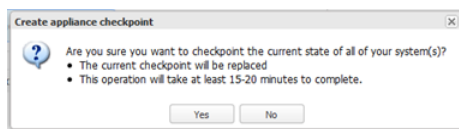
A window appears and shows a validation check is in progress. The validate process ensures that all of the media servers are up and running. A status message appears on the page letting you know whether the checkpoint validation is complete and successful. If the validation is successful and you want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

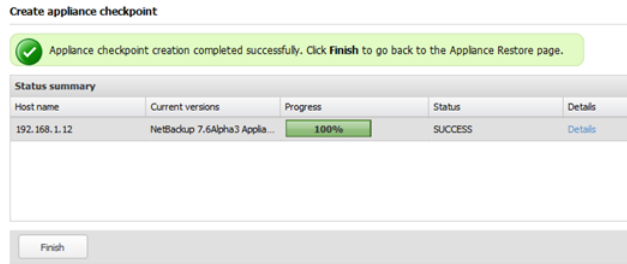
i Appliance checkpoint creation in progress. This process may take at least 15-20 minutes to complete.

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: #FFD700; border: 1px solid #FFD700;"></div> 5%	ACTIVE	Details

See “[Checkpoint creation status](#)” on page 152.

- 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 146.

See “[Manage > Appliance Restore](#)” on page 144.

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 4-16 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 149.

See “[About creating an appliance checkpoint](#)” on page 146.

See “[Manage > Appliance Restore](#)” on page 144.

Creating an appliance checkpoint from the appliance shell menu

Use the following procedure to create a user-directed checkpoint from the appliance shell menu.

Note: If a user-directed checkpoint already exists, the checkpoint that you are about to create replaces the existing checkpoint. Only one user-directed checkpoint can exist at any given time.

To create a new checkpoint from the appliance shell menu

- 1 Log on to the appliance as an administrator and open the appliance shell menu.
- 2 Enter the following command to

```
Main_Menu > Support > Checkpoint Create
```

The following interactive process begins. The shell menu informs you of any existing checkpoints before you can create a new checkpoint. In the following example, no existing checkpoints exist.

Creating an Appliance Checkpoint allows the user to easily rollback the entire system back to a point-in-time to undo any misconfiguration or system failure that might have occurred. An Appliance Checkpoint captures the following components:

- 1) Appliance Operating System
- 2) Appliance Software
- 3) NetBackup Software
- 4) Tape media configuration on the master server
- 5) Networking Configuration
- 6) LDAP configuration if any exists
- 7) Fibre channel configuration
- 8) Any previously applied patches
- 9) NetBackup catalog on the master server is not included
- 10) Backup data is not included

```
There are no checkpoints in the system. Please continue to create
a user checkpoint
>> Would you like to proceed? (yes/no) yes
```

- 3 Enter **Yes** to proceed with the creation of the new checkpoint.

4 Enter a description for your checkpoint. That is an optional field.

5 Enter **Yes** to begin the Create checkpoint process.

```
- [Info] Deleting checkpoint: USER
- [Info] CREATING USER CHECKPOINT
- [Info] Creating checkpoint. This operation can take 10 to
    15 minutes.
```

```
Please wait...
```

```
- [Info] Appliance Checkpoint creation was successful
```

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 152.

See [“About creating an appliance checkpoint”](#) on page 146.

See [“Manage > Appliance Restore”](#) on page 144.

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 the NetBackup Appliance Web Console and not the appliance shell menu.

See [“Rollback an appliance”](#) on page 155.

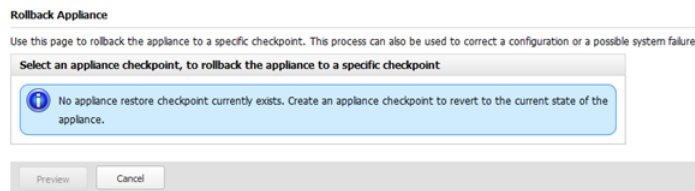
See [“Rollback appliance validation”](#) on page 157.

See [“Checkpoint rollback status”](#) on page 161.

Rollback an appliance

You can roll back your appliance to an existing restore checkpoint from the NetBackup Appliance Web Console or the 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 from the NetBackup Appliance Web Console you should 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.

Rollback Appliance

Use this page to rollback the appliance to a specific checkpoint. This process can also be used to correct a configuration or a possible system failure.

Select an appliance checkpoint, to rollback the appliance to a specific checkpoint

☐ Pre-upgrade checkpoint

Wed Mar 20 11:27:32 2013

☐ Post-upgrade checkpoint

Wed Mar 20 11:27:32 2013

☒ User-directed checkpoint

Thu Mar 21 11:06:22 2013

test

Select the additional actions to be performed during the appliance rollback process

☐ Restart Host(s) automatically after rollback

Version information

Host name	Current versions	Versions after rollback
192.168.1.12	NetBackup 7.6 Appliance 2.6	NetBackup 7.5 Appliance 2.5.2

Preview

Cancel

Table 4-17 contains the following fields and functions:

Table 4-17 Rollback Appliance page

Field	Description
Select an appliance checkpoint, to rollback the appliance to a specific checkpoint	<div>This field shows the available checkpoints that you can use to revert your appliance. The available checkpoints can be:</div> <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	<div>You can elect to automatically restart the appliances after the rollback operation completes.</div>

Table 4-17 Rollback Appliance page (*continued*)

Field	Description
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 The IP address of the master or media server appliance. ■ Current versions The NetBackup and appliance software versions currently installed before the rollback operations begins. ■ Versions after rollback The NetBackup and appliance software versions that are installed after the rollback operation succeeds.
Action icons	<p>The Preview icon provides you with the ability to preview the appliance(s) to ensure that they are up and running so that a rollback operation can proceed. If an appliance is not up and running, a message appears that identifies the appliance, so that you can make any necessary adjustments.</p> <p>The Cancel icon cancels the rollback operation.</p>

See [“Rollback appliance validation”](#) on page 157.

See [“Checkpoint rollback status”](#) on page 161.

Rollback appliance 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 NetBackup catalog on the master server appliance is not included.
- 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 [“Rollback an appliance”](#) on page 155.

See [“Checkpoint rollback status”](#) on page 161.

See [“Rollback an appliance”](#) on page 155.

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 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.

Rollback Appliance - User-directed checkpoint

The following components of the appliance will be rolled back

- The appliance operating system
- The appliance software
- The NetBackup software
- The network configuration
- Any previously applied patches
- The backup data is not rolled back

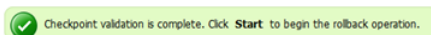
Version information

Host name	Current versions	Versions after rollback
192.168.1.12	NetBackup 7.6 Appliance 2.6	NetBackup 7.5 Appliance 2.5.2

Back Validate Start Cancel

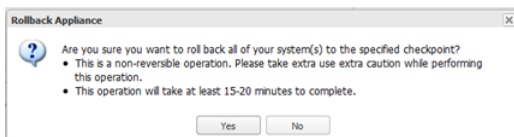
6 Click **Validate**.

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.



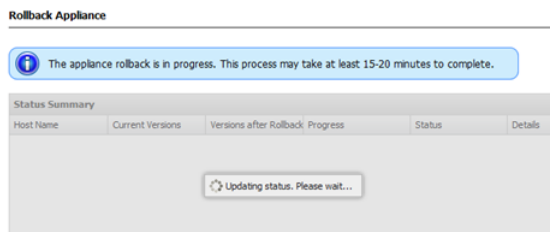
If the checkpoint validation was unsuccessful, you are not able to start the rollback operation. A link is provided that you can select to view more information about the cause of the issue. You can then, correct that issue, and click **Validate**. If the validation is successful, click **Start**.

- 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 161.

See [“Manage > Appliance Restore”](#) on page 144.

Checkpoint rollback status

When you begin the checkpoint Rollback process each system is rolled back at the same time to ensure that all systems are at the same software version level. Each of the systems is listed in the **Checkpoint Rollback status** table. This table provides the following information about each system.

Table 4-18 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.
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.

This page also displays the steps of the revert process once a rollback has been started. The field titled, **Following steps will be performed**, shows the appliance name(s) that must be rolled back to a checkpoint and then restarted.

See [“Rollback appliance validation”](#) on page 157.

See [“Rollback an appliance ”](#) on page 155.

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 to

```
Main_Menu > Support > Checkpoint Rollback
```

The following interactive process begins. The shell menu informs you of the components that are reverted during this process. It also lists all of the existing checkpoints.

Rolling back to an Appliance Checkpoint will restore the system back to the checkpoint's point-in-time. This can help undo any misconfiguration or system failures that might have occurred.

Rolling back to an Appliance Checkpoint will revert the following components:

- 1) Appliance Operating System
- 2) Appliance Software
- 3) NetBackup Software
- 4) Networking Configuration
- 5) Any previously applied patches
- 6) Backup data is not reverted

The existing Appliance Checkpoints in the system are:

```
-----
(1) Checkpoint Name: User directed checkpoint
Date Created: Fri Oct 5 09:27:32 2012
Description: User checkpoint after configuring network
-----
```

Please enter the checkpoint to rollback to (Available options: 1 only):

- 3 Enter the number of the checkpoint that you want to use for the Rollback operation.

- 4 Enter **Yes**, if you want to automatically restart all appliances after the rollback completes.

A reboot of the appliance is required to complete the checkpoint rollback. Reboot automatically after rollback (yes/no)?

Automatically rebooting the appliance after the rollback will not provide you with an opportunity to review the progress/final status of the rollback. Are you sure you would like to automatically reboot the appliance (yes/no) yes

- 5 Enter **Yes** a second time to confirm that you want to restart the appliance automatically after the rollback operation completes.

- 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 152.

See [“About creating an appliance checkpoint”](#) on page 146.

See [“Manage > Appliance Restore”](#) on page 144.

Appliance factory reset

The purpose of an appliance factory reset is to return your appliance to a clean, unconfigured, and default state. The same state in which you receive the appliance. 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 and back up data if any currently exists. In addition, you can elect to restart the host appliance or appliances after the reset completes.

From the **Manage > Restore** page on the NetBackup Appliance Web Console you can select **Appliance Factory Reset** to begin the reset process. Symantec recommends that you record your network configuration information before you begin a factory reset. After the reset operation completes the appliance is restarted, either automatically or manually and you may need that 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

☐ 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.

The **Select the additional actions to be performed during the factory reset process** field 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.
 - If you are on a single master server appliance, the catalog, and EMM database is removed.
- **Restart host(s) automatically after reset**
Select this option if you want to have the appliance restarted automatically after the factory reset completes.

[Table 4-19](#) describes the remaining fields that are contained in the **Appliance Factory Reset** page.

Table 4-19 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 <p>Note: Because the network configuration is reset during this procedure and the appliance(s) are restarted, you must log on to the appliance through the remote management port to reconfigure the appliance for reuse.</p> <p>See “Starting a factory reset from the NetBackup Appliance Web Console” on page 167.</p> <ul style="list-style-type: none"> ■ 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"> ■ Validate - Initiate a validation process to determine whether the appliances are in a running state and factory checkpoints exist. ■ 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"> ■ Host name - Shows the IP address of the appliance(s) that are about to be reset. ■ 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.

See [“Starting a factory reset from the NetBackup Appliance Web Console”](#) on page 167.

See [“Factory reset status”](#) on page 170.

See [“Manage > Appliance Restore”](#) on page 144.

About factory reset best practices

This topic contains best-practice information about a factory reset operation that you should know.

- Factory reset is not supported if you have upgraded a 52xx master server or media server to version 2.6. If you want the latest version of the appliance software on your appliance you can install the latest software version from the USB flash drive. Contact Symantec Technical Support for the latest version of the appliance software.
- 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.
- 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 2.6 Troubleshooting Guide* for more information.

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 is not supported if you have upgraded a 52xx master server or media server to version 2.6. If you want the latest version of the appliance software on your appliance you can install the latest software version from the USB flash drive. Contact Symantec Technical Support for the latest version of the appliance software.

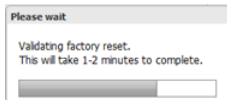
Note: A factory reset operation returns the password to the original, default value.

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 your storage configuration. If you do, check the **Retain storage configuration and backup data** check box.
- 4 Determine if you want to restart the appliance automatically after the reset operation completes. If you do, check the **Restart appliance automatically after reset** check box.
- 5 Click **Validate**.

The screenshot shows the 'Appliance Factory Reset' web console interface. At the top, it says 'Appliance Factory Reset'. Below that, it prompts the user to 'Select the additional actions to be performed during the factory reset process'. There are two checkboxes: 'Retain storage configuration and backup data' and 'Restart Host(s) automatically after reset'. Below the checkboxes, a box titled 'A factory reset operation resets the entire system, that includes the following actions' lists six items: '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', and 'Resets the storage configuration and backup data'. Below this list, a yellow warning box states: '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.' At the bottom, there are three buttons: 'Validate', 'Start', and 'Cancel'.

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

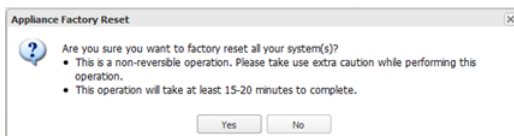


The following results can occur from the validation operation:

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



- 6 Click **Start**.
- 7 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.

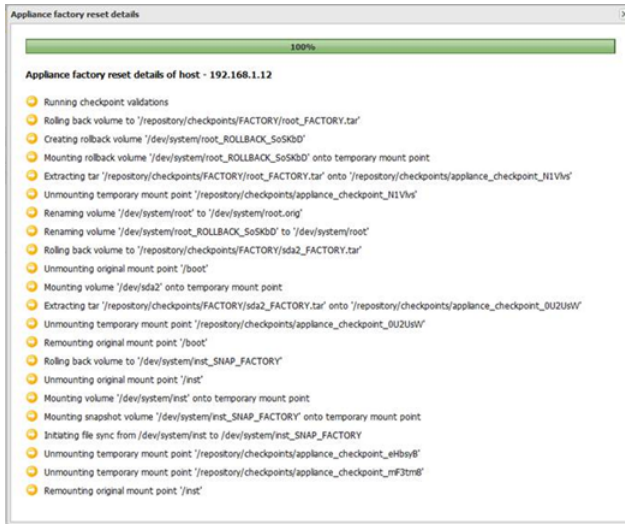
Note: Once you begin the factory reset, you cannot perform any other functions on the NetBackup Appliance Web Console until the operation completes.

- 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 “Factory reset status” on page 170.

- After the reset operation completes the storage reset operation begins if you elected to retain your storage configuration and backup data at the beginning if this procedure.

Appliance Factory Reset

Storage reset completed.

Status Summary					
Host Name	Current Versions	Versions after Reset	Progress	Status	Details
192.168.1.13	NetBackup 7.6Beta...	NetBackup 7.6Beta...		SUCCESS	Details
192.168.1.12	NetBackup 7.6Beta...	NetBackup 7.6Beta...		SUCCESS	Details

- 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.

- 10 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 [“Appliance factory reset”](#) on page 163.

See [“Starting a factory reset from the appliance shell menu”](#) on page 171.

See [“Factory reset status”](#) on page 170.

Factory reset status

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

Table 4-20

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 .

Table 4-20 (continued)

Field name	Description
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 “[Appliance factory reset](#)” on page 163.

See “[Manage > Appliance Restore](#)” on page 144.

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 is not supported if you have upgraded a 52xx master server or media server to version 2.6. If you want the latest version of the appliance software on your appliance you can install the latest software version from the USB flash drive. Contact Symantec Technical Support for the latest version of the appliance software.

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

To begin a factory reset from the appliance shell menu

- 1 Log on to the appliance as an administrator and open the appliance shell menu.
- 2 Enter `Main_Menu > Support > FactoryReset`. This command shows the following messages and requires you to answer the following questions before the factory reset begins.

Appliance Factory Reset will reset the entire system to the factory installed image. The following components will be 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
- 6) Storage configuration and backup data (optionally retain)

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

```
- [Info] Factory reset validation successful.
```

```
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)? yes
```

- 3 After you respond to these questions, the following summary information is shown:

FACTORY RESET SUMMARY

```
-----
Reset Appliance OS, software configuration      : [YES]
Reset Appliance storage configuration (REMOVE DATA) : [YES]
Auto reboot after reset?                       : [YES]
```

Appliance Factory Reset will make the following version changes:

+-----+		
Appliance	Current Version	Reverted Version
+-----+		
appl.symantec.com	NetBackup 7.6	NetBackup 7.6
	Appliance 2.6	Appliance 2.6
+-----+		
app2.symantec.com	NetBackup 7.6	NetBackup 7.6
	Appliance 2.6	Appliance 2.6
+-----+		

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 [“Appliance factory reset”](#) on page 163.

See [“Starting a factory reset from the NetBackup Appliance Web Console”](#) on page 167.

See [“Factory reset status”](#) on page 170.

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 176.

See [“Adding a permanent license key if an evaluation license key expires”](#) on page 177.

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 view, 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** fields for the option that you want to install.
- 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 175.

See [“Managing license keys on the NetBackup appliance”](#) on page 176.

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 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:
 - 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

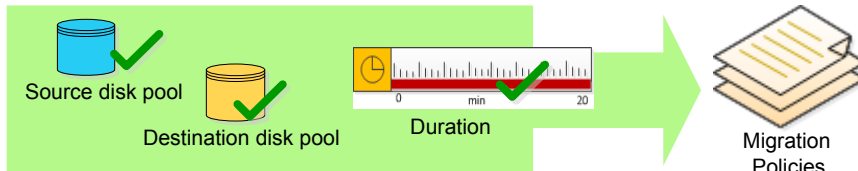
The following diagram provides a brief overview of the Migration Utility feature:

How does the Migration Utility work?

1. From the **Selection Criteria** screen, identify the following, and click **Apply Search**:



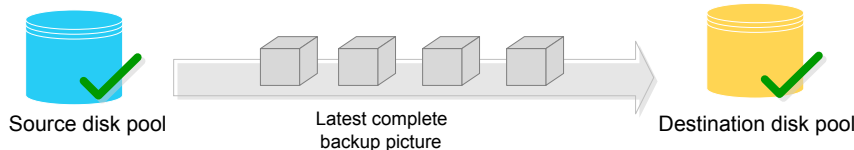
2. Using the selections from step 1. Migration Utility identifies the policy/client backup picture candidates. This allows migration to place limits on the amount of NetBackup catalog data to be searched.



3. From the Selection Criteria screen, select the migration Policies and schedule the migration :



4. The backup picture (and deduplication history) is transferred using the selected policy.



5. From the **Migration Job Status** screen monitor the Migration and optional policy conversion results. The utility monitors, estimates, and displays the transfer time. You can refine the estimates by identifying how much data can be migrated within the specified migration window duration.

Home	Monitor	Manage	Settings
Host	Storage	Appliance Features	License
		Migration Utility	Software Updates
			Additional Services

Policy Conversion	Selection Criteria	Migration Job Status
Migration Job ID	Status	Start Time
0	Running	06:13
		Planned Duration (min)
		Actual Duration (min)
		Images Copied
		Outcome
		Job Details

```

Job Details
DP - Source copy 1 of backup of resident_130299005, is not required copy 1.
DP - Destination storage unit dpa_m_130299005 is not required.
DP - Destination policy requires schedule resident_130299005 backup of resident_130299005 copy 1 created on 11/10/2012
DP - Duplicate of backup resident_130299005 successful.
DP - Duplicate of backup resident_130299005 successful.
DP - Destination policy requires schedule resident_130299005 backup of resident_130299005 copy 1 created on 11/10/2012
DP - Duplicate of backup resident_130299005 successful.
DP - Destination policy requires schedule resident_130299005 backup of resident_130299005 copy 1 created on 11/10/2012
DP - Duplicate of backup resident_130299005 successful.
DP - Destination policy requires schedule resident_130299005 backup of resident_130299005 copy 1 created on 11/10/2012
DP - Duplicate of backup resident_130299005 successful.
DP - Destination policy requires schedule resident_130299005 backup of resident_130299005 copy 1 created on 11/10/2012
DP - Duplicate of backup resident_130299005 successful.
DP - Status = successfully duplicated 5 of 6 images.
Migration transfer rate was 0.00 MB/sec.
    
```

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 181.

See [“Selecting the search criteria and scheduling the migration job”](#) on page 184.

See [“Policy Conversion”](#) on page 188.

See [“Setting-up a policy conversion map”](#) on page 190.

See [“Migration Job Status”](#) on page 185.

See [“Viewing migration job status and details”](#) on page 188.

See [“Best practices to run a migration job”](#) on page 191.

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 4-21](#) 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 4-21 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 4-21 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 4-22](#) 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 4-22 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 4-22 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 185.
 - **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 188.
- See [“Selecting the search criteria and scheduling the migration job”](#) on page 184.
- See [“About the Migration Utility”](#) on page 179.
- See [“Best practices to run a migration job”](#) on page 191.

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 181.

See “[About the Migration Utility](#)” on page 179.

See “[Best practices to run a migration job](#)” on page 191.

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 4-23](#) describes the status and the result conditions that are reported.

Table 4-23 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 4-23 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 188.

See [“Selection Criteria”](#) on page 181.

See [“Policy Conversion”](#) on page 188.

See [“About the Migration Utility”](#) on page 179.

See [“Best practices to run a migration job”](#) on page 191.

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 185.

See [“About the Migration Utility”](#) on page 179.

See [“Best practices to run a migration job”](#) on page 191.

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 4-24](#) describes the information you must enter to **Select Policy Conversion map** section.

Table 4-24 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 4-25](#) describes the information you must enter to change the source disk pools and the destination disk pools.

Table 4-25 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 4-25 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 190.

See [“Selection Criteria”](#) on page 181.

See [“Migration Job Status”](#) on page 185.

See [“About the Migration Utility”](#) on page 179.

See [“Best practices to run a migration job”](#) on page 191.

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 188.

See [“About the Migration Utility”](#) on page 179.

See [“Best practices to run a migration job”](#) on page 191.

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 181.

See [“About the Migration Utility”](#) on page 179.

See [“Policy Conversion”](#) on page 188.

See [“Migration Job Status”](#) on page 185.

About software release updates

Symantec provides bundled, release-update packages for the appliance that you can download from the Symantec Support website. Through the NetBackup Appliance Web Console or the NetBackup Appliance Shell Menu, you can check the Symantec Support website and determine if an update is available.

The bundled packages can include updates for the following appliance software applications:

- Linux operating system
- NetBackup server and client
- NetBackup Appliance Web Console

When you prepare to upgrade the software on your appliance, you should plan for a period of downtime for your appliance. The upgrade process provides an estimate on how long the process takes to complete. You are given the choice to proceed

with the upgrade, or schedule the upgrade for a different time so that you can continue your work.

Appliance upgrades should follow the same order as traditional NetBackup upgrades. The master server appliance should be updated first, then the media server appliances can be upgraded. 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 your media server appliance with the NetBackup Appliance version 2.6, Symantec recommends that you first upgrade the NetBackup master server to version 7.6.

The upgrade process takes the necessary steps to make sure that your upgrade completes successfully. It first determines if the available update is newer than the version of software that you currently have installed. It then determines if there is enough available space on your appliance to install the release update.

To help make sure that the upgrade is successful, the upgrade mechanism is designed to stop processes. The upgrade process checks to see if there are any active NetBackup jobs. The upgrade process only proceeds if it is determined that no active jobs are detected.

After a successful upgrade, the appliance version is updated to the latest release update level.

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 (`app_debug.log`) and the administrator is notified. If additional assistance is required, contact Symantec Technical Support.

From the NetBackup Appliance Web Console, you can select **Manage > Software Updates** to view which software updates are available to download and install. From the NetBackup Appliance Shell Menu you can use the following commands to view the detailed list of software information, see which update is currently installed, and see the current version of the appliance:

- `Main_Menu > Manage > Software > List Details`
Use this command to see a detailed list of all of the installed RPMs or a detailed list of all of the factory-installed RPMs.
- `Main_Menu > Manage > Software > List Downloaded`
This command shows a list of the downloaded software updates.
- `Main_Menu > Manage > Software > List EEBs`
This command shows a list of EEBs that are installed on the appliance.
- `Main_Menu > Manage > Software > List Version`

This command shows the current version of your appliance and of NetBackup.
 See “[Manage > Software Updates](#)” on page 194.

Manage > Software Updates

Use the **Manage > Software Updates** tab to view and initiate the installation of a software upgrade on your appliance.

This page shows the following software update information:

- **Downloaded software updates**
 Identifies the software updates that have been downloaded to the appliance and can be selected to install.
- **Online software updates**
 Identifies the software updates that are available for you to download to the appliance.

The following tables describe the information that appears on this page.

Table 4-26 Downloaded Software Updates

Field name	Description
Available Software Update Name	Shows the name and the version of the appliance software updates that are available for you to select and install.
NetBackup Version	Shows the version of NetBackup software that is included with that version of the appliance software update.
Software Update Size	Shows the size of the software update to help ensure that you have enough space on your appliance to accommodate the installation.
Details	Click Details to view additional information about the software update.

Table 4-26 Downloaded Software Updates (*continued*)

Field name	Description
Install	<p>After you have selected a software update to install, click Install to start the upgrade process.</p> <p>After you click Install, some software updates may present pre-installation popup windows with questions related to changes from the selected software update. The following describes how to proceed:</p> <ul style="list-style-type: none"> ■ Answer the question that appears in each popup window. After all questions are answered, the server upgrade list appears 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.

On the **Manage > Software Updates** tab, the **Online Software Updates** table remains visible throughout the upgrade process. It shows the available software updates that are applicable to your appliance that you can download.

Table 4-27 Online Software Updates

Field name	Description
Online Software Update Name	This column displays the version of the appliance software update that you can select to download to your appliance.
Software Update 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	After you have selected a software update version, click Download to start the download process.

See [“Media servers to upgrade”](#) on page 208.

See [“Software Updates > Status”](#) on page 209.

See [“Upgrading an appliance using the NetBackup Appliance Web Console”](#) on page 196.

See [“Upgrading an appliance using the NetBackup Appliance Shell Menu”](#) on page 200.

See [“About software release updates”](#) on page 192.

Upgrading an appliance using the 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 following items that pertain to the 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. The last step in the following procedure describes how to rescan the FC ports, after the upgrade has been completed.
- 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
```

- According to the requirement from the software update, the system may restart during the upgrade process. While the system restarts, 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.
- If you plan to upgrade more than one media server, you must perform the upgrade procedure on each media server.

To upgrade your appliance using the NetBackup Appliance Web Console

- 1 Log on to your 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 **Software updates available** 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 Available** table on the page, select a software update and click **Download**.
 During the download operation, the status of **Downloading** is displayed. After the download process completes successfully, the software update status changes to **Finish**. Click **Finish**. The software update appears in the **Software updates available** table. Proceed to Step 4.

- 4 Select the check box that is associated with the software update that you want to install and click **Install**.

The following occurs after you click **Install**:

- An interactive, pre-upgrade checklist window appears.
- You must provide answers to the pre-upgrade questions. Then select to continue with the upgrade process.
- 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 current version of the server (master or media).

Note: If you plan to upgrade more than one media server, you must run this upgrade procedure on each media server

- 5 Click **Next**.
- 6 The **Confirm** pop-up window appears. That 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 The **Confirmation Required** pop-up window appears. An administrator must enter a user name and password as a final step before the upgrade begins. After you enter the user name and password, click **Confirm**. If you want to stop this process, click **Cancel**.

The **Software updates** page refreshes and presents the **Status** table. This page displays the status of each media server as the upgrade operation progresses.

Note: 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 service is 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: According to the requirement from the software update, the system may restart during the upgrade process. While the system restarts, 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.

- 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 begin. That checkpoint is used to enable the server to roll back

to if an upgrade fails. If you receive this failure message, it indicates that the creation of 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 does process does not continue. If you encounter this issue you must attempt to resolve it before you continue.
- 9 Complete this step only if your backup environment includes SAN client machines.

The fibre channel (FC) ports must be rescanned to allow any SAN client machines 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 [“Manage > Software Updates”](#) on page 194.

See [“Upgrading an appliance using the NetBackup Appliance Shell Menu”](#) on page 200.

See [“Software Updates > Status”](#) on page 209.

Upgrading an appliance using the NetBackup Appliance Shell Menu

To download and install a software update from the NetBackup Appliance Shell Menu, you can use an automated download procedure or a manual download procedure. Both procedures are documented.

Note: If you perform an upgrade from the NetBackup Appliance Shell Menu, you are still able to use the NetBackup Appliance Web Console during the upgrade operation.

Note: When you upgrade a NetBackup appliance, the FTMS server is rebooted automatically. As a result, the fibre channel (FC) ports must be rescanned to allow any SAN client machines to reconnect to the fibre transport (FT) devices. The last step in the following procedure describes how to rescan the FC ports, after the upgrade has been completed.

You can use the following commands to view the available release updates, see which update is currently installed, and see the current version of the appliance:

- `Main_Menu > Manage > Software > Check`
 Use this command to check the Symantec Support Web site for the latest software update.
- `Main_Menu > Manage > Software > List Downloaded`
 This command shows the available release updates for your appliance.
- `Main_Menu > Manage > Software > List Details All`
 This command shows all of the software packages that are currently installed on the appliance.
- `Main_Menu > Manage > Software > List Details Base`

This command shows all of the software packages that were installed on your appliance during the factory installation.

- `Main_Menu > Manage > Software > List Version`

This command shows the appliance version, the NetBackup version, and the appliance build date.

To upload and install NetBackup appliance software updates using an automated download procedure

- 1 You should perform this procedure from a computer that is connected to the appliance as well as to the Internet. That ensures that you can download the release update from the Symantec Support Web site to the appliance.
- 2 Open an SSH session and log on to the appliance as an administrator.
- 3 Enter the following command to determine if a software update is available from the Symantec Support Web site.

```
Main_Menu > Manage > Software > List AvailablePatch
```

- 4 Enter the following command to download a software update. Use the name of an available rpm to download.

```
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.

You can also use the `Main_Menu > Manage > Software > UpgradeStatus` command to monitor the status of the upgrade. This command provides a percentage of completion while the upgrade operation runs.

- 5 Enter the following command to verify that the rpm downloaded successfully.

```
Main_Menu > Manage > List Downloaded
```

- 6 Switch to the appliance console and enter the following command to install the release update. Use the name of the release update rpm from Step 4.

```
Main_Menu > Manage > Software > Install patch_name
```

Where *patch_name* is the name of the release update to install. You must make sure that the name you enter matches the update name that you uploaded on the appliance.

- 7 The upgrade takes approximately 45 minutes to complete and the appliance restarts after the operation completes. You can use the following command to check that the appliance version is correct.

```
Main_Menu > Manage > Software > List Version
```

- 8 After the restart, the appliance runs a self-diagnostic test after the disk pools are back online. You can refer to the results in `/log/selftest_report_SYM<timedate>.txt` for the results of this self test.
If SMTP is configured, an email notification that contains the self test result is sent.
- 9 Complete this step only if your backup environment includes SAN client machines.

The fibre channel (FC) ports must be rescanned to allow any SAN client machines 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.

The following procedure describes how to download and install a software update manually by entering file names individually.

To upload and install NetBackup appliance software updates using a manual download procedure

You can use this procedure to download and install a software update using the appliance shell menu. If the automated procedure failed, you can use this procedure to accomplish the same task.

- 1 You should perform this procedure from a computer that is connected to the appliance as well as to the Internet. That ensures that you can download the release update from the Symantec Support Web site to the appliance.
- 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 on your computer:

```
\\<appliance-name>\incoming patches
```

UNIX systems

Mount the following appliance NFS share:

```
■ mkdir -p /mount/<appliance-name>
■ mount
  <appliance-name>:/inst/patch/incoming
  /mount/<appliance-name>
```

Note that on Windows systems, you are prompted to provide the user name, `admin`, and its corresponding password.

- 5 Download and unzip or untar the release update from the Symantec Support site.

The following URL indicates the download location for the NetBackup release updates.

<http://www.symantec.com/business/support/index?page=landing&key=58991>

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.

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>

- 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
```

- 7 Run the following command to compute the md5 checksum value for the `SYMC_NBAPP_update-<version>-<release>.x86_64.rpm`. Verify that this checksum value matches the content of the `update.rpm.md5_checksum` file.

```
md5sum SYMC_NBAPP_update-<version>-<release>.x86_64.rpm
```

- 8 Copy this release update `.rpm` to the mounted share.

Note: During the copy process do not run any commands on the appliance. Doing so can cause the update installation to fail.

- 9 Unmap or unmount the shared directory after you have successfully copied the release update `.rpm` into the mounted share.
- 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 update is moved from the share directory location to its proper location. 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 Enter the following command to list the available release updates on the appliance. Note the name of the uploaded release update.

```
Main_Menu > Manage > Software > List Downloaded
```

This validates and moves the update from the share directory to its proper location. You are not notified that this move has occurred.

- 12 Switch to the appliance console and enter the following command to install the release update.

```
Main_Menu > Manage > Software > Install patch_name
```

Where *patch_name* is the name of the release update to install. You must make sure that the name you enter matches the update name that you uploaded on the appliance.

Note: You can also install on a remote appliance and have the release update copied and installed to that appliance. Use the following command to install a remote appliance:

```
Main_Menu > Manage > Software > Install patch_name  

target_appliance
```

Where *patch_name* is the name of the software update to install, and *target_appliance* is the name of the appliance that you want to install the software update.

- 13 The upgrade takes approximately 45 minutes to complete and the appliance restarts after the operation completes. You can use the following command to check that the appliance version is correct.

```
Main_Menu > Manage > Software > List Version
```

You can also use the `Main_Menu > Manage > Software > UpgradeStatus` command to monitor the status of the upgrade. This command provides a percentage of completion while the upgrade operation runs.

- 14 After the restart, the appliance runs a self-diagnostic test after the disk pools are back online. You can refer to the results in `/log/selftest_report_SYM<timedate>.txt` for the results of this self test.

If SMTP is configured, an email notification that contains the self test result is sent.
- 15 Complete this step only if your backup environment includes SAN client machines.

The fibre channel (FC) ports must be rescanned to allow any SAN client machines 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 [“Manage > Software Updates”](#) on page 194.

See [“Upgrading an appliance using the NetBackup Appliance Web Console”](#) on page 196.

See [“Software Updates > Status”](#) on page 209.

Media servers to upgrade

After you click **Install**, the **Manage > Software Updates** page refreshes and displays the following tables:

- **Select the media servers to upgrade**
This table displays the media 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.
See [“Manage > Software Updates”](#) on page 194.

Table 4-28 Select the media servers to upgrade

Field name	Description
Media Server	The name of the media server that is currently configured in your master server environment. In a cluster configuration, multiple media servers are displayed.
Current Version	The version of the appliance software that is installed on the media server before the upgrade begins.
Version after upgrade	The version of the appliance software that is installed on the media server after the upgrade completes successfully.
Next	Click Next to continue with the upgrade process after you have chosen the media servers that you want to upgrade. After you click Next , a pop-up window appears that lists the media servers that you selected. To continue, do the following: <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	Click Cancel to cancel the upgrade.

See [“Software Updates > Status”](#) on page 209.

See [“Upgrading an appliance using the NetBackup Appliance Web Console”](#) on page 196.

See [“Upgrading an appliance using the NetBackup Appliance Shell Menu”](#) on page 200.

See [“Manage > Software Updates”](#) on page 194.

Software Updates > Status

After you entered your user name and password and clicked **Confirm**, the **Manage > Software Updates** page refreshes and displays the following two tables:

- **Status**
This table enables you to view the progress of the upgrade as it applies to each media server that you chose to upgrade.
- **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 194.

This page enables you to see progress of the upgrade across all of the media servers that you selected. After the upgrade is complete across all servers, you must then click **Finish**. The following information is presented to you on the page.

Table 4-29 Status

Field name	Description
Media Server	The name of the media servers that you chose to upgrade.
Status	Displays whether each media server is online or offline.
Progress	Shows the progress and the completion status of the upgrade process for each media server.

See [“Media servers to upgrade”](#) on page 208.

See [“Upgrading an appliance using the NetBackup Appliance Web Console”](#) on page 196.

See [“Upgrading an appliance using the NetBackup Appliance Shell Menu”](#) on page 200.

See [“Manage > Software Updates”](#) on page 194.

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 appliance shell menu.

See [“Installing an EEB”](#) on page 210.

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.

See [“Upgrading an appliance using the NetBackup Appliance Web Console”](#) on page 196.

To upload and install an appliance emergency engineering binary using the 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:

```
\\<appliance-name>\incoming_patches
```

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.

Note: The `Software > Check and Software > Download` method applies only for uploading software release updates.

- 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 Downloaded` 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 available EEBs.

```
Main_Menu > Manage > Software > List EEBs
```

- 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.

See [“About installing an EEB”](#) on page 210.

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 on clients through CIFS and NFS shares”](#) on page 212.

See [“Installing NetBackup client software from the packages”](#) on page 213.

See [“Installing the NetBackup Administration Console”](#) on page 216.

Installing NetBackup client software on clients 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 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.

To install the NetBackup client software on a UNIX client through an NFS share

- 1 On the UNIX client computer where you want to install the NetBackup client software, log on as root.
- 2 Mount the following NFS share:
`<appliance_name>:/inst/client`
- 3 Browse the files within the NFS share directory. Files that are similar to the following appear:

<code>.packages</code>	<code>clientconfig</code>	<code>quickinstall.exe</code>
<code>PC_Clnr</code>	<code>docs</code>	<code>unix-client-install</code>

- 4 Run the `unix-client-install` script.
This action installs the NetBackup client software.
- 5 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/openv/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.

See [“About installing NetBackup Administration Console and client software”](#) on page 211.

See [“Installing NetBackup client software from the packages”](#) on page 213.

Installing NetBackup client software from the packages

You can install client software and the NetBackup Administration Console software on the clients that you want to back up. The log on page of the NetBackup Appliance user interface provides a **Software** link that you can use to install that software. The drop-down list shows the available operating systems that are available for you to install on.

To install the agent software to a client

- 1 Log into the client that you want to back up.
- 2 In the right pane of the landing page, click **Software**. The following list shows the choices that you have to choose from:
 - All
 - Windows
 - Linux
 - Solaris
 - AIX
 - HP
 - BSD
 - Mac OS

Note: If you choose to extract Linux, UNIX, Solaris, AIX, or BSD images, Symantec recommends that you use GNU tar version 1.16 or higher to extract all .tar packages.

See, the following Technote on the Symantec Support Web site for more information.

<http://www.symantec.com/docs/TECH154080>

- 3 Choose **All** or select an operating system from the **Operating System** drop-down.
- 4 Right-click the appropriate file under **Software** to download the agent software. The browser writes the software files to the location you specify. Example locations are as follows:
 - On Windows platforms, download the software to C:\temp or to the desktop.
 - On Linux or UNIX platforms, download the software to /tmp.To determine the type of hardware on your Windows system, right-click **My Computer** and select **Properties**.
- 5 Unzip or untar the software package.

6 Install the client software

For Windows, click on the Windows executable, **setup.exe**

For UNIX systems, run the `.install` script.

- 7 After you have successfully installed the client software, you should add the appliance master server name to the client.
 - On Windows systems, you can use the Backup, Archive, and Restore interface to add the appliance master server name on the client. Perform the following:
 - After NetBackup has been loaded 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 **Server to use for backups and restores** field and 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.
 - Open a Windows Command prompt.
 - Enter `services.msc` and press **Enter**.
 - On UNIX systems, 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.

See [“Installing NetBackup client software on clients through CIFS and NFS shares”](#) on page 212.

See “[About installing NetBackup Administration Console and client software](#)” on page 211.

Installing the NetBackup Administration Console

You can install the NetBackup Administration Console software on the clients that you want to back up. The log on page of the NetBackup appliance user interface provides a **Software** link that you can use to install that software. The drop-down list shows the available operating systems that are available for you to install on.

To install the NetBackup Administration Console software on a client

- 1 Log into the client that you want to back up.
- 2 In the right pane of the landing page, click **Software**. The following list shows the choices that you have to choose from:
 - All
 - Windows
 - Linux
 - Solaris
 - AIX
 - HP
 - BSD
 - Mac OS

Note: If you choose to extract Linux, UNIX, Solaris, AIX, or BSD images, Symantec recommends that you use GNU tar version 1.16 or higher to extract all .tar packages.

See, the following Technote on the Symantec Support Web site for more information.

<http://www.symantec.com/docs/TECH154080>

- 3 Choose **All** or select an operating system from the **Operating System** drop-down.
- 4 Right-click the appropriate file under **Software** to download the agent software. The browser writes the software files to the location you specify. Example locations are as follows:
 - On Windows platforms, download the software to `C:\temp` or to the desktop.

- On Linux or UNIX platforms, download the software to `/tmp`.

To determine the type of hardware on your Windows system, right-click **My Computer** and select **Properties**.

- 5 Unzip or untar the software package.

- 6 Install the administration console software

For Windows, click on the Windows executable, **setup.exe** in the `Addons/JavaInstallFiles` directory.

For UNIX systems, run the `.install` script.

- 7 After you have successfully installed the NetBackup Administration Console, you should add the appliance master server name to the client.

- On Windows systems, you can use the Backup, Archive, and Restore interface to add the appliance master server name on the client. Perform the following:
 - After NetBackup has been loaded 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 **Server to use for backups and restores** field and 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.
 - Open a Windows Command prompt.
 - Enter `services.msc` and press **Enter**.
- On UNIX systems, 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/openv/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.

See [“About installing NetBackup Administration Console and client software”](#) on page 211.

See [“Installing NetBackup client software on clients through CIFS and NFS shares”](#) on page 212.

See [“Installing NetBackup client software from the packages”](#) on page 213.

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 [“Adding additional servers to the appliance”](#) on page 218.

Adding additional servers to the appliance

The following procedures enable you to add or delete servers.

Use the following procedure to add additional servers to the appliance.

To add an additional server

- 1 Logon to the NetBackup Appliance NetBackup Appliance Web Console.
- 2 Click **Manage > Additional Servers**.
- 3 Click **Add**. The Add Additional Server window opens.
- 4 In the **Server Name** field, enter the name of the server that you want to add, and then click **OK**.
- 5 Click **Cancel** to exit the Add Additional Server window.

Use the following procedure to delete servers from the appliance.

To delete an additional server

- 1 Logon to the NetBackup Appliance NetBackup Appliance Web Console.
- 2 Click **Manage > Additional Servers**.
- 3 Select the check box against the server that you want to delete, and then click **Delete**.

- 4 The following message appears when you click **Delete**. The following message is displayed:

Deleting the selected server(s) will disable related features
in NetBackup. Are you sure you want to proceed?

Click **OK** to delete the selected server.

- 5 To delete all the servers from the appliance, select the **Server Name** checkbox, and click **Delete**.

See [“Manage > Additional Servers”](#) on page 218.

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 52xx 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 administrative Web UI or the appliance shell menu.

You can use the command-line interface 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 appliance shell menu.

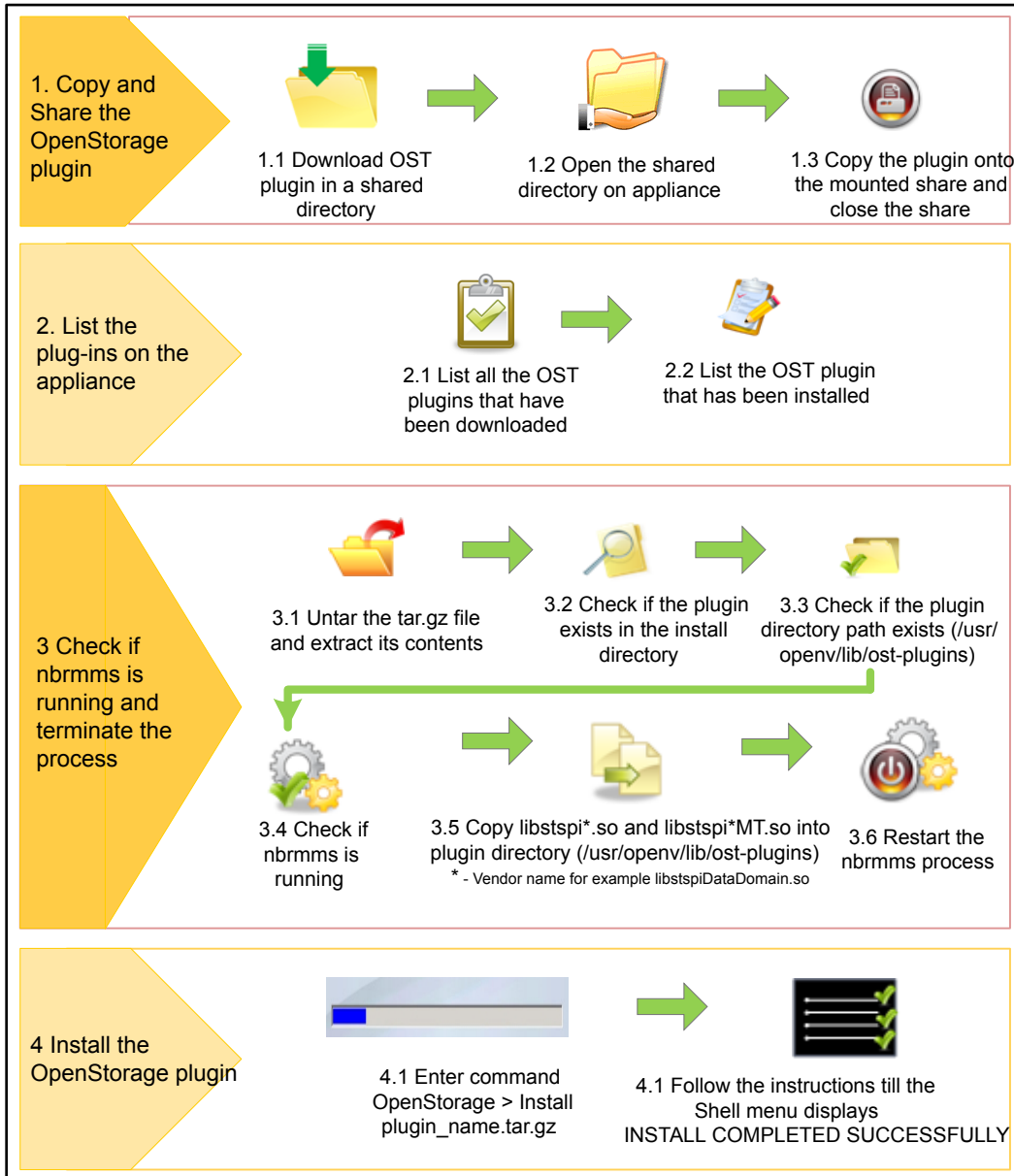
See the `SetProperty` command in the *Symantec NetBackup Appliance Command Reference Guide*.

About OpenStorage plugin installation

You can install and open an OpenStorage (OST) plugin on the **NetBackup Appliance** using the 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 5-1 OpenStorage plugin installation process



See “Installing OpenStorage plugin” on page 223.

See “[Uninstalling OpenStorage plugin](#)” on page 224.

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 appliance shell menu.

To install the OpenStorage plugin

- 1 Log on to the administrative 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` for 52xx media and master appliances.

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:
 - `MainMenu > Manage > OpenStorage > Share Close` for 52xx media and master appliances.
- 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 52xx 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 221.

See [“Uninstalling OpenStorage plugin”](#) on page 224.

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 52xx 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 221.

See [“Installing OpenStorage plugin”](#) on page 223.

About mounting a remote NFS

You can use the 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 appliance shell menu:

Table 5-1 Commands to work with NFS drive

Command	Descriptions
Mount	Use the <code>Mount</code> command to mount an NFS drive.

Table 5-1 Commands to work with NFS drive *(continued)*

Command	Descriptions
<code>MountList</code>	Use the <code>MountList</code> command to list all the existing mount points on your appliance.
<code>Unmount</code>	Use the <code>Unmount</code> command to un-mount a previously mounted NFS drive.

See [“Mounting an NFS remote drive”](#) on page 226.

See [“Unmounting an NFS drive”](#) on page 228.

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 your 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

	<i>RemotePath</i>	<i>MountPoint</i>	[FileSystemType]	[Options]
Example	suryan. engba. symantec.com :/build1	/mymounts/moun1	nfs, nfs4 or any other supported type by the underlying Mount command.	ro 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 your appliance shell menu using your admin 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:

```
MountList [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.

See [“About mounting a remote NFS”](#) on page 225.

Unmounting an NFS drive

This procedure describes how to unmount an NFS drive.

To unmount an NFS drive

- 1 Log in to your appliance shell menu using your admin 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.	Specify this parameter to unmount the NFS forcibly.
	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. 	
Format	The directory name must start with / and must have the correct directory name. <p>Note: If the specified directory is a valid mount directory, it is unmounted.</p>	
Parameter type	Mandatory	Optional
Example	/mymounts/moun1	

- 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 225.

See [“About mounting a remote NFS”](#) on page 225.

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 230.

See [“Creating NetBackup administrator user accounts”](#) on page 234.

See [“Managing NetBackup administrator user account passwords”](#) on page 236.

See [“Auditing NetBackup Administrator accounts”](#) on page 237.

See [“Deleting NetBackup administrator user accounts”](#) on page 237.

See [“Viewing NetBackup administrator user accounts”](#) on page 238.

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 229.

See [“About running NetBackup commands”](#) on page 231.

See [“Creating NetBackup administrator user accounts”](#) on page 234.

See [“Deleting NetBackup administrator user accounts”](#) on page 237.

See [“Viewing NetBackup administrator user accounts”](#) on page 238.

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 232.

See [“About operating systems commands”](#) on page 232.

See [“About best practices”](#) on page 233.

See [“About known limitations”](#) on page 234.

About creating a NetBackup touch file

A NetBackup administrator can create and edit a NetBackup touch configuration file in the `/usr/opensv/netbackup/db/config` directory. For example, to create a touch file called `DEFERRED_IMAGE_LIMIT`, use the following steps:

- Create a file with that name in NetBackup administrator home directory or a subdirectory.
- Use the `cp-nbu-config` command to add the desired content in the touch file, for example:

```
# echo 128 > ~/DEFERRED_IMAGE_LIMIT
# cp-nbu-config ~/DEFERRED_IMAGE_LIMIT
```

See [“About running NetBackup commands”](#) on page 231.

See [“About operating systems commands”](#) on page 232.

See [“About best practices”](#) on page 233.

See [“About known limitations”](#) on page 234.

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 231.

See [“About creating a NetBackup touch file”](#) on page 232.

See [“About best practices”](#) on page 233.

See [“About known limitations”](#) on page 234.

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.
- You should not delete the alias file in the home directory. If for any reason the alias file is deleted, you must recreate it manually from the same shell from where the alias file was deleted. The following steps from within the same shell where the alias was deleted to create a new alias file:
 - `# alias > ~/.alias`
 - `# chmod 664 ~/.alias`
 - If you are not able to recover the alias file with this method, then you can create an alias file manually for all the NetBackup commands. Otherwise, you must specify `sudo` even if you choose to use a base command name to run NetBackup commands.
- 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 231.

See [“About operating systems commands”](#) on page 232.

See [“About best practices”](#) on page 233.

See [“About known limitations”](#) on page 234.

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 `cp-nbu-config` command supports creating and editing NetBackup touch configuration files only in the `/usr/opensv/netbackup/db/config` directory.
- 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 231.

See [“About creating a NetBackup touch file”](#) on page 232.

See [“About operating systems commands”](#) on page 232.

See [“About best practices”](#) on page 233.

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 229.

See [“About NetBackup administrator capabilities”](#) on page 230.

See [“Managing NetBackup administrator user account passwords”](#) on page 236.

See [“Auditing NetBackup Administrator accounts”](#) on page 237.

See [“Deleting NetBackup administrator user accounts ”](#) on page 237.

See [“Viewing NetBackup administrator user accounts”](#) on page 238.

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 230.

See [“Creating NetBackup administrator user accounts ”](#) on page 234.

See [“Managing NetBackup administrator user account passwords”](#) on page 236.

See [“Auditing NetBackup Administrator accounts”](#) on page 237.

See [“Deleting NetBackup administrator user accounts”](#) on page 237.

See [“Viewing NetBackup administrator user accounts”](#) on page 238.

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 5-2](#) describes the functions that you can perform as you manage your account passwords.

Table 5-2 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 229.

See [“About NetBackup administrator capabilities”](#) on page 230.

See [“Logging on as a NetBackup administrator”](#) on page 235.

See [“Creating NetBackup administrator user accounts ”](#) on page 234.

See [“Auditing NetBackup Administrator accounts”](#) on page 237.

See [“Deleting NetBackup administrator user accounts ”](#) on page 237.

See [“Viewing NetBackup administrator user accounts”](#) on page 238.

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 234.

See [“Managing NetBackup administrator user account passwords”](#) on page 236.

See [“Deleting NetBackup administrator user accounts ”](#) on page 237.

See [“Viewing NetBackup administrator user accounts”](#) on page 238.

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 229.

See [“About NetBackup administrator capabilities”](#) on page 230.

See [“Creating NetBackup administrator user accounts”](#) on page 234.

See [“Managing NetBackup administrator user account passwords”](#) on page 236.

See [“Auditing NetBackup Administrator accounts”](#) on page 237.

See [“Viewing NetBackup administrator user accounts”](#) on page 238.

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 229.

See [“About NetBackup administrator capabilities”](#) on page 230.

See [“Creating NetBackup administrator user accounts”](#) on page 234.

See [“Managing NetBackup administrator user account passwords”](#) on page 236.

See [“Auditing NetBackup Administrator accounts”](#) on page 237.

See [“Deleting NetBackup administrator user accounts ”](#) on page 237.

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 239.
- 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 244.

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.

You can perform Auto Image Replication between the following:

- A 2.6 MSDP to another 2.6 MSDP

Note: You cannot perform Auto Image Replication from a 2.5 MSDP to a 2.6 MSDP. To be able to perform Auto Image Replication, you must first upgrade to 2.6 MSDP.

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 240.
2.	Review the prerequisites for Auto Image Replication.	See “Prerequisites for Auto Image Replication” on page 241.
3.	Configure the replication target	See “Configuring a replication target” on page 242.
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.

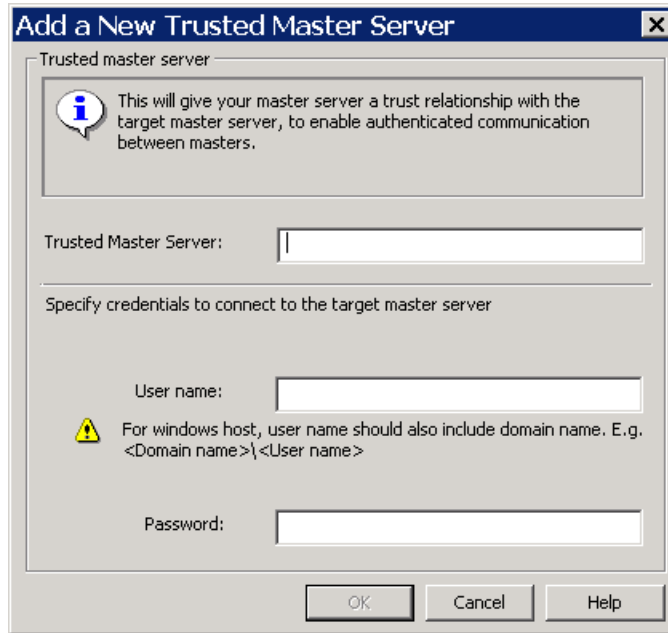
To add a trusted master server

- 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 243.

- 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*.

Decommissioning a NetBackup appliance

This chapter includes the following topics:

- [About decommissioning a NetBackup 52xx appliance](#)
- [Decommissioning a NetBackup 52xx master appliance](#)
- [Decommissioning a NetBackup 52xx media appliance](#)

About decommissioning a NetBackup 52xx appliance

To decommission an appliance means to physically remove or eliminate the appliance from the backup environment. When you decide which appliance to decommission, you must make sure that the appliance is not configured as a backup destination for any clients.

You may need to decommission an appliance for any of the following reasons:

- The appliance has issues and needs to be reset to factory settings.
- The appliance has hardware issues and needs to be replaced.
- The appliance is no longer needed (down-sizing your backup environment).
- The appliance may need to be removed from the network domain to be repaired.
- The appliance is no longer supported and needs to be replaced.

After you determine that you need to decommission a media appliance, you can provision a new appliance to act as a target for all backups. With this technique the load is decreased on the existing appliance and moved to the new appliance. The existing can be removed from the domain eventually.

Decommissioning a NetBackup 52xx master appliance

When you decommission a master appliance it means all of the catalog and backup images stored on the disk will be lost. You can simply use Factory reset command to reset this appliance.

To decommission a NetBackup master appliance

- 1 Open an SSH session on the master appliance.
- 2 Log on as admin.
- 3 Run the following command and follow any additional prompts to reset the appliance to factory default settings.

```
Main_Menu > Support > FactoryReset
```

Decommissioning a NetBackup 52xx media appliance

When you decommission a media appliance it means all of the backup images that are stored on the disk will be destroyed. You must use the appliance shell menu to decommission a media appliance from a master appliance. Use the following procedure to decommission a media backup appliance to another appliance.

Note: If the media server that you are about to decommission has a deduplication pool storage unit configured, you must manually expire the images on that storage unit before you attempt to remove the media server.

To decommission a NetBackup media appliance

- 1 Open an SSH session on the master appliance.
- 2 Log on as admin.

- 3 Enter the following command to remove media appliance and move the ownership of the tape library:

```
Main_Menu > Appliance > Remove MediaServer TargetMediaServer
```

The variable *MediaServer* is the host name of the media server that you want to decommission. This media server can be an appliance or non-appliance media server. And *TargetMediaServer* is the host name of the media server that you have selected to receive the media. Again, the *TargetMediaServer* media server can be an appliance or non-appliance media server.

You can specify **NONE** for the *TargetMediaServer* variable if you do not need to move the media. If you specify **NONE** for the *TargetMediaServer* variable, then all of the backup images on the media that are attached to the media server appliance are lost.

- 4 Enter *Yes*, to confirm that you want to remove this appliance.
- 5 If you designated a valid media server appliance in the *TargetMediaServer* variable, enter the following command on each of the appliances to shut them down after a successful decommission of the appliance

```
Main_Menu > Support > Shutdown
```

- 6 You must cable the tape library to the target media server appliance.
- 7 Run the following command to turn on the media server.

```
Main_Menu > Support > Reboot
```

- 8 Enter the following command to configure the tape library to a media server appliance that is defined in the *TargetMediaServer* variable.

```
Main_Menu > Manage > Libraries > Configure MediaServer
```

Note: If you want to use a media server that is not an appliance media server, then you must use the NetBackup Administration Console to configure the tape library to that media server.

Where *MediaServer* is the media server appliance that you connected to the tape library and need to configure.

- 9 From the decommissioned media server, run the following command and follow any additional prompts to reset the appliance to factory default settings.

```
Main_Menu > Support > FactoryReset
```

Once you have completed the factory reset process and finished decommissioning the media server, you can configure it to serve any role that you choose. If you configure it as a master server, then you can use the

```
Main_Menu > Appliance > Add
```

 command to add a media appliance.

If a problem occurs, contact Symantec Technical Support for assistance.

Note: After you decommission a media server, the process does not remove disk pool and storage server objects of type PureDisk. You must use the NetBackup Administration Console from the NetBackup master server to remove these objects.

See the section "Decommissioning a media server" in the *Symantec NetBackup Administrator's Guide, Volume I* for more information on how to decommission a NetBackup media server.

You can refer to the following Technote on decommissioning a NetBackup 7.x media server:

<http://www.symantec.com/docs/TECH62119>

You can also refer to the following Technote on how to remove NetBackup Media Server Deduplication Option (MSDP) configurations from a NetBackup environment:

<http://www.symantec.com/docs/TECH150431>

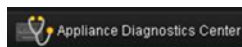
Troubleshooting

This chapter includes the following topics:

- [Troubleshooting and tuning Appliance from the Appliance Diagnostics Center](#)
- [NetBackup Appliance log file location information](#)
- [About password recovery](#)
- [About disaster recovery](#)
- [Gathering device logs with the Datacollect command](#)

Troubleshooting and tuning Appliance from the Appliance Diagnostics Center

You can troubleshoot multiple failures and resolve issues in NetBackup Appliance by using some interactive self-repair wizards in the Appliance Diagnostics Center. A separate wizard helps you perform specific 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:

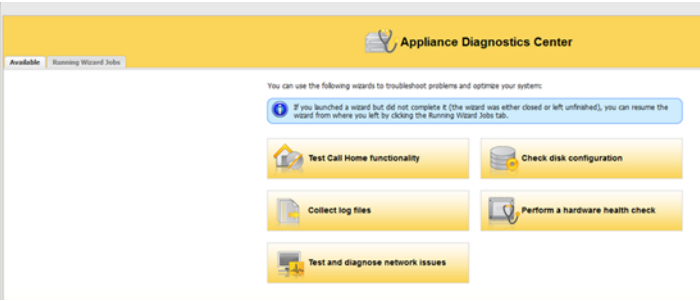


When you click this icon, the Appliance Diagnostics Center page appears where you can see the **Available** and the **Running Wizard Jobs** tab. You can access the NetBackup Appliance Web Console by closing this page.

All the troubleshooting wizards are listed under the **Available** tab.

[Figure 7-1](#) shows a sample view of the **Available** tab.

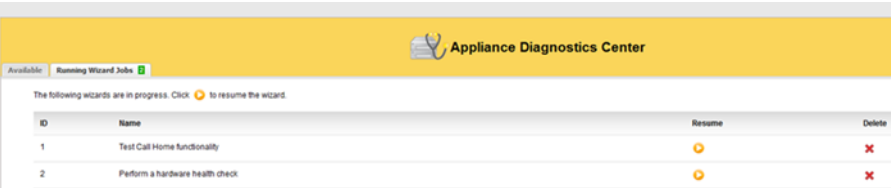
Figure 7-1 Available tab



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 7-2 shows a sample view of the **Running Wizard Jobs** tab.

Figure 7-2 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 are able to 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, MSDP 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. You can do any of the following:</p> <ul style="list-style-type: none"> ■ Collect log files from a 52xx Appliance. <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 7-1 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 to Symantec Support. 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. ■ In order 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 etc. 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 7-1](#) 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 7-1 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 <p>Note: The legacy logs and the vxlogs are collected based on the time frame that you specify.</p>
Appliance	<p>Appliance logs including hardware and event logs. The following Appliance logs are collected:</p> <ul style="list-style-type: none"> <code>hostchange.log</code>, <code>app_vxul 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>
Operating System	<p>Operating system logs that include the following:</p> <p><code>boot.log</code>, <code>boot.msg</code>, <code>boot.ormsg</code>, <code>messages</code>.</p>
Deduplication (Media Server Deduplication Pool or PureDisk)	<p>Logs related to Media Server Deduplication Pool (MSDP):</p> <p><DIR> PD</p> <ul style="list-style-type: none"> <FILE> log <DIR> puredisk
Appliance Web Console	<p>Appliance Web console logs that include the following:</p> <p><DIR> WEBGUI</p>
NetBackup support utility (<code>nbsu</code>)	<p>Diagnostic information about NetBackup and the operating system.</p>

Table 7-1 Log files collected by the Collect Logs Wizard (*continued*)

Log Type	What is collected?
DataCollect	Hardware and storage device logs. The logs created by the <code>CallhomeDataGather</code> utility are collected.

Note: During checkpoint creation, other parts of the NetBackup Appliance Web Console are not available. Hence if a checkpoint is being created and you are running a wizard from another window at the same time, the wizard will not be available.

NetBackup Appliance log file location information

As you define and troubleshoot a problem, always try to capture potentially valuable information. The NetBackup appliance has the ability to capture data as log files in specific locations.

Browse and view the log files as follows:

- Enter browse mode by running the `Main_Menu > Support > Logs` followed by the `Browse` command in the appliance shell menu. The `LOGROOT/>` prompt appears.
- To display the available log directories on your appliance, type `ls` at `LOGROOT/>` prompt.
- 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.
- To view the files, use the `less <FILE>` or `tail <FILE>` command. Files are marked with `<FILE>` and directories with `<DIR>`.

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.

Refer to the *NetBackup Appliance Command Reference Guide* for more information on how to use the `Logs` commands.

Table 7-2 lists the log files and where they are located in appliance.

Table 7-2 NetBackup Appliance log file locations

NetBackup appliance logs	Log file location
NetBackup appliance configuration log	<DIR> APPLIANCE config_nb_factory.log
NetBackup appliance command log	<DIR> APPLIANCE app_change_control.log
NetBackup appliance debug log	<DIR> APPLIANCE app_debug.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
NetBackup appliance operating system (OS) installation log	<DIR> OS boot.log boot.msg boot.omsg messages
NetBackup Administrative Web user interface log and the NetBackup Web server log	<DIR> WEBGUI <ul style="list-style-type: none"> ■ <DIR> gui ■ <DIR> webserver

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, call Symantec Technical Support for assistance.

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 239.

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 4, “Configuring Backups”, review the following topics:
 - “Protecting the NetBackup Catalog”
<http://www.symantec.com/docs/HOWTO68036>
<http://www.symantec.com/docs/HOWTO33415>
 - “Strategies that ensure successful NetBackup catalog backups”
<http://www.symantec.com/docs/HOWTO34437>
<http://www.symantec.com/docs/HOWTO33393>
 - In Section 4, “Configuring Backups”, review the topic, “Creating policies for backups and snapshots”.
 This topic explains the functionality and principles of backup policies in a way to help you determine a disaster recovery plan for the appliance.
 - Review the topics within Section 3, “Configuring Storage”.
- *NetBackup Troubleshooting Guide*

Gathering device logs with the Datacollect command

You can use the `Datacollect` command from the `Main > Support` shell menu to gather storage device logs. You can share these device logs with the Symantec Support team to resolve device-related issues.

To gather device logs with the Datacollect command

- 1 Log on to the administrative 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:

```
appliance123:Support> DataCollect
=====DataCollect=====
Begin To Collect NetBackup 5220 Device Logs.
This Will Take a Moment,Please Be Patient!

NetBackup 5220 Device OS Information collection is complete!
NetBackup 5220 Device IPMI Information collection is complete!
NetBackup 5220 Device RAID AdpAllInfo collection is complete!
NetBackup 5220 Device RAID BbuStatus collection is complete!
NetBackup 5220 Device RAID CfgDsply collection is complete!
NetBackup 5220 Device RAID EncInfo collection is complete!
NetBackup 5220 Device RAID LdPdInfo collection is complete!
NetBackup 5220 Device RAID AdpEventLog collection is complete!
NetBackup 5220 Device RAID FwTermLog collection is complete!
NetBackup 5220 Device SMARTinfo collection is complete!
NetBackup 5220 Device log collection is complete!
All logs have been collected in /tmp/DataCollect.zip

Log file can be collected from the appliance shared folder -
\\appliance123\logs\APPLIANCE
Share can be opened using Main->Support->Logs->Share Open

=====End of DataCollect=====
```

The appliance generates the device log file. You can find this file in the `/tmp/DataCollect.zip` folder.

- 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.

Reconfiguring a NetBackup appliance

This chapter includes the following topics:

- [About reconfiguring a NetBackup appliance](#)

About reconfiguring a NetBackup appliance

If you experience problems with the appliance software, you can attempt to roll back the appliance software to a checkpoint or you can perform a factory reset operation. With the factory reset option, you can reset the appliance to its original default settings or if checkpoints exist, you can reset the appliance to an existing checkpoint. If you chose to perform a factory reset, you have the option to preserve your catalog configuration and existing data.

If you experience major issues with the appliance software or no valid checkpoints exist, then you may need to reimage the appliance. You may need to reset or reconfigure a 52xx master server appliance, or a 52xx media server appliance in the following situations:

- The disks that host the operating system fail.
- The operating system experiences a fatal error and you are not able to start the appliance.

In a disaster recovery situation you must determine if you have lost all of the data and any software updates that were currently on the media or master server appliance. Or you may determine that you have an opportunity to save all of the data. No matter which scenario you face, you must image the appliance and then reconfigure the appliance in the same way you did as a new appliance. Symantec recommends that you record all of your initial configuration information so that you can reference that information should you need to reconfigure.

Note: During the reimaging process, all Symantec storage shelves that were already attached to the appliance should remain attached. In addition, do not attach any additional Symantec storage shelves.

Note: Because NetBackup 5200 appliances are no longer shipped, Symantec does not support the ability to reimage a 5200 that has an earlier version of software with the current n2.6 software release. You must reimage the 5200 appliance with the same supported software version, such as n2.5, and then upgrade to the n2.6 release.

Note: NetBackup appliance version n2.6 contains enhancements in the storage configuration area and it supports a new disk layout version of SF 6.0. Because of the enhancements, Symantec does not support the ability to reimage a 52xx appliance to a lower version such as n2.5, after you have installed and configured version n2.6.

Best practices before you begin reconfiguring your appliance

Before you reconfigure your appliance, you should consider the following with regards to license keys:

- If you intend to preserve data during the reconfiguration process, you must use the appliance shell menu. Reconfiguration using the NetBackup Appliance Web Console is not supported in this release.
- If during the reconfiguration process, the media or master server appliance goes through an initial configuration, then you must use the appliance shell menu to install the license keys before the initial configuration process begins. In addition, the user name and password may be set back to the default values if a factory reset operation was performed.

Record your configuration information before you begin a reconfiguration

Before you begin a reimage process, Symantec recommends that you record the configuration information that you entered when you performed the initial configuration process on the appliance. If a factory reset is run after the reimage process completes you should enter the same configuration information to connect to the appliance. In addition, after a factory reset the user name and password are reset to the default values.

- Network configuration:
 - Network interface

- IP address
- Subnet mask
- Gateway
- Network name
- Host configuration:
 - For Domain Name System (DNS) - Domain name suffix, DNS IP address, and the Search domain
 - For non-DNS systems - IP address, Fully qualified host name, and the short host name
- User name and password - Default user name is `admin` and the default password is `P@ssw0rd`.
- Role configuration - It is important that you configure the appliance using the same role as you did when it was initially configured.
- Storage configuration - If you are reconfiguring a media server appliance that has backup data on a disk that you want to preserve, you can record the following information so you have it available when you are ready to configure your storage.
 - Storage pool size
 - Disk pool name
 - Storage unit name

See [“Reimaging a NetBackup appliance”](#) on page 260.

See [“Reconfiguring a 52xx master server appliance from the USB drive using the NetBackup Appliance Shell Menu”](#) on page 268.

See [“Reconfiguring a 52xx media server appliance from the USB drive using the NetBackup Appliance Shell Menu”](#) on page 275.

Reimaging a NetBackup appliance

The following procedure describes the steps required to install a new image on a media server appliance. If you want to preserve your backup data, you must perform the following procedure using the appliance shell menu.

To reimage an appliance from the USB drive

- 1 If you cannot log into the appliance, insert the USB drive into the appliance, turn on the appliance, and then proceed to Step 4.

If you can log into the appliance and you can access the appliance shell menu, export (copy) and move the IPsec credentials to a remote drive using the following steps and then continue with Step 2.

- Open a CIFS and an NFS share with the following command:

```
Manage > Software > Share Open
```

- To export (copy) the IPsec credentials, enter the following command:

```
Network > Security > Export <yes/no> /inst/patch/incoming
```

Where <yes/no> is for whether you want password protection.

Note: The output from the `export` command creates a backup `.pfx` file of the actual certificate. If you select `yes` to use a password, the file name is a number with the `.pfx` extension (`nnnnnnnn.pfx`). If you select `no` for no password, a period precedes the file name (`.nnnnnnnn.pfx`).

If you use a password, retain the name of the password to use when you run the `Import` command later in this procedure.

- To move the `.pfx` files into a local directory on a remote computer, create and mount a mount point and then move the files as follows:

Windows

This example assumes that the Windows system uses Samba.

- Create and mount a mount point as follows:

```
net use <AnAvailableDriveLetter>:  
\\<appliance-host>\incoming patches"
```

- Copy the `.pfx` file as follows:

```
# copy /inst/patch/incoming/*.pfx  
/mnt/<computer_name>
```

UNIX or Linux

This example assumes that the UNIX or Linux system uses NFS.

- Create and mount a mount point as follows:

```
# mkdir -p /mnt/<computer_name>  
# mount -t nfs <computer_name>:/<share_name>  
/mnt/<computer_name>
```

- Copy the `.pfx` file as follows:

```
# cp /inst/patch/incoming/*.pfx  
/mnt/<computer_name>
```

- 2 Insert the USB drive into an appliance USB port on the media server appliance that you want to reimage.

- 3 Connect the remote management port of the appliance that you are reconfiguring to the corporate network, then do the following:
 - Connect the remote management port on the media server appliance to the corporate network.
 - Log on to the remote management port of media server appliance from a remote machine, using the IP address that you assigned to the remote management port.

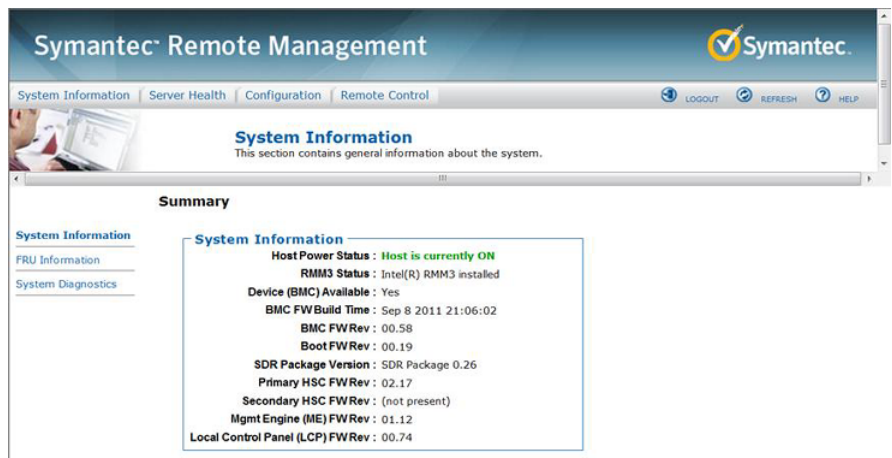


Please log in to access the device.

Username

Password

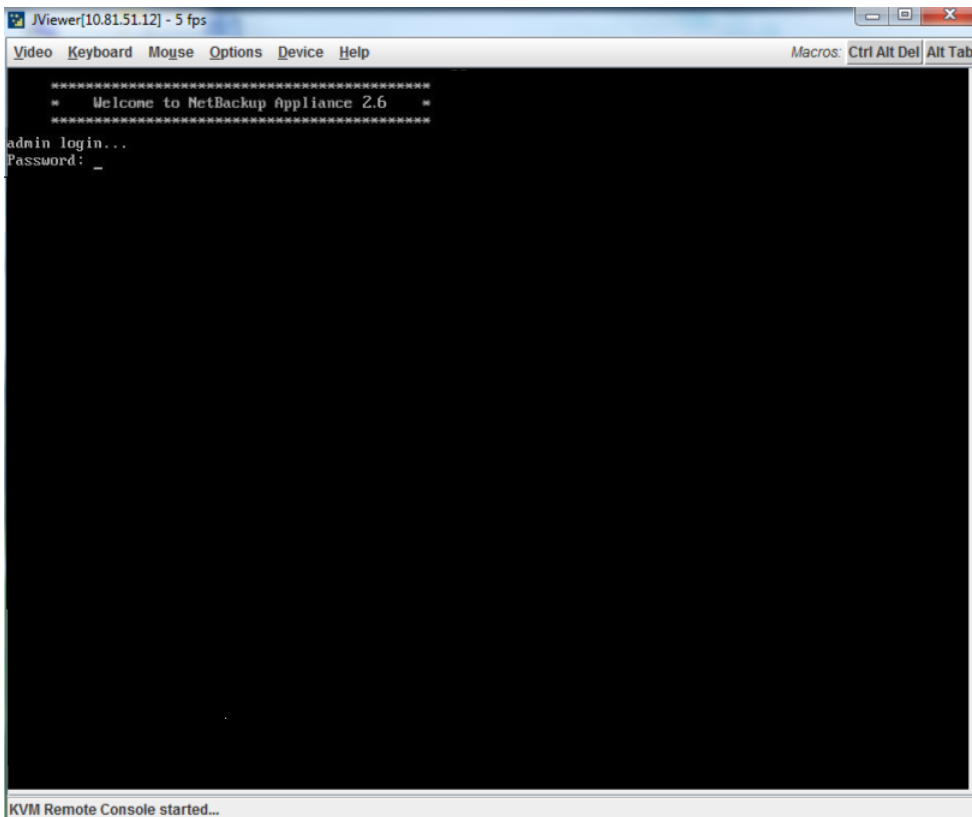
On the **System Information** page, click **Remote Control**.



On the **Remote Control** page, click **Launch Console**.



- 4 Click **Launch Console**. This step opens a **JViewer** application that enables you to remotely monitor and control the media server appliance.

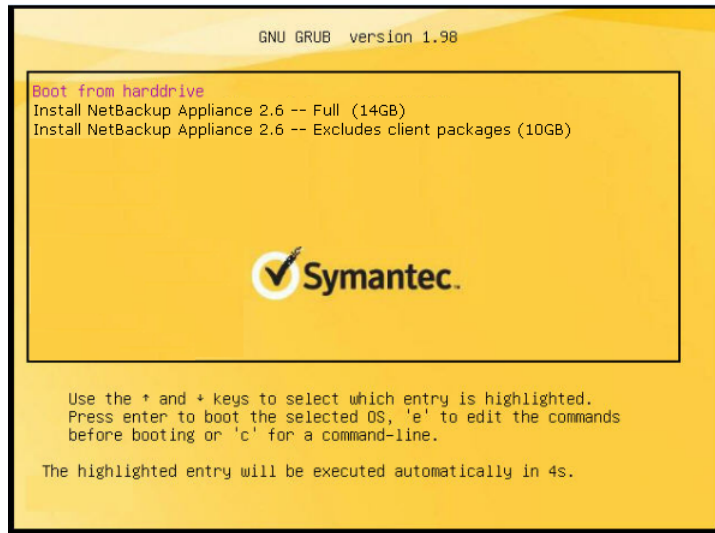


- 5 From the **Symantec Remote Management** interface, select **Server Power Control**. On that Web page do the following:
 - Select the **Reset Server** radial button.
 - Check the **Force-enter BIOS Setup** check box.
 - Click **Perform Action**.
- 6 In the JViewer application window, press F6. That action enables you to enter into the BIOS of the media server appliance.



- 7 After you select the USB drive, press the ESC key, you are presented with a screen that enables you to select which type of installation you want to perform. You can choose to install the full NetBackup appliance installation or a smaller version that excludes the installation of the client packages.

Make your selection and press **Enter** to begin the reimage operation.



- 8 When the installation of the new appliance package is complete, you receive a **Welcome** message in the **JViewer** application window that is similar to the following. Enter the default appliance password (**password**). You are now logged in to the appliance shell menu.

Note: Before you begin the reconfiguration process, you may want to reference the configuration information that you recorded prior to beginning the reimage operation.

```
JViewer[10.81.50.146] - 0 fps
Video Keyboard Mouse Options Device Help
Macros: Ctrl Alt Del Alt Tab

Start Unicode mode done
Setting up (remotefs) network interfaces:
Setting up service (remotefs) network . . . . . done
Starting SSH daemon done
Starting irqbalance done
Starting Name Service Cache Daemon done
Starting mail service (Postfix) done
Starting CRON daemon done
Starting Firewall Initialization (phase 2 of 2) done
Master Resource Control: Running /etc/init.d/after.local done
Master Resource Control: runlevel 3 has been reached
Skipped services in runlevel 3: nfs smbfs splash

Welcome to SUSE Linux Enterprise Server 11 SP1 (x86_64) - Kernel 2.6.32.59-0.3-
default-fsl (tty1).

*****
* Welcome to NetBackup Appliance 2.6 *
*****

admin login...
Password: _
```

- 9 Import the IPsec credentials, **.pfx** files, from the remote computer where you exported them earlier:
 - Open a share from the appliance shell menu as follows:
Main_Menu > Manage > Software > Share Open
The CIFS share **\\<appliance-name>\incoming\patches** and the NFS share **<appliance-name>:/inst/patch/incoming** are now open on this appliance.
 - To move the earlier saved **.pfx** files to the open share location, create and mount a mount point and then move the files as follows:

Windows This example assumes that the Windows system uses Samba.

- Create and mount a mount point as follows:

```
net use
<AnAvailableDriveLetter>:\\<appliance-host>\incoming
patches"
```
- Move the .pfx files back to the appliance as follows:

```
# move /mnt/computer_name/*.pfx
/inst/patch/incoming/
```

UNIX or Linux This example assumes that the UNIX or Linux system uses NFS.

- Create and mount a mount point as follows:

```
# mkdir -p /mnt/computer_name
move <directory where the pfx file was
save>/*.pfx <mounted drive>
```
- Move the .pfx files back to the appliance as follows:

```
mv <local directory where the pfx file was
kept>/*.pfx <mount point>
```

- Import the files by entering the following command:

```
Main_Menu > Network > Security > Import
<yes/no>/inst/patch/incoming
```

Note: If you used a password in Step 1 when you performed the `Export` command, then you must enter the same password when you run the `Import` command.

- Close the share from the appliance shell menu as follows:

```
Main_Menu > Manage > Software > Share Close
```

10 Enter the following command twice to return to the main menu:

```
Return
```

```
Return
```

11 Verify that you are at the main menu.

Navigate to the following topics to reconfigure your specific NetBackup appliance:

See [“Reconfiguring a 52xx master server appliance from the USB drive using the NetBackup Appliance Shell Menu”](#) on page 268.

See [“Reconfiguring a 52xx media server appliance from the USB drive using the NetBackup Appliance Shell Menu”](#) on page 275.

Reconfiguring a 52xx master server appliance from the USB drive using the NetBackup Appliance Shell Menu

The following procedure describes how to reconfigure a 52xx master server appliance from the NetBackup Appliance Shell Menu.

Warning: NetBackup appliances do not support configuring two IP addresses that belong to the same subnet. The appliance runs on the Linux operating system and this type of networking is a current limitation. Each bond that you create must use an IP address that belongs to a different subnet.

Note: You cannot remove an IP address if the appliance host name resolves to that IP address.

Caution: Before or immediately after initial configuration, you must change the default maintenance password (`P@ssw0rd`) for your appliance. This password must be provided to technical support in case you need future troubleshooting assistance. You must change the maintenance password through the NetBackup Appliance Shell Menu with one of the following commands: `Main > Settings > Password maintenance` or `Main > Support > Maintenance > passwd`. For complete information, see the *Symantec NetBackup Appliance Command Reference Guide*.

To reconfigure a 52xx master server appliance from the USB drive using the NetBackup Appliance Shell Menu

- 1 If you cannot log into the appliance, insert the USB drive into the appliance, turn on the appliance, and then proceed to Step 4.

If you can log into the appliance and you can access the NetBackup Appliance Shell Menu, export (copy) and move the IPsec credentials to a remote drive using the following steps and then continue with Step 2.

- Open a CIFS and an NFS share with the following command:
`Manage > Software > Share Open`
- To export (copy) the IPsec credentials, enter the following command:
`Network > Security > Export <yes/no> /inst/patch/incoming`
Where `<yes/no>` is for whether you want password protection.

Note: The output from the `export` command creates a backup `.pfx` file of the actual certificate. If you select `yes` to use a password, the file name is a number with the `.pfx` extension (`nnnnnnnn.pfx`). If you select `no` for no password, a period precedes the file name (`.nnnnnnnn.pfx`).

If you use a password, retain the name of the password to use when you run the `Import` command later in this procedure.

- To move the `.pfx` files into a local directory on a remote computer, create and mount a mount point and then move the files as follows:

Windows	<p>This example assumes that the Windows system uses Samba.</p> <ul style="list-style-type: none"> ■ Create and mount a mount point as follows: <pre>net use <AnAvailableDriveLetter>: \\<appliance-host>\incoming patches"</pre> ■ Copy the <code>.pfx</code> file as follows: <pre># copy /inst/patch/incoming/*.pfx /mnt/<computer_name></pre>
UNIX or Linux	<p>This example assumes that the UNIX or Linux system uses NFS.</p> <ul style="list-style-type: none"> ■ Create and mount a mount point as follows: <pre># mkdir -p /mnt/<computer_name> # mount -t nfs <computer_name>:/<share_name> /mnt/<computer_name></pre> ■ Copy the <code>.pfx</code> file as follows: <pre># cp /inst/patch/incoming/*.pfx /mnt/<computer_name></pre>

- 2 Insert the USB drive into an appliance USB port on the media server appliance that you want to reimage.

- 3 From the **Main_Menu > Network** view, enter the following command to configure the IP address of a single network that you want your appliance to connect to.

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

Where *IPAddress* is the new IP address, *Netmask* is the netmask, and *GatewayIPAddress* is the default gateway for the interface. The `[InterfaceNames]` option is optional.

The *IP Address* or the *Gateway IP Address* can be an IPv4 or IPv6 address. Only global-scope and unique-local IPv6 addresses are allowed.

Remember that you should not use both IPv4 and IPv6 address in the same command. For example, you cannot use `Configure 9ffe::9 255.255.255.0 1.1.1.1..` You should use `Configure 9ffe::46 64 9ffe::49 eth1`

See [“About IPv4-IPv6-based network support”](#) on page 61.

If you want to configure multiple networks you must first configure the IP address of each network that you want to add. Then you configure the Gateway address for each network you added. You must make sure that you add the default Gateway address first. Use the following two commands:

Configure the IP address of each network

Use either of the following commands depending on whether you want to configure an IPv4 or an IPv6 address for the network interface:

To configure the IPv4 address of a network interface:

```
IPv4 IPAddress Netmask [InterfaceName]
```

Where *IPAddress* is the new IP address, *Netmask* is the netmask, and `[InterfaceName]` is optional.

Repeat this command for each IP address that you want to add.

To configure the IPv6 address of a network interface:

```
IPv6 <IP Address> <Prefix> [InterfaceNames]
```

Where *IPAddress* is the IPv6 address, *Prefix* is the prefix length, and `[InterfaceName]` is optional.

Configure the gateway address for each network that you added

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

Where *GatewayIPAddress* is the gateway for the interface and *TargetNetworkIPAddress*, *Netmask*, and *InterfaceName* are optional. Repeat this command to add the gateway to all of the destination networks.

The *Gateway IP Address* or the *TargetNetworkIPAddress* can be an IPv4 or an IPv6 address.

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

- 4 From the **Main_Menu > Network** view, use the following command to set the appliance DNS domain name.

Note: If you do not use DNS, then you can proceed to Step 7.

```
DNS Domain Name
```

Where *Name* is the new domain name for the appliance.

- 5 From the **Main_Menu > Network** view, use the following command to add the DNS name server to your appliance configuration.

```
DNS Add NameServer IPAddress
```

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

The address can be either IPv4 or IPv6. Only global-scope and unique-local IPv6 addresses are allowed.

See [“About IPv4-IPv6-based network support”](#) on page 61.

To add multiple IP addresses, use a comma to separate each address and no space.

- 6 From the **Main_Menu > Network** view, use the following command to add a DNS search domain to your appliance configuration so the appliance can resolve the host names that are in different domains:

```
DNS Add SearchDomain SearchDomain
```

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

- 7 This step is optional. It lets you add the IP addresses of other hosts in the appliance hosts file.

From the **Main_Menu > Network** view, use the following command to add host entries to the hosts file on your appliance.

```
Hosts Add IPAddress FQHN ShortName
```

Where *IPAddress* is the IPv4 or IPv6 address, *FQHN* is the fully qualified host name, and *ShortName* is the short host name.

See [“About IPv4-IPv6-based network support”](#) on page 61.

- 8 From the **Main_Menu > Network** view, use the following command to set the host name for your appliance.

```
Hostname Set Name
```

Where *Name* is the fully qualified host name.

With this step, NetBackup is re-configured to operate with the new host name. This process may take a while to complete.

For the command `Hostname set` to work, at least one IPv4 address is required. For example, you may want to set the host name of a specific host to v46. To do that, first ensure that the specific host has at least an IPv4 address and then run the following command.

```
Main_Menu > Network > Hostname set v46
```

- 9 From the **Main_Menu > Settings** view, use the following commands to enter the SMTP server name and the email addresses for appliance failure alerts.

Enter the SMTP server name `Email SMTP Add smtp [acct] [pass]`

Where *smtp* is the host name of the target SMTP server, *acct* is the account name for authentication to the SMTP server, and *pass* is the password for authentication to the SMTP server.

Enter email addresses

```
Email Software Add eaddr
```

Where *eaddr* is the Email address where you want to receive failure alerts from the appliance.

To enter multiple addresses, separate each address with a semi-colon.

- 10 Set the role for the appliance to a master server.

From the **Main_Menu > Appliance** view, run the following command:

```
Master
```

- 11 If you have a media server that needs reconfiguration, now is the time to configure the master server to communicate with it, then reconfigure your media server.

See [“Configuring a master server to communicate with an appliance media server”](#) on page 273.

See [“Reconfiguring a 52xx media server appliance from the USB drive using the NetBackup Appliance Shell Menu”](#) on page 275.

Configuring a master server to communicate with an appliance media server

Before you configure a reimaged media server appliance, you must ensure that the master server you plan to use with it is configured. That allows for appropriate communication to occur between the master server and the reconfigured media server appliance.

The following procedure describes how to configure a master server to communicate with an appliance media server.

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

- 1 Log in to the master server as the administrator and make sure the name of the media server appliance is added to the master server:

For an appliance master server:

From the NetBackup Appliance Web Console:

- Click **Manage > Additional Servers > Add**.
- In the **Appliance Hostname** field, enter the fully qualified host name (FQHN) of the appliance media server that you want to add.
- Click **Add**.
 If the appliance has more than one host name, you must add all of the names.

From the appliance shell menu:

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

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

 Where *media-server* is the fully qualified host name (FQHN) of the appliance media server that is not yet configured.
 If the appliance has more than one host name, you must add all of the names.

For a traditional NetBackup master server:

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

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

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

- `vnetd: 13724`
 - `bprd: 13720`
 - `PBX: 1556`
 - If the master server is a NetBackup appliance that uses TCP, open the following ports:
80, 5900, and 7578.
- 3 Make sure that the date and time of the media server matches the date and time on the master server. You can use an NTP server or set the time manually.
- See [“Reconfiguring a 52xx media server appliance from the USB drive using the NetBackup Appliance Shell Menu”](#) on page 275.

Reconfiguring a 52xx media server appliance from the USB drive using the NetBackup Appliance Shell Menu

The following procedure describes how to reconfigure a 52xx media server appliance from the NetBackup Appliance Shell Menu.

Warning: NetBackup appliances do not support configuring two IP addresses that belong to the same subnet. The appliance runs on the Linux operating system and this type of networking is a current limitation. Each bond that you create must use an IP address that belongs to a different subnet.

Note: You cannot remove an IP address if the appliance host name resolves to that IP address.

Caution: Before or immediately after initial configuration, you must change the default maintenance password (`P@ssw0rd`) for your appliance. This password must be provided to technical support in case you need future troubleshooting assistance. You must change the maintenance password through the NetBackup Appliance Shell Menu with one of the following commands: `Main > Settings > Password maintenance` or `Main > Support > Maintenance > passwd`. For complete information, see the *Symantec NetBackup Appliance Command Reference Guide*.

To reconfigure a 52xx media server appliance from the USB drive using the NetBackup Appliance Shell Menu

- 1 If you cannot log into the appliance, insert the USB drive into the appliance, turn on the appliance, and then proceed to Step 4.

If you can log into the appliance and you can access the NetBackup Appliance Shell Menu, export (copy) and move the IPsec credentials to a remote drive using the following steps and then continue with Step 2.

- Open a CIFS and an NFS share with the following command:

```
Manage > Software > Share Open
```

- To export (copy) the IPsec credentials, enter the following command:

```
Network > Security > Export <yes/no> /inst/patch/incoming
```

Where <yes/no> is for whether you want password protection.

Note: The output from the `export` command creates a backup `.pfx` file of the actual certificate. If you select `yes` to use a password, the file name is a number with the `.pfx` extension (nnnnnnnn.pfx). If you select `no` for no password, a period precedes the file name (.nnnnnnnn.pfx).

If you use a password, retain the name of the password to use when you run the `Import` command later in this procedure.

- To move the `.pfx` files into a local directory on a remote computer, create and mount a mount point and then move the files as follows:

Windows

This example assumes that the Windows system uses Samba.

- Create and mount a mount point as follows:

```
net use <AnAvailableDriveLetter>:  
\\<appliance-host>\incoming patches"
```

- Copy the `.pfx` file as follows:

```
# copy /inst/patch/incoming/*.pfx  
/mnt/<computer_name>
```

UNIX or Linux

This example assumes that the UNIX or Linux system uses NFS.

- Create and mount a mount point as follows:

```
# mkdir -p /mnt/<computer_name>  
# mount -t nfs <computer_name>:/<share_name>  
/mnt/<computer_name>
```

- Copy the `.pfx` file as follows:

```
# cp /inst/patch/incoming/*.pfx  
/mnt/<computer_name>
```

- 2 Insert the USB drive into an appliance USB port on the media server appliance that you want to reimage.

- 3 From the **Main_Menu > Network** view, enter the following command to configure the IP address of a single network that you want your appliance to connect to.

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

Where *IPAddress* is the new IP address, *Netmask* is the netmask, and *Gateway/IPAddress* is the default gateway for the interface. The [*InterfaceNames*] option is optional.

The *IP Address* or the *Gateway IP Address* can be an IPv4 or IPv6 address. Only global-scope and unique-local IPv6 addresses are allowed.

Remember that you should not use both IPv4 and IPv6 address in the same command. For example, you cannot use `Configure 9ffe::9 255.255.255.0 1.1.1.1..` You should use `Configure 9ffe::46 64 9ffe::49 eth1`

See [“About IPv4-IPv6-based network support”](#) on page 61.

If you want to configure multiple networks you must first configure the IP address of each network that you want to add. Then you configure the Gateway address for each network you added. You must make sure that you add the default Gateway address first. Use the following two commands:

Configure the IP address of each network	Use either of the following commands depending on whether you want to configure an IPv4 or an IPv6 address for the network interface:
--	---

To configure the IPv4 address of a network interface:

```
IPv4 IPAddress Netmask [InterfaceName]
```

Where *IPAddress* is the new IP address, *Netmask* is the netmask, and [*InterfaceName*] is optional.

Repeat this command for each IP address that you want to add.

To configure the IPv6 address of a network interface:

```
IPv6 <IP Address> <Prefix> [InterfaceNames]
```

Where *IPAddress* is the IPv6 address, *Prefix* is the prefix length, and [*InterfaceName*] is optional.

Configure the gateway address for each network that you added

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

Where *GatewayIPAddress* is the gateway for the interface and *TargetNetworkIPAddress*, *Netmask*, and *InterfaceName* are optional. Repeat this command to add the gateway to all of the destination networks.

The *Gateway IP Address* or the *TargetNetworkIPAddress* can be an IPv4 or an IPv6 address.

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

- 4 From the **Main_Menu > Network** view, use the following command to set the appliance DNS domain name.

Note: If you do not use DNS, then you can proceed to Step 7.

```
DNS Domain Name
```

Where *Name* is the new domain name for the appliance.

- 5 From the **Main_Menu > Network** view, use the following command to add the DNS name server to your appliance configuration.

```
DNS Add NameServer IPAddress
```

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

The address can be either IPv4 or IPv6. Only global-scope and unique-local IPv6 addresses are allowed.

See [“About IPv4-IPv6-based network support”](#) on page 61.

To add multiple IP addresses, use a comma to separate each address and no space.

- 6 From the **Main_Menu > Network** view, use the following command to add a DNS search domain to your appliance configuration so the appliance can resolve the host names that are in different domains:

```
DNS Add SearchDomain SearchDomain
```

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

- 7 This step is optional. It lets you add the IP addresses of other hosts in the appliance hosts file.

From the **Main_Menu > Network** view, use the following command to add host entries to the hosts file on your appliance.

```
Hosts Add IPAddress FQHN ShortName
```

Where *IPAddress* is the IPv4 or IPv6 address, *FQHN* is the fully qualified host name, and *ShortName* is the short host name.

See [“About IPv4-IPv6-based network support”](#) on page 61.

- 8 From the **Main_Menu > Network** view, use the following command to set the host name for your appliance.

```
Hostname Set Name
```

Where *Name* is the fully qualified host name.

With this step, NetBackup is re-configured to operate with the new host name. This process may take a while to complete.

For the command `Hostname set` to work, at least one IPv4 address is required. For example, you may want to set the host name of a specific host to v46. To do that, first ensure that the specific host has at least an IPv4 address and then run the following command.

```
Main_Menu > Network > Hostname set v46
```

- 9 From the **Main_Menu > Settings** view, use the following commands to enter the SMTP server name and the email addresses for appliance failure alerts.

Enter the SMTP server name `Email SMTP Add smtp [acct] [pass]`

Where *smtp* is the host name of the target SMTP server, *acct* is the account name for authentication to the SMTP server, and *pass* is the password for authentication to the SMTP server.

Enter email addresses

```
Email Software Add eaddr
```

Where *eaddr* is the Email address where you want to receive failure alerts from the appliance.

To enter multiple addresses, separate each address with a semi-colon.

10 Set the role for the appliance to a media server.

Note: Before you configure this appliance as a media server, you must add the name of this appliance to the master server that must work with this appliance.

From the **Main_Menu > Appliance** view, run the following command:

```
Media MasterServer
```

Where *MasterServer* is either a standalone master server, a multihomed master server, or a clustered master server. The following defines each of these scenarios:

Standalone master server	This scenario shows one master server host name. This name does not need to be a fully qualified name as long as your appliance recognizes the master server on your network. The following is an example of how the command would appear.
--------------------------	--

```
Media MasterServerName
```

Multihomed master server	In this scenario, the master server has more than one host name that is associated with it. You must use a comma as a delimiter between the host names. The following is an example of how the command would appear.
--------------------------	--

```
Media MasterNet1Name,MasterNet2Name
```

Clustered master server	In this scenario, the master server is in a cluster. Symantec recommends that you list the cluster name first, followed by the active node, and then the passive nodes in the cluster. This list requires you to separate the node names with a comma. The following is an example of how the command would appear.
-------------------------	---

```
Media  
MasterClusterName,ActiveNodeName,PassiveNodeName
```


Multihomed clustered master server In this scenario, the master server is in a cluster and has more than one host name that is associated with it. Symantec recommends that you list the cluster name first, followed by the active node, and then the passive nodes in the cluster. This list requires you to separate the node names with a comma. The following is an example of how the command would appear.

```
Media MasterClusterName,ActiveNodeName,  
PassiveNodeName,MasterNet1Name,MasterNet2Name
```

To prevent any future issues, when you perform the appliance role configuration, Symantec recommends that you provide all of the associated master server names.

- 11 The configuration process determines whether NetBackup storage objects have been detected. You must decide if you want to preserve any preexisting storage objects.

If storage objects are detected, you receive the following message:

```
NetBackup storage objects have been detected that belong to this  
media server node. You have an option to clean up (delete and  
recreate) or preserve any preexisting NetBackup storage objects  
that are solely owned by this appliance node.
```

If you choose 'yes' the following occurs:

1. The NetBackup catalog images owned by this node are expired, if applicable.
2. The storage servers, disk pools, and storage units are cleaned up on the master server.

Whether you chose 'yes' or 'no', the backup data on the disk is preserved.

If you want to remove the backup data, run 'Support->Storage Reset' before you proceed.

```
>> Do you want to clean up existing storage objects? [yes,no]
```

If you enter `Yes` the following occurs:

- The NetBackup catalog images owned by this media server compute node are expired.

- The storage servers, disk pools, and storage units are cleaned up on the master server.
- The backup data on the disk is preserved.

If you choose `No` the following occurs:

- NetBackup catalog images are retained.
- The backup data on the disk is preserved.

Note: If you want to remove the backup data, run the following command from the NetBackup Appliance Shell Menu before you proceed.

```
Main_Menu > Support > Storage Reset
```

- 12 Enter the storage configuration properties to configure storage pools for AdvancedDisk, for Deduplication (MSDP), or both.

When you configure storage pool sizes after a reimage process, the default storage sizes are displayed. If you adjusted the storage pool sizes before the reimage, those new storage pool sizes become the new default values that appear. However, the default disk pool name and the storage unit name that appear are the same default names as in the initial configuration process. If you changed the disk pool name and the storage unit name before the reimage, you must enter the names that you had chosen again during the reconfiguration process.

Note: To skip this step enter 0 when you are prompted for the size. This also deletes any existing data for that partition.

If you enter a 0 when you are prompted and a storage partition does not exist, then a partition is not created. If you enter 0 and a partition already exists then the partition is deleted and any existing data is also deleted.

To configure an AdvancedDisk storage pool provide the following information:

- AdvancedDisk storage pool size in GB/TB (e.g., 50 GB)
[1.6395 GB..51.8 TB]:
- AdvancedDisk diskpool name:
- AdvancedDisk storage unit name:

Note: You may need to reference the configuration notes that you recorded before starting this reimaging procedure so you can recreate the same storage pool configurations.

- 13** The configuration process asks if you want to edit the storage configuration. The greater the total storage size that you specify, the longer it takes to complete the storage configuration.

```
Do you want to edit the storage configuration? [yes,no]: no
```

Call Home upload information

This appendix includes the following topics:

- [About the appliance hardware information that is uploaded](#)
- [About the storage shelf information that is uploaded](#)

About the appliance hardware information that is uploaded

Call Home is designed to upload appliance-specific and the customer-specific information to a Symantec Call Home server. The Symantec Technical Support uses this information to provide assistance to you. The hardware information that is gathered covers the appliance and any storage shelves (or enclosures) that are configured.

The following is an example of the appliance hardware information that is bundled together into a report and uploaded to the Call Home server.

The following data is uploaded for an appliance:

Disk Information										
ID	Slot	Status	Foreign	Firmware	Serial	Capacity	Type	Enclosure	State	Acknowledge
	Number		State	Version	Number			ID		
1	0	Online,	None	0002	Z1N28E94	930.390GB	SAS	99	OK	N/A
		Spun Up								

2	1	Online,	None	0002	Z1N2BLFK	930.390GB	SAS	99	OK	N/A
		Spun Up								
3	0	Online,	None	0002	Z1N2BM45	930.390GB	SAS	252	OK	N/A
		Spun Up								
4	1	Online,	None	0002	Z1N2BM5H	930.390GB	SAS	252	OK	N/A
		Spun Up								
5	2	Online,	None	0002	Z1N2BMLK	930.390GB	SAS	252	OK	N/A
		Spun Up								
6	3	Online,	None	0002	Z1N28FTX	930.390GB	SAS	252	OK	N/A
		Spun Up								
7	4	Online,	None	0002	Z1N28KLJ	930.390GB	SAS	252	OK	N/A
		Spun Up								
8	5	Online,	None	0002	Z1N2BLMA	930.390GB	SAS	252	OK	N/A
		Spun Up								
9	6	Online,	None	0002	Z1N28E9Z	930.390GB	SAS	252	OK	N/A
		Spun Up								
10	7	Hotspare,	None	0002	Z1N2BME1	930.390GB	SAS	252	OK	N/A
		Spun down								

RAID Information

ID	Name	Status	Capacity	Type	Disks	Write Policy	Enclosure ID	All hotspares available	State	Acknowledge
1	VD-0	Optimal	4.541TB	RAID-6	3 4 5	WriteBack	252	yes	OK	N/A
2	VD-0	Optimal	35.469TB	RAID-6	7 8 9	WriteBack	24	no	Warning	No

Fan Information						
ID	Name	Status	Speed	LowWaterMark	State	Acknowledge
1	System Fan 1	OK	8281.00 RPM	1715.00 RPM	OK	N/A
2	System Fan 2	OK	8379.00 RPM	1715.00 RPM	OK	N/A
3	System Fan 3	OK	8183.00 RPM	1715.00 RPM	OK	N/A
4	System Fan 4	OK	8183.00 RPM	1715.00 RPM	OK	N/A
5	System Fan 5	OK	7987.00 RPM	1715.00 RPM	OK	N/A
Power Supply Information						
ID	Status	Wattage	HighWaterMark	State	Acknowledge	
1	Power Supply AC lost	0.00 Watts	920.00 Watts	Warning	No	
2	Present	268.00 Watts	920.00 Watts	OK	N/A	
CPU Information						
ID	Status	Voltage	LowWaterMark	HighWaterMark	State	Acknowledge
1	OK	0.95 Volts	0.55 Volts	1.51 Volts	OK	N/A
2	OK	0.77 Volts	0.55 Volts	1.51 Volts	OK	N/A
Temperature Information						
ID	Type	Temperature	LowWaterMark	HighWaterMark	State	Acknowledge
1	Intake Vent	27.00	0.00 degrees	65.00 degrees	OK	N/A
	Temperature	degrees C	C	C		
2	Outtake Vent	43.00	0.00 degrees	85.00 degrees	OK	N/A
	Temperature	degrees C	C	C		
3	P1 DTS Therm Mgn	-48.00	-128.00	-15.00	OK	N/A
		degrees C	degrees C	degrees C		

4	P2 DTS Therm Mgn	-47.00	-128.00	-15.00	OK	N/A
		degrees C	degrees C	degrees C		

FibreChannel HBA Information

ID	Status	Mode	PCI Slot	Port	WWN	Speed	Remote Port	State	Acknowledge
1	Linkdown	Initiator*	Slot5	21:00:00:24:FF:46:88:00	gbit/s	/-		OK	N/A
2	Linkdown	Initiator	Slot5	21:00:00:24:FF:46:88:01	gbit/s	/-		OK	N/A
3	Linkdown	Initiator*	Slot6	21:00:00:24:FF:46:84:80	gbit/s	/-		OK	N/A
4	Linkdown	Initiator	Slot6	21:00:00:24:FF:46:84:81	gbit/s	/-		OK	N/A
5	Linkdown	Initiator	Slot4	21:00:00:24:FF:46:82:3E	gbit/s	/-		OK	N/A
6	Linkdown	Initiator	Slot4	21:00:00:24:FF:46:82:3F	gbit/s	/-		OK	N/A
7	Linkdown	Initiator	Slot2	21:00:00:24:FF:46:8A:28	gbit/s	/-		OK	N/A
8	Linkdown	Initiator	Slot2	21:00:00:24:FF:46:8A:29	gbit/s	/-		OK	N/A

PCI Information

ID	Slot	Details	State	Acknowledge
1	1	RAID bus controller	OK	N/A
2	2	QLE2562	OK	N/A
3	3	Intel X520	OK	N/A
4	4	QLE2562	OK	N/A
5	5	QLE2562	OK	N/A
6	6	QLE2562	OK	N/A

Network Card Information									
ID	Port	Card Model	Serial Number	Port	MAC Address	Link	State	Acknow-	
	Name			Speed		State		ledge	
1	eth0	BaseBoard	8e-22-59-ff-ff-67-1e-00	1Gb/s	00:1E:67:59:22:8E	UNPLUGGED	OK	N/A	
2	eth1	BaseBoard	8e-22-59-ff-ff-67-1e-00	1Gb/s	00:1E:67:59:22:8F	UNPLUGGED	OK	N/A	
3	eth2	BaseBoard	8e-22-59-ff-ff-67-1e-00	1Gb/s	00:1E:67:59:22:90	PLUGGED	OK	N/A	
4	eth3	BaseBoard	8e-22-59-ff-ff-67-1e-00	1Gb/s	00:1E:67:59:22:91	UNPLUGGED	OK	N/A	
5	eth4	Intel_X520	f4-d3-51-ff-ff-67-1e-00	10Gb/s	00:1E:67:51:D3:F5	UNPLUGGED	OK	N/A	
6	eth5	Intel_X520	f4-d3-51-ff-ff-67-1e-00	10Gb/s	00:1E:67:51:D3:F4	UNPLUGGED	OK	N/A	
7	eth6	Intel_X520	2c-c3-2a-ff-ff-ba-e2-90	10Gb/s	90:E2:BA:2A:C3:2C	UNPLUGGED	OK	N/A	
8	eth7	Intel_X520	2c-c3-2a-ff-ff-ba-e2-90	10Gb/s	90:E2:BA:2A:C3:2D	UNPLUGGED	OK	N/A	

Adapter Information										
ID	Adapter	Adapter	Learn	Charge	Charging	Voltage	Temperature	Manufacturing	State	Acknow-

	model	Status	Cycle		Status			Date		ledge
			active							

	Intel®)									
	Integrated									
2	RAID	OK	N/A	326 J	None	OK	OK	May 11, 2012	OK	N/A
	Module									
	RMS25CB080									

	Intel ®)									
1	RAID	OK	N/A	331 J	None	OK	OK	Jun 15, 2012	OK	N/A
	Controller									
	RS25SB008									

Partition Information										

ID	Partition	Total	Used	Status	State	Acknowledge				

1	MSDP	37.2 TB	1 %	Optimal	OK	N/A				

2	Catalog	251 GB	1 %	Optimal	OK	N/A				

3	Configuration	25 GB	2 %	Optimal	OK	N/A				

4	AdvancedDisk	1 TB	1 %	Optimal	OK	N/A				

5	System	117 GB	6 %	Optimal	OK	N/A				

6	Log	367 GB	1 %	Optimal	OK	N/A				

MSDP Information										

ID	Queue Size	Oldest tlog	Creation Date	State	Acknowledge					

1	0	N/A		OK	N/A					

About the storage shelf information that is uploaded

The following is an example of storage shelf information that is uploaded to the Call Home server.

Time Monitoring Ran: Thu Aug 22 2013 05:06:20 PDT

StorageShelf 1 Disk Information										
ID	Slot	Status	Foreign	Firmware	Serial	Capacity	Type	StorageShelf	State	Acknowledge
	Number		State	Version	Number			ID		
1	1	Online, Spun Up	None	A222	YVH54VTD	2.727TB	SAS	24	OK	N/A
2	2	Online, Spun Up	None	A222	YVH4Y9DD	2.727TB	SAS	24	OK	N/A
3	3	Online, Spun Up	None	A222	YVH4ZGND	2.727TB	SAS	24	OK	N/A
4	4	Online, Spun Up	None	A222	YVH4V4WD	2.727TB	SAS	24	OK	N/A
5	5	Online, Spun Up	None	A222	YVH4YAPD	2.727TB	SAS	24	OK	N/A
6	6	Online, Spun Up	None	A222	YVH4Y7YD	2.727TB	SAS	24	OK	N/A
7	7	Online, Spun Up	None	A222	YVH100ZD	2.727TB	SAS	24	OK	N/A
8	8	Online, Spun Up	None	A222	YVH54W2D	2.727TB	SAS	24	OK	N/A
9	9	Online, Spun Up	None	A222	YVH4YA2D	2.727TB	SAS	24	OK	N/A
10	10	Online, Spun Up	None	A222	YVH4W6UD	2.727TB	SAS	24	OK	N/A
11	11	Online, Spun Up	None	A222	YVH4Y8RD	2.727TB	SAS	24	OK	N/A
12	12	Online, Spun Up	None	A222	YVH4Y8BD	2.727TB	SAS	24	OK	N/A

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										
13 13	Online,	None	A222	YVH101BD 2.727TB	SAS	24		OK	N/A	
	Spun Up									
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										
8 8	Online,	None	A222	YVH54W2D 2.727TB	SAS	24		OK	N/A	
	Spun Up									
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										
9 9	Online,	None	A222	YVH4YA2D 2.727TB	SAS	24		OK	N/A	
	Spun Up									
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										
10 10	Online,	None	A222	YVH4W6UD 2.727TB	SAS	24		OK	N/A	
	Spun Up									
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										
11 11	Online,	None	A222	YVH4Y8RD 2.727TB	SAS	24		OK	N/A	
	Spun Up									
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										
12 12	Online,	None	A222	YVH4Y8BD 2.727TB	SAS	24		OK	N/A	
	Spun Up									
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										
13 13	Online,	None	A222	YVH101BD 2.727TB	SAS	24		OK	N/A	
	Spun Up									
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										
14 14	Online,	None	A222	YVH4Y8PD 2.727TB	SAS	24		OK	N/A	
	Spun Up									
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										
15 15	Online,	None	A222	YVGPVS1D 2.727TB	SAS	24		OK	N/A	
	Spun Up									
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										
16 16	Hotspare,	None	A222	YVGSU6GD 2.727TB	SAS	24		OK	N/A	
	Spun down									
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										
StorageShelf 1 Fan Information										
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										
ID	Status		Speed	LowWaterMark		State	Acknowledge			
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										
1	Device Present		3260 RPM	2000 RPM		OK	N/A			
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										
2	Device Present		3260 RPM	2000 RPM		OK	N/A			
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										
3	Device Present		3260 RPM	2000 RPM		OK	N/A			
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										
4	Device Present		3160 RPM	2000 RPM		OK	N/A			
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										

StorageShelf 1 Power Supply Information					
+-----+					
ID	Status		State		Acknowledge
-----+					
1	Presence detected		OK		N/A
-----+					
2	Unrecoverable		Warning		No
+-----+					
StorageShelf 1 Temperature Information					
+-----+					
ID	Type		Temperature		HighWaterMark
-----+					
1	Backplane Temp 1		30 degrees C		51 degrees C
-----+					
2	Backplane Temp 2		31 degrees C		51 degrees C
+-----+					
+-----+					

Fibre Channel and Fibre Transport connectivity

This appendix includes the following topics:

- [About the card slots on NetBackup 52xx series appliances](#)
- [About Fibre Channel port configuration options for the NetBackup 52xx appliances](#)
- [About NetBackup SAN Client and Fibre Transport](#)
- [About the NetBackup appliance as a VMware backup host](#)
- [About backup to tape support for NetBackup appliances](#)

About the card slots on NetBackup 52xx series appliances

The NetBackup 5200 appliance contains vertical card slots for PCI expansion.

The NetBackup 5220 and 5230 appliances contain horizontal card slots for PCI expansion. The following diagrams show the card slot locations on each appliance.

Figure B-1 NetBackup 5200 and 5020 PCI expansion slots

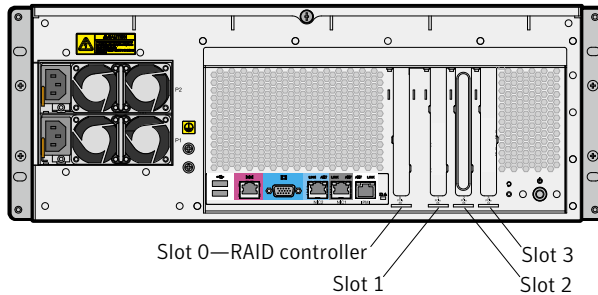


Figure B-2 NetBackup 5220 PCI expansion slots

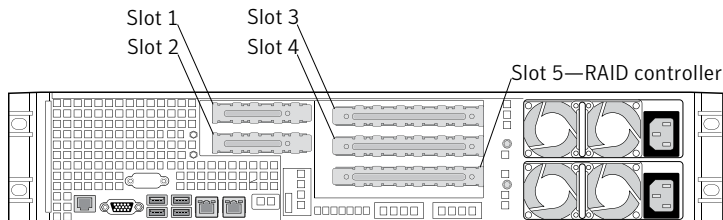
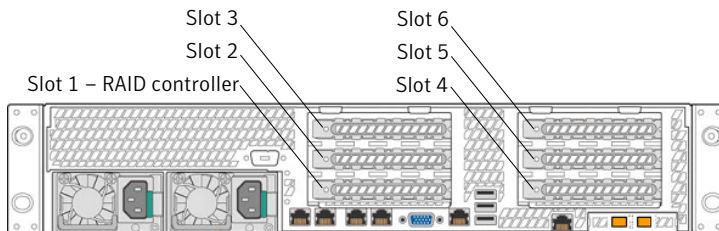


Figure B-3 NetBackup 5230 PCI expansion slots



The FC HBA capability varies for each appliance series.

The following describes the FC HBA capability for the NetBackup 52xx series and the 50xx series appliances.

Table B-1 FC HBA capability for NetBackup appliances

Appliance model	FC HBA capability
5200	Slot 3 - FC HBA for Tape Out or NetBackup for VMware (4GB/s)
5220	<ul style="list-style-type: none"> ■ A series Not available ■ B series Slot 3 - FC HBA for Tape Out or NetBackup for VMware (8GB/s) ■ C series Slot 3 - FC HBA for Tape Out or NetBackup for VMware (8GB/s) ■ D and E series Slots 2 and 4 - FC HBA for SAN Client/Fibre Transport, Optimized duplication to a NetBackup 5020, or NetBackup for VMware (8GB/s) Slot 3 - FC HBA for Tape Out or NetBackup for VMware (8GB/s) <p>Note: Optimized duplication between two NetBackup 52xx series appliances using Fibre Channel is not currently supported.</p>

Table B-1 FC HBA capability for NetBackup appliances (*continued*)

Appliance model	FC HBA capability
5230	<ul style="list-style-type: none"> ■ A series Not available ■ B series and C series Slot 4 - FC HBA for VMware, Optimized duplication over Fibre Channel only to a 5020 or 5030, connectivity to Tape Library, Optimized duplication to a NetBackup 5020 or 5030, or NetBackup for VMware (8GB/s). FC for SAN client is not supported. ■ D series Slots 5 and 6 - FC HBAs support Fibre Transport Media Server (FTMS). Port 1 of the FC HBA in these slots must be configured for the Target mode. Ports in slots 2 and 4 can be used for Optimized duplication over Fibre Channel or connectivity to Tape Library and Optimized duplication to a NetBackup 5020 or 5030, or NetBackup for VMware (8GB/s). If FTMS is not configured, FC HBAs (slots 2,4,5,6) are in Initiator mode. ■ E series Slots 5 and 6 - FC HBAs support Fibre Transport Media Server (FTMS). Port 1 of the FC HBA in these slots must be configured for the Target mode. Ports in slots 2 and 4 can be used for Optimized duplication over Fibre Channel or connectivity to Tape Library, Optimized duplication to a NetBackup 5020 or 5030, or NetBackup for VMware (8GB/s). If FTMS is not configured, all FC HBAs (slots 2,3,4,5,6) are in Initiator mode. <p>Note: FTMS is not supported for models A, B and, C in a 5230 NetBackup Appliance.</p> <p>Further, Optimized duplication between two NetBackup 52xx series appliances using Fibre Channel is not currently supported.</p>
5020	<p>Slots 1 and 3 - FC HBA (4GB/s)</p> <p>Note: Optimized duplication between NetBackup 5020 and 52xx series appliances using Fibre Channel is not currently supported.</p>
5030	<p>Slots 2 and 5 - FC HBA (8GB/s)</p> <p>Note: Optimized duplication between NetBackup 5030 and 52xx series appliances using Fibre Channel is not currently supported.</p>

All FC HBA ports on the NetBackup 52xx series appliances default to the initiator mode. Port 1 can be changed to the target mode by enabling the SAN Client FT media server feature.

See [“Changing the Fibre Transport settings”](#) on page 54.

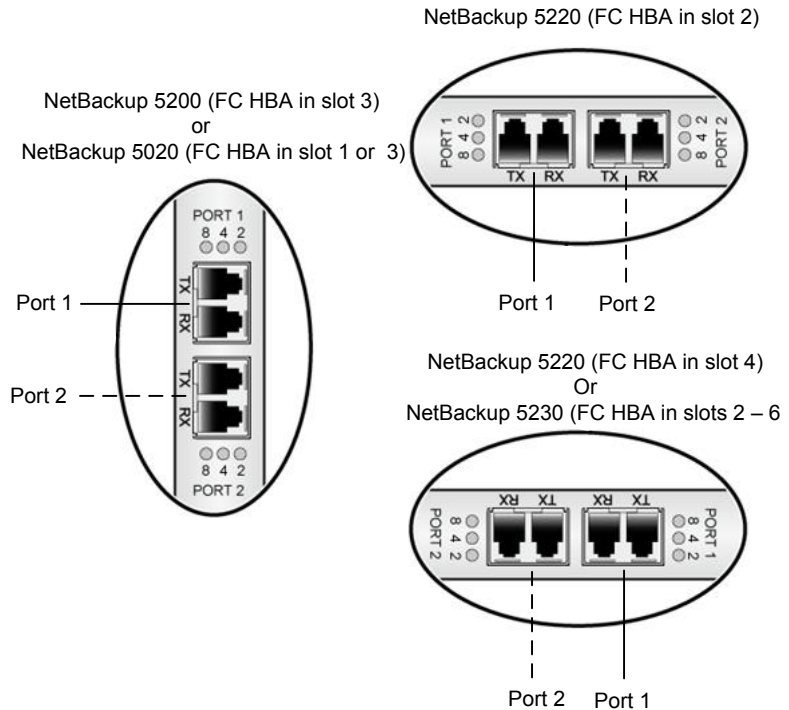
The following describes how to identify the ports on the installed FC HBA cards:

- NetBackup 5200 (slot 3) and NetBackup 5020 (slots 1 and 3)
 Port identification is determined by starting from the top port (Port 1) of the installed card.
- NetBackup 5220 (slot 2)
 Port identification is determined by starting from the left port (Port 1) of the installed card.
- NetBackup 5220 (slot 4)
 Port identification is determined by starting from the right port (Port 1) of the installed card.
- NetBackup 5230 (slots 2 through 6)
 Port identification is determined by starting from the right port (Port 1) of the installed card.

Note: For the 5230, only slots 5-6 support SAN Client target mode configuration for port 1.

The following example shows the port identification for FC HBA cards in the supported slots of each appliance.

Figure B-4 FC HBA slot and port identification



About Fibre Channel port configuration options for the NetBackup 52xx appliances

The NetBackup 52xx appliances support the use of Fibre Channel (FC) with the following features:

- **SAN Client**

This feature provides high-speed backups and restores of NetBackup clients. A SAN client is a special NetBackup client that can back up large amounts of data rapidly over a SAN connection rather than a LAN. The backup and restore traffic occurs over FC, and the NetBackup server and client administration traffic occurs over the LAN.

For information about how to configure a NetBackup 5220 or 5230 to work with the SAN Client feature, refer to the following topics:

See [“About the card slots on NetBackup 52xx series appliances”](#) on page 293.

See [“About NetBackup SAN Client and Fibre Transport”](#) on page 304.

See [“About zoning the SAN for a NetBackup 5220 or 5230 appliance”](#) on page 305.

See [“About Fibre Transport paths for NetBackup appliances”](#) on page 310.

See [“How to determine appliance HBA WWPNS”](#) on page 315.

- Optimized duplication to a NetBackup 5020 or 5030
 Optimized duplication copies the backup images from a NetBackup 5220 or 5230 appliance (source) to a NetBackup 5020 or 5030 appliance (destination). The source and the destination must use the same NetBackup master server. The optimized duplication operation is more efficient than normal duplication because only the unique, deduplicated data segments are transferred. Optimized duplication reduces the amount of data transmission over your network and is a good method to copy your backup images off-site for disaster recovery. For information about how to configure a NetBackup 5220 or 5230 for optimized duplication to a NetBackup 5020 or 5030 deduplication appliance, refer to the following topics:
 See [“About the card slots on NetBackup 52xx series appliances”](#) on page 293.
 See [“About zoning the SAN for a NetBackup 5220 or 5230 appliance”](#) on page 305.
 See [“About Fibre Transport paths for NetBackup appliances”](#) on page 310.
 See [“How to determine appliance HBA WWPNS”](#) on page 315.
 For complete details about the NetBackup 5020 and 5030 appliances, see the *Symantec NetBackup Deduplication Appliance Software Administrator's Guide*.
- NetBackup for VMware
 This feature provides backup and restore of the VMware virtual machines that run on VMware ESX servers. NetBackup for VMware takes advantage of VMware vStorage APIs for data protection. The backup process is off-loaded from the ESX server to a VMware backup host.
 Starting with NetBackup 52xx appliance software version 2.5, you can use the appliance as a VMware backup host. Earlier software versions required a separate Windows system as the host.
 For information about how to configure a NetBackup 5220 or 5230 as a VMware backup host, refer to the following topics:
 See [“About the NetBackup appliance as a VMware backup host”](#) on page 316.
 See [“Notes on the NetBackup appliance as a VMware backup host”](#) on page 316.
 For complete details about NetBackup for VMware and how to configure VMware policies, see the *Symantec NetBackup for VMware Administrator's Guide*.
- Tape out

NetBackup appliances support backups to tape so that you can connect one or more tape libraries to them with FC. An FC host bus adapter (HBA) provides for connection to a TLD tape storage device.

For information about how to configure a NetBackup 5220 or 5230 for backups to tape, refer to the following topics:

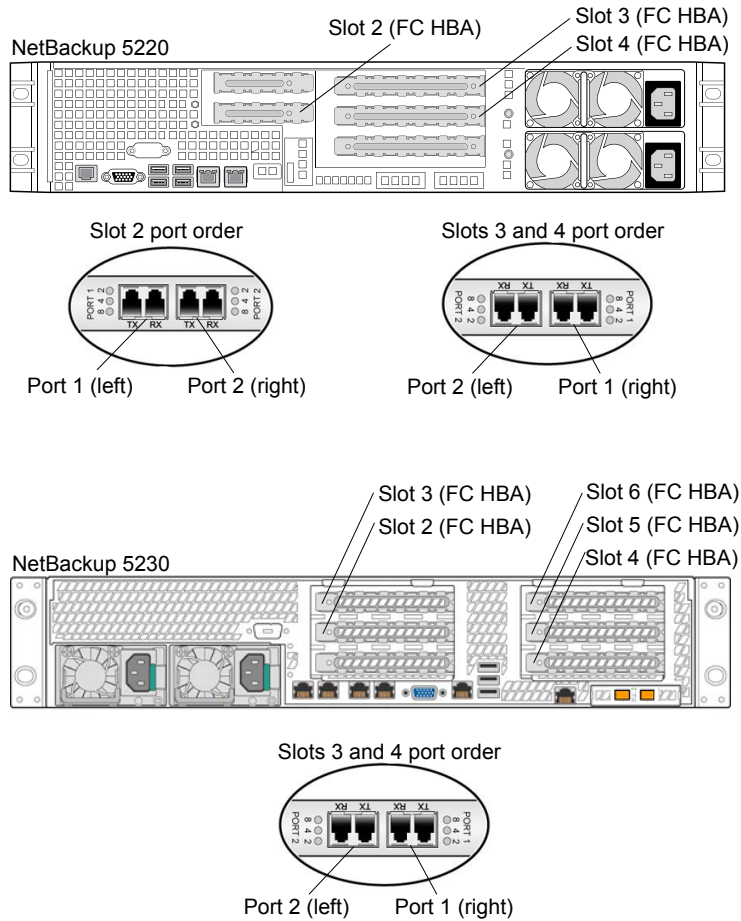
See [“About the card slots on NetBackup 52xx series appliances”](#) on page 293.

See [“About backup to tape support for NetBackup appliances”](#) on page 317.

The following information describes the supported FC HBA slot locations and the port order for the installed FC HBA cards.

On a NetBackup 5230, slots 2 - 6 support FC. The cards are installed in the NetBackup in a horizontal position.

Figure B-5 NetBackup 5220 and 5230 FC HBA slots and ports



The following provides a summary of the supported NetBackup 5220 and 5230 FC options. The 5220 and 5230 slot location and the required port configuration for each option are also included.

Table B-2 Summary of supported NetBackup 5220 and 5230 FC options

FC HBA slot	Supported options and required port configuration
Slot 2 (5220 and 5230)	<p>Port 1</p> <ul style="list-style-type: none"> ■ SAN Client - target <p>Note: All FC HBA ports on the NetBackup 5220 appliance default to the initiator mode. For SAN Client applications, the SAN Client FT media server feature must be enabled. When you enable this feature, Port 1 on the FC HBA cards in slots 2 and 4 is changed to the target mode. To use the SAN Client feature, Port 1 on both of the FC HBA cards in these slots must be used.</p> <p>The ports are in the initiator mode when slot 2 on the NetBackup 5230 appliance is populated with a FC HBA.</p> <p>See "Changing the Fibre Transport settings" on page 54.</p> <ul style="list-style-type: none"> ■ Tape out - initiator ■ NetBackup for VMware - initiator <p>Port 2</p> <ul style="list-style-type: none"> ■ Optimized duplication (FT storage zone) - initiator ■ Tape out - initiator ■ NetBackup for VMware - initiator <p>Use only one option on each port.</p>
Slot 3 (5220 and 5230)	<p>Port 1</p> <ul style="list-style-type: none"> ■ Tape out - initiator ■ NetBackup for VMware - initiator <p>Port 2</p> <ul style="list-style-type: none"> ■ Tape out - initiator ■ NetBackup for VMware - initiator <p>Use only one option on each port.</p>

Table B-2 Summary of supported NetBackup 5220 and 5230 FC options
(continued)

FC HBA slot	Supported options and required port configuration
Slot 4 (5220 and 5230)	<p>Port 1</p> <ul style="list-style-type: none"> ■ SAN Client - target <p>Note: All FC HBA ports on the NetBackup 5220 appliance default to the initiator mode. For SAN Client applications, the SAN Client FT media server feature must be enabled. When you enable this feature, Port 1 on the FC HBA cards in slots 2 and 4 is changed to the target mode. To use the SAN Client feature, Port 1 on both of the FC HBA cards in these slots must be used.</p> <p>The ports are in the initiator mode when slot 4 on the NetBackup 5230 appliance is populated with a FC HBA.</p> <p>See “Changing the Fibre Transport settings” on page 54.</p> <ul style="list-style-type: none"> ■ Tape out - initiator ■ NetBackup for VMware - initiator <p>Port 2</p> <ul style="list-style-type: none"> ■ Optimized duplication (FT storage zone) - initiator ■ Tape out - initiator ■ NetBackup for VMware - initiator <p>Use only one option on each port.</p>
Slots 5 - 6 (5230 only)	<p>Port 1</p> <ul style="list-style-type: none"> ■ SAN Client - target <p>Note: All FC HBA ports on the NetBackup 52xx series appliances default to the initiator mode. For SAN Client applications, the SAN Client FT media server feature must be enabled. When you enable this feature, Port 1 on the FC HBA cards in slots 5 and 6 is changed to the target mode. To use the SAN Client feature, Port 1 on both of the FC HBA cards in these slots must be used.</p> <p>See “Changing the Fibre Transport settings” on page 54.</p> <ul style="list-style-type: none"> ■ Tape out - initiator ■ NetBackup for VMware - initiator <p>Port 2</p> <ul style="list-style-type: none"> ■ Tape out - initiator ■ NetBackup for VMware - initiator <p>Use only one option on each port.</p>

See [“About NetBackup SAN Client and Fibre Transport”](#) on page 304.

See [“About zoning the SAN for a NetBackup 5220 or 5230 appliance”](#) on page 305.

See [“How to determine appliance HBA WWPNs”](#) on page 315.

See [“About Fibre Transport paths for NetBackup appliances”](#) on page 310.

About NetBackup SAN Client and Fibre Transport

SAN Client is a NetBackup optional feature that provides high-speed backups and restores of NetBackup clients.

Note: If you plan to use the SAN Client feature with your appliance and you have SLES 10 clients with QLogic FC HBA cards, a driver update is required. Before you proceed with backups of any SLES 10 clients, Symantec recommends that you first upgrade the QLogic driver in all SLES 10 clients to version 8.03.07.03.10.3-k or later.

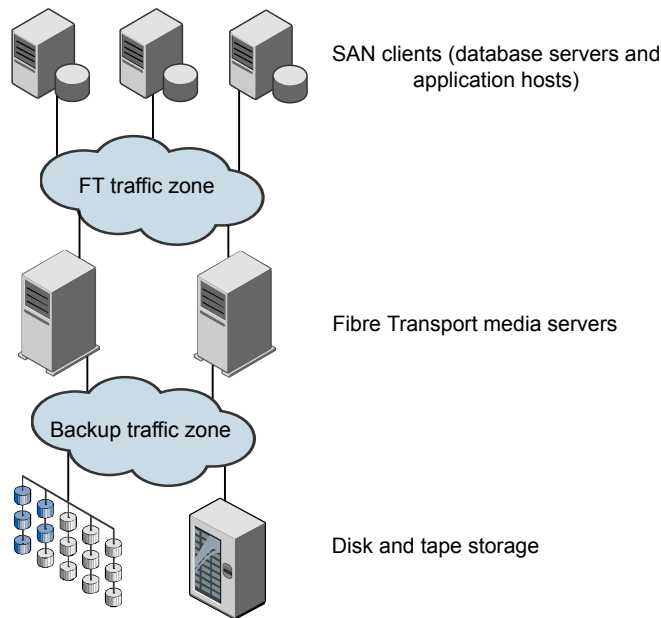
A SAN client is a special NetBackup client that can back up large amounts of data rapidly over a SAN connection rather than a LAN. For example, a database host can benefit from high-speed backups and restores. Fibre Transport is the name of the NetBackup high-speed data transport method that is part of the SAN Client feature.

The backup and restore traffic occurs over Fibre Channel, and the NetBackup server and client administration traffic occurs over the LAN.

For a NetBackup 5220 or 5230 appliance, Fibre Transport also provides high-speed traffic to a NetBackup 5000 series appliance that supports Fibre Transport. The traffic can be for duplication or for backups with the 5000 series appliance functioning as the storage host.

[Figure B-6](#) shows a SAN Client configuration.

Figure B-6 A SAN Client configuration



More information about configuring and using SAN Client is available.

See the [NetBackup SAN Client and Fibre Transport Guide](#).

See “[About the SAN Client license key](#)” on page 305.

See “[About zoning the SAN for a NetBackup 5220 or 5230 appliance](#)” on page 305.

See “[About Fibre Transport paths for NetBackup appliances](#)” on page 310.

About the SAN Client license key

Enter the SAN Client license key on the NetBackup master server.

If the NetBackup Enterprise Media Manager server runs on a host other than the master server, also enter the license key on that host.

If the license key expires or is unavailable (such as in a disaster recovery situation), backups and restores occur over the LAN.

About zoning the SAN for a NetBackup 5220 or 5230 appliance

Before you can configure and use the NetBackup Fibre Transport (FT) mechanism, the SAN must be configured and operational.

The NetBackup appliance supports the following SAN configurations:

- Node port (N_Port) switched configuration.
- Fibre Channel arbitrated loop (FC-AL) configuration.
FC-AL hubs are not supported.

For SAN switched configurations, proper zoning prevents Fibre Transport traffic from using the bandwidth that may be required for other SAN activity. Proper zoning also limits the devices that the host bus adapter (HBA) ports discover; the ports should detect the other ports in their zone only. Without zoning, each HBA port detects all HBA ports from all hosts on the SAN. The potentially large number of devices may exceed the number that the operating system supports.

Instructions for how to configure and manage a SAN are beyond the scope of the NetBackup documentation. However, the following recommendations may help you optimize your SAN traffic.

Table B-3 Best practices for zoning the SAN on a NetBackup 5220 or 5230

Guideline	Description
One initiator per zone, multiple targets acceptable.	<p>Symantec recommends that you create zones with only a single initiator per zone. Multiple targets in a single zone are acceptable, only if all of the targets are similar.</p> <p>Tape target resources should be in separate zones from disk target resources, regardless of initiator. However, both sets of resources may share the same initiator.</p>
Be aware of performance degradation when a port is configured for multiple zones.	<p>If you use a single port as an initiator or a target for multiple zones, this port can become a bottleneck for the overall performance of the system. You must analyze the aggregate required throughput of any part of the system and optimize the traffic flow as necessary.</p>
For fault tolerance, spread connectivity across HBA cards and not ports.	<p>To ensure the availability of system connections, if you incorporate a multi-path approach to common resources, pair ports on separate cards for like zoning. This configuration helps you avoid the loss of all paths to a resource in the event of a card failure.</p>

Table B-3 Best practices for zoning the SAN on a NetBackup 5220 or 5230
(continued)

Guideline	Description
Zone the SAN based on WWN to facilitate zone migrations, if devices change ports.	It is recommended that you perform SAN zoning based on WWN. If switch port configurations or cabling architectures need to change, the zoning does not have to be recreated.

[Table B-4](#) describes the zones you should use for your SAN traffic.

Diagrams that show the zones are available.

See [“About Fibre Transport paths for NetBackup appliances”](#) on page 310.

Note: You must use physical port ID or World Wide Port Name (WWPN) when you specify the HBA ports on NetBackup appliances.

See [“How to determine appliance HBA WWPNs”](#) on page 315.

Table B-4 Appliance zones

Zone	Description
Fibre Transport backup zone	<p>A Fibre Transport backup zone should include only the Fibre Transport traffic between the SAN clients and the appliance.</p> <p>The backup zone should include the following HBA ports:</p> <ul style="list-style-type: none"> ■ The target port of the HBA—connect this port to a Fibre Channel switch port. If you have two HBAs, you can use both of them. The use of two ports provides redundancy. <p>Note: The supplied QLogic FC HBA card in a NetBackup 5220 or 5230 uses a special NetBackup target mode driver for the target port. The target mode driver replaces the default, initiator mode Fibre Channel driver. The target mode driver applies only to the supplied QLogic HBA card.</p> <p>You must define the appliance target port by physical port ID or World Wide Port Name (WWPN). The target mode driver WWPNs are not unique because they are derived from the Fibre Channel HBA WWPN.</p> <ul style="list-style-type: none"> ■ Ports on the SAN client HBAs that connect to the appliance—connect each SAN client HBA port to ports on the same Fibre Channel switch. <p>You can define SAN client ports by either port ID or WWPN. However, if you use one method for all devices, zone definition and management is easier.</p> <p>The ports on the SAN clients use the standard initiator mode driver.</p> <p>To promote multistream throughput, each SAN client should detect all target mode devices of the appliance HBA port or ports in the zone. Each appliance HBA target port exposes two target mode devices.</p> <ul style="list-style-type: none"> ■ Define the zones on the switch so that the client ports and the HBA target ports are in the same zone. <p>Some Symantec appliance models include one or more Fibre Channel HBACards that can be used for Fibre Transport. If your appliance does not include any of these cards, an authorized Symantec representative must install and configure an approved FC HBA.</p>

Table B-4 Appliance zones (*continued*)

Zone	Description
Fibre Transport storage zone	<p>A Fibre Transport storage zone carries the Fibre Transport traffic from a 5220 or 5230 appliance to a 5020 deduplication appliance. The traffic can be either for duplication or for backups. For backups, the data first travels to the 5220 or 5230 appliance and is then sent to the 5020 deduplication appliance for storage.</p> <p>The storage zone should include the following HBA ports:</p> <ul style="list-style-type: none"> ■ The initiator port of the HBA in the 5220 appliance—connect this port to a Fibre Channel switch port. It does not have to be the same switch as the backup zone. The 5220 appliance is the source for the duplication. The initiator ports use the standard initiator mode driver. ■ The 5020 deduplication appliance ports—connect the target ports (Port 1) of the HBAs in slots 1, 2, and / or 3 to the same Fibre Channel switch. The 5020 deduplication appliance is the target of the duplication jobs. <p>Note: To use Fibre Channel on a NetBackup 5020, you must enable the Fibre Channel communication feature. For details, see the Symantec NetBackup Deduplication Appliance Software Administrator's Guide.</p> <ul style="list-style-type: none"> ■ Define the zones on the switch so that the 5220 or 5230 appliance initiator port and the 5020 deduplication appliance target port are in the same zone. <p>Note: Only one initiator port and one target port can be configured for the same zone. Multiple initiator ports and target ports in the same zone are not supported.</p>
External tape storage zone	<p>If you use a tape library as storage, create a separate zone for that traffic. The tape storage zone does not use NetBackup Fibre Transport; it uses the standard initiator mode driver.</p> <p>The tape storage zone should include a port or ports on the FC HBA in slot 3 of a 5200, 5220, or 5230 appliance.</p>

Guidelines for changing NetBackup appliance FT target ports to receive data streams from multiple SAN Client FC initiator ports

If you want an appliance Fibre Transport (FT) target port to handle data streams from more than two SAN client Fibre Channel (FC) initiator ports concurrently, consider changing the following NetBackup master server setting:

```
nbftconfig -setconfig -ncp 4
```

Caution: This setting applies to all target ports on all FT media servers in your NetBackup domain. This setting should only be increased from the default (2) when all of the following conditions exist:

All FT target ports on all FT media servers are eight gBit/s link speeds.

The total mix of FT jobs is such that all of the FT media servers have unused FT pipes.

A large number of jobs from other SAN Client machines are waiting for resources.

The back-end storage units have a lot of unused throughput capacity.

If you increase the `-ncp` setting too high, the load balancing between multiple FT media servers when all SAN Client machines are zoned to all FT media servers could become highly imbalanced.

Note: A mix of SAN Client job loads where some clients use four or more FT pipes concurrently with several other SAN Clients that only attempt to use a single FT pipe at a time increases the odds that a higher `-ncp` setting may cause FT media server imbalance.

For four gBit/s links, there may be situations where overall throughput can degrade when some or all SAN Clients are using multiple concurrent data streams. This scenario may be especially true for NetBackup 5220 appliances. In those situations, `nbftconfig -setconfig -ncp 3` may be a better option.

About Fibre Transport paths for NetBackup appliances

[Table B-5](#) shows the backup, restore, and duplication paths for NetBackup Fibre Transport for NetBackup appliances. It also shows the user interface Fibre Transport settings in the administrative Web UI that enable the functionality.

See [“Changing the Fibre Transport settings”](#) on page 54.

Fibre Transport requires the following appliance software versions:

- NetBackup 5220 and 5230 Appliance versions 2.0.2 and earlier are compatible with NetBackup 5020 Deduplication Appliance versions 1.4.1 and earlier.
- NetBackup 5220 and 5230 Appliance versions 2.0.3 and later are compatible with NetBackup 5020 Deduplication Appliance versions 1.4.2 and later.

Table B-5 Appliance Fibre Transport targets

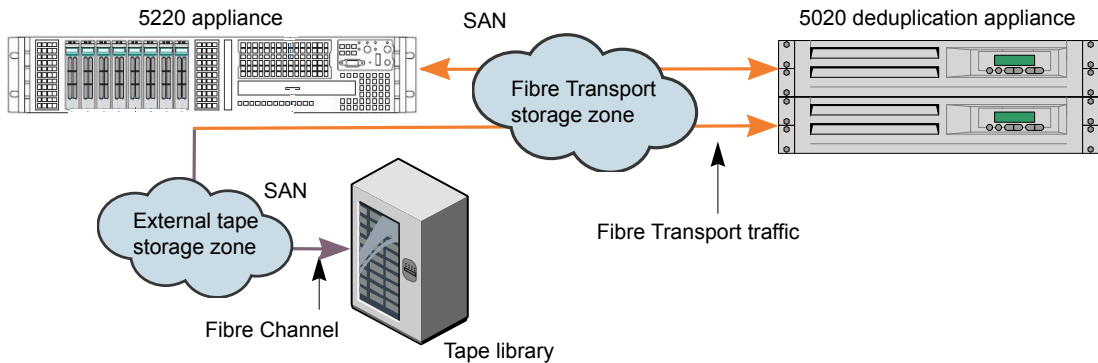
Function	From	To	Fibre Transport settings that activate the functionality
Backups	NetBackup SAN client.	NetBackup 5220 or 5230 appliance. The appliance is the backup server and the storage host.	Enable the SAN Client FT media server (Fibre Transport for backups to this appliance)
Restores	The 5220 and 5230 appliance. The appliance is the restore server and the storage host.	NetBackup SAN client.	Enable the SAN Client FT media server (Fibre Transport for backups to this appliance)
Backups	NetBackup SAN client.	NetBackup 5020 deduplication appliance. The 5020 deduplication appliance is the storage host. The 5220 or 5230 appliance is the backup server and forwards the backups to the 5020 appliance.	Enable the SAN Client FT media server (Fibre Transport for backups to this appliance) Enable the Fibre Transport to a Deduplication appliance (for duplication or for backups)
Restores	NetBackup 5020 appliance. The 5020 deduplication appliance is the storage host. It sends the restore traffic through the 5220 or 5230 appliance, which is the restore server.	NetBackup SAN Client.	Enable the SAN Client FT media server (Fibre Transport for backups to this appliance) Enable the Fibre Transport to a Deduplication appliance (for duplication or for backups)
Duplication	NetBackup 5220 or 5230 appliance.	NetBackup 5020 deduplication appliance.	Enable the Fibre Transport to a Deduplication appliance (for duplication or for backups)

An external tape library uses the standard initiator mode driver over Fibre Channel, not NetBackup Fibre Transport. Therefore, if you duplicate backup images from a tape library to a NetBackup 5020 deduplication appliance, traffic occurs as follows:

- Fibre Channel between the tape library and the 5220 or 5230 appliance.
- Fibre Transport between the 5220 or 5230 appliance and the 5020 deduplication appliance.

Figure B-7 shows the duplication paths from a 5220 appliance to a 5020 deduplication appliance.

Figure B-7 Appliance deduplication paths



The following items describe the path in [Figure B-7](#):

- Duplication from the 5220 or 5230 appliance to the 5020 deduplication appliance. If the duplication source is deduplicated storage on the 5220 or 5230 appliance, the operation is optimized duplication. If the duplication source is AdvancedDisk storage, the operation is normal duplication.
- Duplication from the 5020 deduplication appliance to the 5220 or 5230 appliance. The operation is normal duplication.
- Duplication from the tape storage over Fibre Channel to the 5220 or 5230 appliance and then over Fibre Transport to the 5020 deduplication appliance. The operation is normal duplication.
- Duplication from the 5020 deduplication appliance over Fibre Transport to the 5220 or 5230 appliance and then over Fibre Channel to the tape storage. The operation is normal duplication.

For duplication, you must configure the 5020 deduplication appliance as a storage server in NetBackup. Then, use either a storage lifecycle policy or the NetBackup Catalog utility to duplicate backup images.

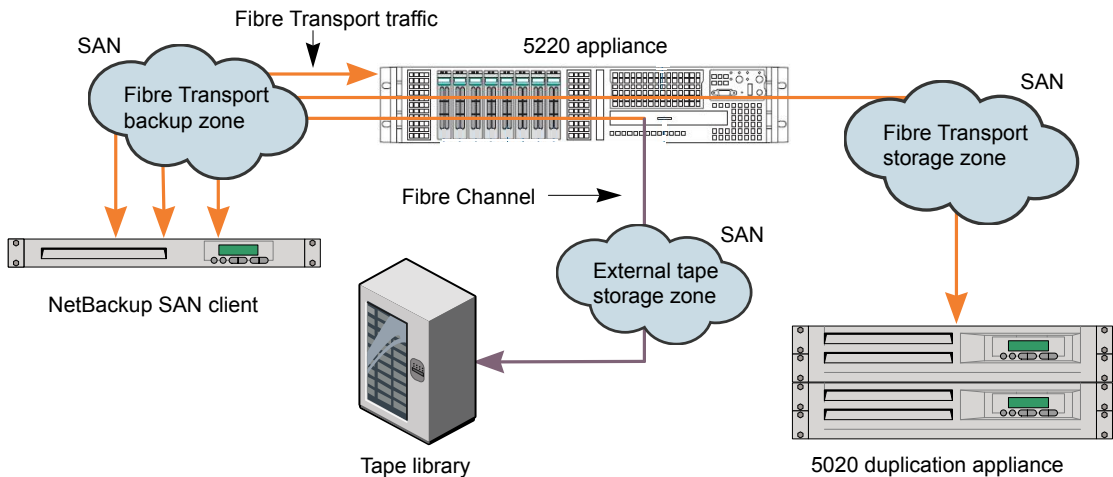
The following describes the resiliency available for Fibre Transport jobs:

- Multiple Fibre Transport paths can exist between hosts.
- Back up, restore, and duplication jobs failover to other Fibre Transport paths if they exist. If no other FT paths are available, jobs fail.
- Optimized duplication jobs failover to other Fibre Transport paths if they exist. If no other FT paths are available, they fail over to the Ethernet network. If no FT connection or IP connection exists, optimized duplication jobs fail.

- If no Fibre Transport connections exist, NetBackup uses an IP connection for new jobs.

Figure B-8 shows the possible backup and restore paths for a NetBackup SAN client.

Figure B-8 SAN client backup and restore paths



The following items describe the paths in Figure B-8:

- Fibre Transport between the client and the 5220 or 5230 appliance. The backups reside on disk storage on the appliance. You can use Fibre Transport both for backups to deduplication storage and backups to AdvancedDisk storage.
- Fibre Transport between the client and the 5020 deduplication appliance through the 5220 or 5230 appliance. The traffic travels through two different SAN zones. The backups are deduplicated and reside on disk storage on the 5020 deduplication appliance.
- Fibre Transport between the client and a 5220 or 5230 appliance, and then Fibre Channel between the appliance and the tape library. The traffic travels through two different SAN zones. The backups are not deduplicated.

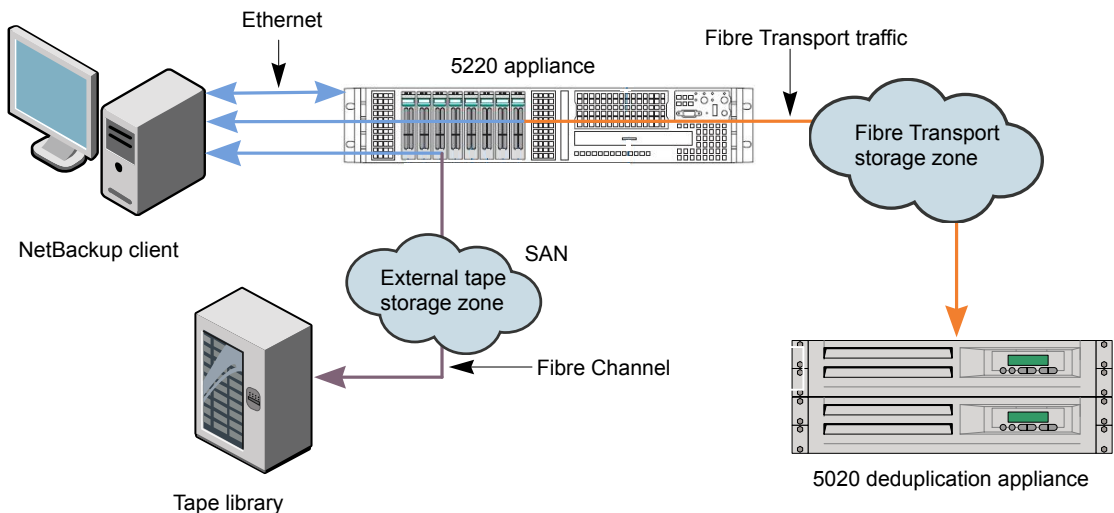
Table B-6 shows the port configurations for SAN Client, optimized duplication (storage zone), and tape applications as described in Figure B-8

Table B-6 Port configurations for SAN Client backup and restore paths

5220 FC HBA slot location	Port 1 usage	Port 2 usage
Slot 2	SAN Client	Optimized duplication (storage zone)
Slot 3	Tape	Tape
Slot 4	SAN Client	Optimized duplication (storage zone)

Figure B-9 shows the possible backup and restore paths for a NetBackup client over a LAN.

Figure B-9 LAN client backup and restore paths



The following items describe the paths in Figure B-9:

- Ethernet between the client and the 5220 or 5230 appliance. The backups reside on either deduplicated storage or AdvancedDisk storage on the appliance.
- Ethernet between the client and the 5220 or 5230 appliance, and then Fibre Transport between the 5220 or 5230 appliance and the 5020 deduplication appliance. The backups are deduplicated and reside on disk storage on the 5020 appliance.

- Ethernet between the client and the 5220 or 5230 appliance, and then Fibre Channel between the appliance and the tape library. The backups are not deduplicated.

[Table B-7](#) shows the port configurations for optimized duplication (storage zone) and tape applications as described in [Figure B-9](#), for both 1G and 10G NICs.

Table B-7 Port configurations for optimized duplication (storage zone) and tape applications

5220 FC HBA slot location	Port 1 usage	Port 2 usage
Slot 2	NA	Optimized duplication (storage zone)
Slot 3	Tape	Tape
Slot 4	NA	Optimized duplication (storage zone)

How to determine appliance HBA WWPNs

You must use physical port ID or World Wide Port Name (WWPN) when you specify the HBA ports on NetBackup appliances.

To determine the WWPNs, use the `FC Show` command in the appliance shell menu. The command output provides the information about ports based on the slot number.

For complete information about the appliance shell menu, see the *Symantec NetBackup 52xx Series Command Reference Guide*.

See [“About zoning the SAN for a NetBackup 5220 or 5230 appliance”](#) on page 305.

See [“About appliance supported tape devices”](#) on page 106.

[Table B-8](#) describes the supported FC HBA slots and their purposes for the 5020 appliance.

Table B-8 5020 appliance FC HBA slots

FC HBA purpose	NetBackup 5020
NetBackup Fibre Transport traffic	For cards in slots 1 or 3: <ul style="list-style-type: none">■ In <code>FC Show</code> output, the top port (Port 1) Mode is <code>Target</code> when configured properly.■ In <code>FC Show</code> output, the bottom port (Port 2) Mode is <code>Initiator</code>.

About the NetBackup appliance as a VMware backup host

The NetBackup appliance can back up virtual machines without a separate Windows system as backup host.

Note: You must use the VMware policy type. The FlashBackup-Windows policy type is not supported with the appliance as backup host. To use the FlashBackup-Windows policy type, you need a separate Windows host that is configured as the backup host (proxy). Any reference in this guide to the FlashBackup-Windows policy assumes the use of a Windows backup host.

To convert policies to the VMware type, you can use the `nbplupgrade` command. For details, see the *NetBackup Commands Reference Guide*.

The following topics contain notes on the appliance as the backup host:

- For an overview of the appliance as backup host in a virtual environment:
See “[Appliance as backup host: component overview](#)” on page 317.
- For a list of requirements and limitations:
See “[Notes on the NetBackup appliance as a VMware backup host](#)” on page 316.
- For further information, see the latest *NetBackup for VMware Administrator’s Guide*:
<http://www.symantec.com/docs/DOC5332>

Notes on the NetBackup appliance as a VMware backup host

Note the following requirements and limitations for the appliance as the backup host:

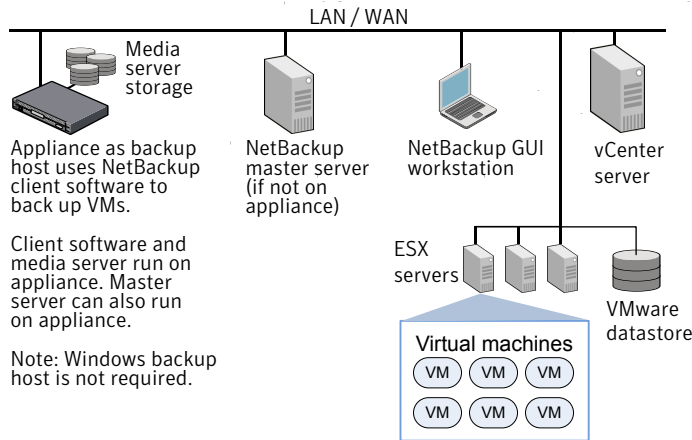
- The appliance must be version 2.5 or later. If the master server is on a separate host (not on the backup host), the master server must use NetBackup 7.5.0.1 or later.
- On the host that runs the NetBackup Administration Console or the Backup, Archive, and Restore interface, NetBackup must be at 7.5.0.1 or later.
- You must use the VMware policy type. The FlashBackup-Windows policy type is not supported.
- The appliance does not support iSCSI connections. References to iSCSI in this guide do not apply to the appliance.

Appliance as backup host: component overview

As [Figure B-10](#) shows, the appliance can operate as the VMware backup host. A separate Windows backup host is not required.

The appliance as backup host can also run the NetBackup media server and master server.

Figure B-10 NetBackup for VMware with appliance as backup host



The NetBackup environment can also be on a SAN:

Note: VMware on NetBackup 52xx appliances does not support multipathing with SAN transport.

Further information is available on the appliance as backup host:

See [“Notes on the NetBackup appliance as a VMware backup host”](#) on page 316.

About backup to tape support for NetBackup appliances

NetBackup appliances support backups to tape so that you can connect one or more tape libraries to them with Fibre Channel. The appliances use a Fibre Channel host bus adapter card (FC HBA) for connection to a TLD tape storage device.

On a NetBackup 52xx, slot 3 is always used for connection to a tape library (tape out).

If you use a tape library as storage, create a separate zone for that traffic. The tape storage zone should include the following FC HBA ports:

- A port or ports on the FC HBA card in slot 3 of a 52xx appliance.
- A port or ports on the tape library.

If you duplicate backup images from a tape library to a NetBackup 5020 deduplication appliance, traffic occurs as follows:

- Fibre Channel between the tape library and the 52xx appliance.
- Fibre Transport between the 52xx appliance and the 5020 deduplication appliance.

Note: Duplication between two NetBackup 5220 or 5230 appliances using Fibre Channel is not supported.

IPMI Configuration

This appendix includes the following topics:

- [About IPMI configuration](#)
- [Configuring IPMI using the BIOS setup](#)
- [Accessing and using the Symantec Remote Management interface](#)
- [Managing settings using the NetBackup Appliance Shell Menu](#)

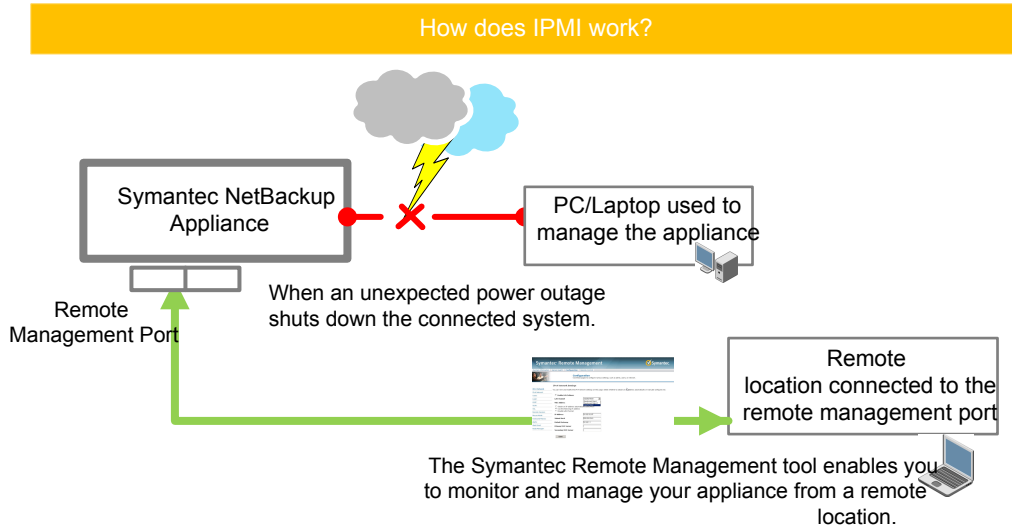
About IPMI configuration

You can configure the IPMI sub-system for your appliances. The Intelligent Platform Management Interface (IPMI) sub-system is beneficial when an unexpected power outage shuts down the connected system. This sub-system operates independently of the operating system and can be connected by using the remote management port, located on the rear panel of the appliance.

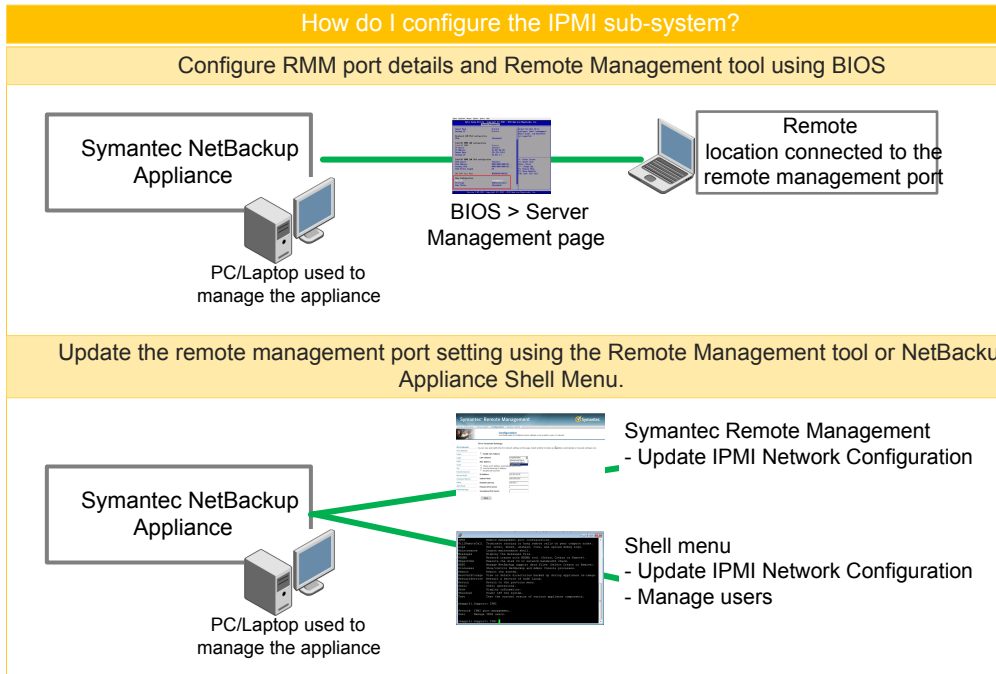
Some of the main uses of IPMI are the following:

- Manage a system remotely in the absence of an operating system
- Change BIOS settings
- Power on, power off, or recycle the appliance
- Situations where local access by monitor is not possible or preferred like branch offices, remote data center, or headless systems.
- Avoid expensive and messy cabling and hardware like keyboard, monitor, and mouse (KVM) solutions
- Reimaging the appliance using the IPMI interface

Note: After you receive, install, and configure a NetBackup Appliance, Symantec recommends that you configure the remote management port. Do not wait until you need to use the remote management port, as it may take valuable time to arrange to have someone on-site.



You can configure the IPMI sub-system and the Symantec Remote Management tool using the BIOS setup. The Symantec Remote Management tool provides an interface to use the remote management port. It lets you monitor and manage your appliance from a remote location. You can also use the appliance shell menu to manage the IPMI configuration and manage the users that access the IPMI sub-system. The following diagram illustrates how to configure and manage the IPMI sub-system.



Note: The IPMI system must be connected to a power source and the monitoring medium, typically using a LAN (local area network) connection, so that you can turn on the appliance from a remote machine.

Configuring IPMI using the BIOS setup

An IPMI lets you monitor and manage your appliance from a remote location by using the Integrated Storage Manager (ISM) or Symantec Remote Management console. Once the operating system is restarted, the IPMI system exposes the management data and structures to the operating system. From the remote location, you can use a laptop or you can use a keyboard, monitor, and mouse (KVM) to access the appliance. Before configuring the IPMI system, verify the following configuration prerequisites:

- For each appliance in the storage pool for which you want to configure the IPMI, obtain the following information from your network administrator:
 - IP address to change the default static IP address of the remote management port.
 - Subnet mask

- Gateway IP address to enable connectivity between your network computer and the appliance.
- Ensure that you have a dedicated network infrastructure.
The remote management port is 100 Mb/s for NetBackup 5220 and 1 Gb/s for NetBackup 5230 appliances.
- Open the required ports in your firewall.
If a firewall exists between the appliance and the remote devices that manage an appliance (like a laptop computer), open the following ports:

22	SSH
80	HTTP
162	SNMP
443	HTTPS
623	KVM
5120	RMM ISO/CD
5123	RMM floppy
5124	CD
5127	SSL
5900	KVM CLI
7578	RMM CLI
7582	SSL

Note: If you have a private internal network, remember to configure the settings accordingly in your network address translation (NAT).

The Symantec Remote Management tool must be set up by configuring the BIOS from the NetBackup 5220 or 5230 appliance. This section provides the procedure to configure the remote management port using the BIOS setup.

To configure the IPMI remote management port

- 1 Connect a standard video cable between the VGA (Video Graphics Array) port on the rear panel of the appliance and a computer monitor.
- 2 Connect a keyboard to a USB port on the appliance.

3 Start the appliance.

When the following Symantec splash screen appears, immediately press **F2** to enter the BIOS Setup menu. You may need to press **F2** multiple times to ensure that the BIOS menu dialog box appears.

Warning: You only get a window of a few seconds to perform this task. If you miss the window, the operating system loads and you can't access the BIOS page.

An `Entering Setup` message displays.



In some instances the Symantec logo may not appear. If that occurs, then only the following appears on the screen:

Press <Esc> to view diagnostic messages Press <F2> to enter setup, <F6> Boot Menu, <F12> Network Boot

4 Use the left and the right arrow keys on the keyboard to navigate to the **Server Management** menu.

- 5 Use the arrow keys to navigate down to the **BMC LAN configuration** section.



- 6 Do one of the following:
- For 5220 appliances, navigate to the **RMM3 LAN Configuration** section.
 - For 5230 appliances, navigate to the **RMM4 LAN configuration** section.

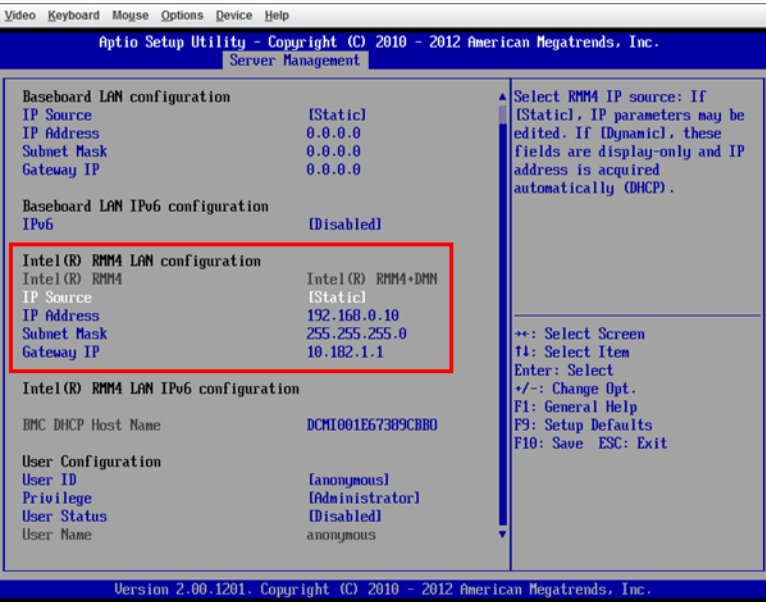
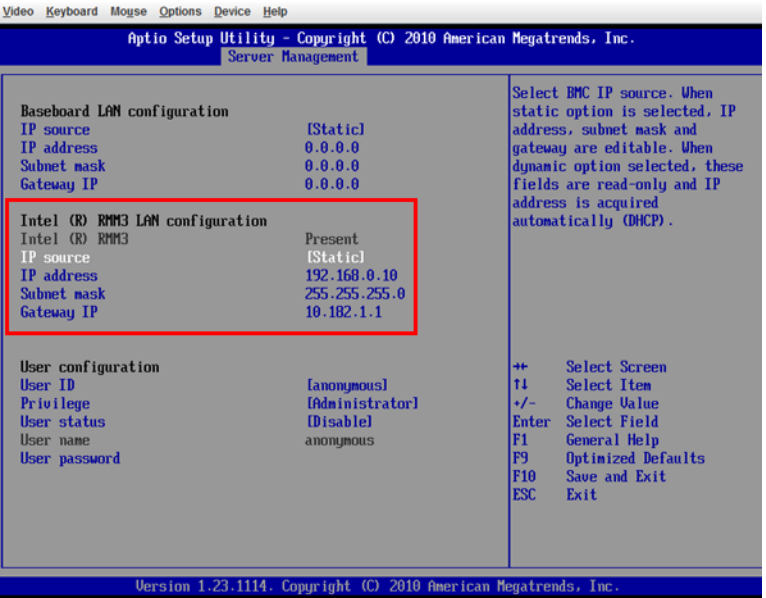
Make sure that the **IP source** option is set to **Static**.

Default addresses display.

The default **Static IP address** of the remote management port is **192.168.0.10**.

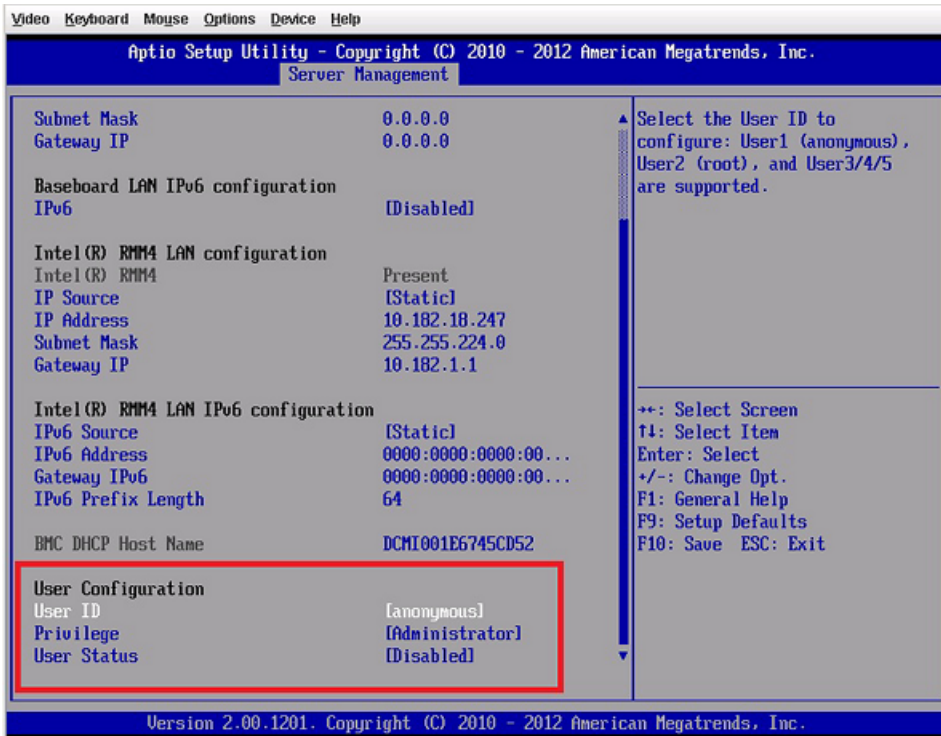
The default **Subnet mask** of the remote management port is **255.255.255.0**.

Note: Do not configure the Baseboard LAN configuration because it fails the IPMI configuration.



- 7 Change the **IP address**, **Subnet mask**, and **Gateway IP** settings to the network address from which you remotely access the appliance.

You will be asked to enter the user name and password to confirm the settings.



- 8 Enter a strong **User password**.
The default **User ID** is **sysadmin**.
The default **User password** is **P@ssw0rd**.
- 9 Press **<F10>** to save your configuration and exit the BIOS.
- 10 In the **Confirmation message**, select **Yes**.

The appliance is automatically restarted.

Now that the IPMI tool is configured, you can use it to turn on and manage your appliance from a remote location.

Accessing and using the Symantec Remote Management interface

The IPMI Web interface is known as Integrated Storage Manager in NetBackup 5200 appliances. The IPMI Web interface is known as Symantec Remote Management in NetBackup 5220 and later appliances.

More information about the Integrated Storage Manager interface is available.

See [“About the Integrated Storage Manager interface for 5200 appliances”](#) on page 336.

Before you use the Symantec Remote Management interface, the following prerequisites must be met:

- The Symantec Remote Management interface must first be configured using the BIOS setup.
- At least one power cable must be connected to a functioning power source.
- For 5220 appliances, the RMM3 channel must be configured as a DHCP or static address.
For 5230 appliances, the RMM4 channel must be configured as a DHCP or static address.

Note: You should not configure the Baseboard Management channel. All the Baseboard port fields must be 0.0.0.0

- At least one user must be enabled to use the LAN channel(s).
- The remote management port can auto-negotiate its link speed of up to 100Mbps for 5220 and 1Gbps for 5230.
- Ensure that port 7578 is open, prior to configuring the IPMI network. The port is used for firewalls.
- Obtain the IP address used for configuring IPMI. There may be specific addresses from your network that are required for connectivity to a remote appliance.

To access and use the IPMI Web interface

- 1 Open a supported Windows browser on your remote computer.
- 2 Enter the remote management port IP address assigned to the appliance in the BIOS. The following page appears:



Please log in to access the device.

Username

Password

- 3 Enter your login information. The default user name is **sysadmin**. The default password is **P@ssw0rd**, where **0** is the number zero.

Click **Login**.

- The **System Information** section appears. This section shows general hardware information about the appliance. You can also obtain **Field Replaceable Unit (FRU)** component information from this page.


Symantec™ Remote Management

System Information

Server Health

Configuration

Remote Control



System Information

This section contains general information about the system.

Summary

System Information

FRU Information

System Information

Host Power Status : Host is currently ON

RMM3 Status : Intel(R) RMM3 installed

Device (BMC) Available : Yes

BMC FW Build Time : May 5 2011 11:42:29

BMC FW Rev : 02.56

Boot FW Rev : 00.18

SDR Package Version : SDR Package 0.26

Primary HSC FW Rev : 02.17

Secondary HSC FW Rev : (not present)

Mgmt Engine (ME) FW Rev : 01.12

Local Control Panel (LCP) FW Rev : 00.74

For 5230 appliances, the **System Debug Log**, **CPU information**, and **DIMM information** tabs are also available under **System Information**. The **System Debug Log** tab helps you to collect debug information about the appliance which is useful for problem resolution. The **CPU information** and the **DIMM information** tabs show CPU and DIMM data for the appliance.

Symantec Remote Management

System Information


Server Health

Configuration

Remote Control

LOGOUT

REFRESH



System Information

This section contains general information about the system.

System Information

FRU Information

System Debug Log

CPU Information

DIMM Information

The following operations generate an encrypted zip file that contains debug information which is useful to the system manufacturer for problem resolution. The information collected includes Baseboard Management Controller (BMC) status, BMC configuration settings, BMC Sensor readings, Power supply data, System Event Log, sensor readings, SMBIOS tables, CPU machine check registers and PCI configuration space information. If you elect to forward this information to a third party, it contains no personal information and may be used for the purpose of investigating the problem. Downloading debug information by clicking on the link does not change any configuration files or read application data on any of the hard drives.

Log files should be sent to the system manufacturer for analysis.

System Debug Log

Last Log:

None

Generate Log

- The **Server Health** section shows data related to the server's health, such as sensor readings and the event log. The event log information is useful for troubleshooting appliance boot issues.


Symantec Remote Management

System Information

Server Health

Configuration

Remote Control



Server Health

This section shows you data related to the server's health, such as sensor readings and the event log.

Sensor Readings

Event Log

Drv 0 Stat	All deasserted	0x8E00
Drv 1 Stat	All deasserted	0x8E00
Drv 2 Stat	All deasserted	0x8E00
Drv 3 Stat	All deasserted	0x8E00
Drv 4 Stat	All deasserted	0x8E00
Drv 5 Stat	All deasserted	0x8E00
Drv 6 Stat	All deasserted	0x8E00
Drv 7 Stat	All deasserted	0x8E00
Drv 0 Pres	reports the device has been inserted or is present	0x8002
Drv 1 Pres	reports the device has been inserted or is present	0x8002
Drv 2 Pres	reports the device has been inserted or is present	0x8002
Drv 3 Pres	reports the device has been inserted or is present	0x8002
Drv 4 Pres	reports the device has been inserted or is present	0x8002
Drv 5 Pres	reports the device has been inserted or is present	0x8002
Drv 6 Pres	reports the device has been inserted or is present	0x8002
Drv 7 Pres	reports the device has been inserted or is present	0x8002

Refresh

Show Thresholds

For 5230 appliances, the **Power Statistics** tab is also available in the **Server Health** section. See the following figure:

System Information
Server Health
Configuration
Remote Control
LOGOUT
REFRESH
HELP
ABOUT

Server Health

This section shows you data related to the server's health, such as sensor readings and the event log.

Sensor Readings

Sensor Readings

Event Log

Power Statistics

This page displays system sensor information, including readings and status. You can toggle viewing the thresholds for the sensors by pressing the Show Thresholds button below.

Refreshing readings every 60 seconds

Select a sensor type category:

All Sensors

Sensor Readings: 110 sensors

Name	Status	Health	Reading
Pwr Unit Status	All deasserted	OK	0x0000
Pwr Unit Redund	reports full redundancy has been regained	OK	0x0001
IPMI Watchdog	All deasserted	OK	0x0000
Physical Scrty	All deasserted	OK	0x0000
FP NMI Diag Int	All deasserted	OK	0x0000
SMI Timeout	All deasserted	OK	0x0000
System Event Log	reports the System Event Log (SEL) is full	OK	0x0010
System Event	All deasserted	OK	0x0000
Button	All deasserted	OK	0x0000
VR Watchdog	All deasserted	OK	0x0000
Fan Redundancy	reports full redundancy has been regained	OK	0x0001
SSB Therm Trip	All deasserted	OK	0x0000
IO Mod Presence	reports the device has been inserted or is present	OK	0x0002
SAS Mod Presence	All deasserted	OK	0x0000
BMC FW Health	All deasserted	OK	0x0000
System Airflow	Normal	OK	60 CFM
BB P1 VR Temp	Normal	OK	29 degrees C
Front Panel Temp	Normal	OK	27 degrees C

- 6 The **Configuration** section lets you configure various settings such as alerts, users, or network.

From the left pane, click **Network** and go to the **LAN Channel** drop-down list. The drop-down list displays the **Baseboard Mgmt** and **Intel(R) RMM** options. Select **Intel(R) RMM**.

If you have not configured the remote management port in BIOS, the default IP address, subnet mask, and gateway IP address are shown. If you have not changed these addresses in BIOS, you need to do so now. Specific addresses from your network are required for connectivity to a remote appliance.

If you have configured the remote management port in BIOS, the static IP address, subnet mask, and gateway IP address of your network are shown.

The screenshot shows the Symantec Remote Management web interface. The top navigation bar includes 'System Information', 'Server Health', 'Configuration' (selected), and 'Remote Control'. Below the navigation bar, the 'Configuration' section is active, with a sub-header 'Network Settings'. A left-hand menu lists various configuration options: Network, Users, Login, LDAP, SSL, Remote Session, Mouse Mode, and Keyboard Macros. The main content area for 'Network Settings' contains a description: 'You can view and modify the network settings on this page. Select whether to obtain an IP address automatically or manually configure one.' Below this, there are several input fields: 'LAN Channel' (a dropdown menu currently showing 'Baseboard Mgmt'), 'MAC Address' (a text field showing '00:1E:67:10:CF:12'), 'IP Address' (a text field showing '0.0.0.0'), 'Subnet Mask' (a text field showing '0.0.0.0'), and 'Default Gateway' (a text field showing '0.0.0.0'). There are two radio buttons for IP configuration: 'Obtain an IP address automatically (use DHCP)' and 'Use the following IP address' (which is selected). A 'Save' button is located at the bottom of the form.

- 7 For 5230 appliances, the following settings are available as shown in the figure.

The screenshot shows the Symantec Remote Management interface. The top navigation bar includes links for System Information, Server Health, Configuration (selected), and Remote Control. Below the navigation bar, the Configuration section is active, displaying a list of settings on the left and the IPv4 Network Settings configuration on the right. The IPv4 Network Settings section includes a description, a list of settings on the left, and a form for configuration on the right. The form includes fields for LAN Channel, MAC Address, IP Address, Subnet Mask, Default Gateway, Primary DNS Server, and Secondary DNS Server. The LAN Channel is set to Baseboard Mgmt, and the IP Address, Subnet Mask, and Default Gateway are all set to 0.0.0.0. The Primary and Secondary DNS Servers are empty. A Save button is at the bottom.

Symantec Remote Management

System Information | Server Health | **Configuration** | Remote Control

Configuration
Use these pages to configure various settings, such as alerts, users, or network.

IPv4 Network Settings
You can view and modify the IPv4 network settings on this page. Select whether to obtain an IP address automatically or manually configure one.

IPv4 Network
IPv6 Network
Users
Login
LDAP
VLAN
SSL
Remote Session
Mouse Mode
Keyboard Macros
Alerts
Alert Email
Node Manager

☐ Enable LAN Failover

LAN Channel Baseboard Mgmt

MAC Address 00:1E:67:4E:1A:BC

☐ Obtain an IP address automatically (use DHCP)
☒ Use the following IP address
☐ Disable LAN Channel

IP Address 0.0.0.0

Subnet Mask 0.0.0.0

Default Gateway 0.0.0.0

Primary DNS Server

Secondary DNS Server

Save

From the left pane, click on **IPv4 Network** link. The **IPv4 Network Settings** screen appears.

Go to the **LAN Channel** drop-down list. The drop-down list displays the **Baseboard Mgmt**, **Baseboard Mgmt2** and **Intel(R) RMM** options. Select **Intel(R) RMM**.

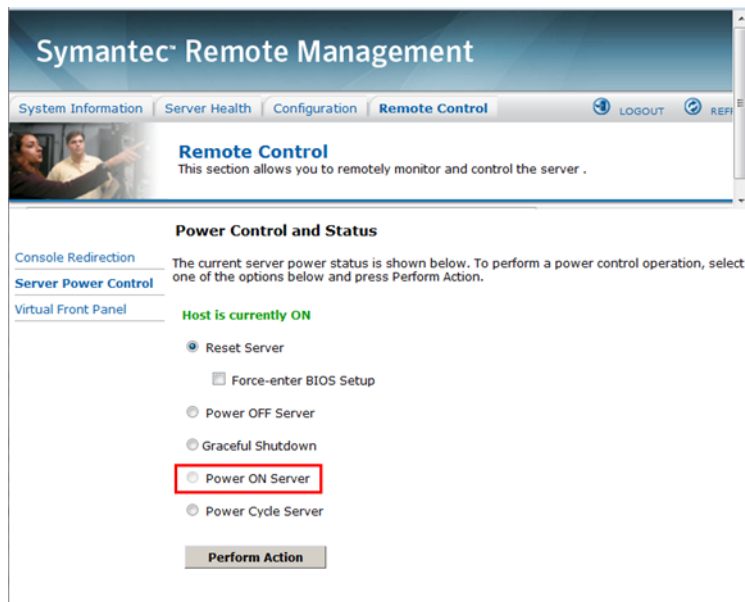
If you have not configured the remote management port in BIOS, the default IP address, subnet mask, and gateway IP address are shown. If you have not changed these addresses in BIOS, you need to do so now. Specific addresses from your network are required for connectivity to a remote appliance.

If you have configured the remote management port in BIOS, the static IP address, subnet mask, and gateway IP address of your network are shown.

- 8 The **Remote Control** section lets you remotely monitor and control the server. Click **Launch Console** under the **Console Redirection** tab to launch the appliance shell menu. This step opens a JViewer application that enables you to remotely monitor and control the appliance. This requires Java Runtime Environment (JRE) version 6.0 or later.



From the left pane, you can click on the **Server Power Control** link to power on and power off the appliance. Select the **Power ON Server** radio button.



Click **Perform Action** to start the appliance.

- 9 For 5230 appliances, you also have **Virtual Front Panel** tab which provides front panel functionality virtually.



About the Integrated Storage Manager interface for 5200 appliances

The IPMI Web interface is known as Integrated Storage Manager (or ISM) in NetBackup 5200 appliances.

The interface looks like the following:

Oceanspace ISM
Integrated Storage Manager Professional Edition

User: admin Level: Administrator

Current Location : Device Management > Device Info

Device Management

- Device Info
- Disk Info
- Sensor List
- Boot Device

Device Configuration

- Set BMC Time
- Boot OS
- Reset BMC
- Device Indicator
- Set IPMI Network
- Start KVM

Alarm Management

- Alarm Statistics
- View Alarm
- Set Trap IP
- Set SMTP

User Management

- User List
- Create User

Upgrade Management

- Upgrade Firmware

Device Info

Product Name	Oceanspace T3200
Serial No.	210235G317Z0A6000051
Manufacturer	Huawei Symantec Technologies Co., Ltd
Asset Tag	00000000000000000000

Boot BIOS

BIOS Name	BIOS Status
BIOS0	Normal

CPU Info

ID	Core Status	Core temp.(°C)	Volts(V)
1	Online	-46.00	1.11
2	Online	-48.00	1.10

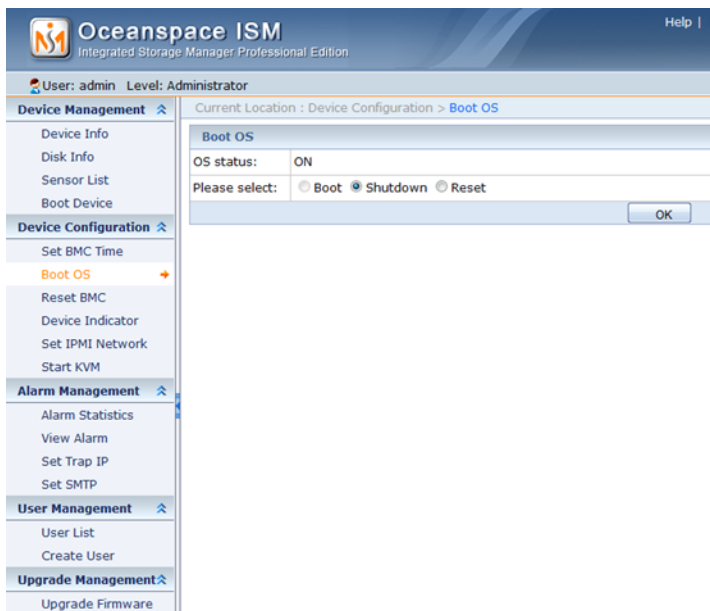
Power Info

ID	Status	Manufacturer	Serial No.	Type
1	OK	VAPEL	VAPE1027000606	ACM
2	Fault	-	-	-

Fan Info

ID	Status	Speed(RPM)	Serial No.
1	OK	7003	03030000000000011
2	OK	6345	03030000000000012
3	OK	6439	03030000000000013
4	OK	6721	03030000000000014

You can also start, shut down, or reset the appliance by clicking the **Boot OS** link from the **Device Configuration** section..



Oceanspace ISM
Integrated Storage Manager Professional Edition

User: admin Level: Administrator

Current Location : Device Configuration > [Boot OS](#)

Device Management

- Device Info
- Disk Info
- Sensor List
- Boot Device

Device Configuration

- Set BMC Time
- Boot OS**
- Reset BMC
- Device Indicator
- Set IPMI Network
- Start KVM

Alarm Management

- Alarm Statistics
- View Alarm
- Set Trap IP
- Set SMTP

User Management

- User List
- Create User

Upgrade Management

- Upgrade Firmware

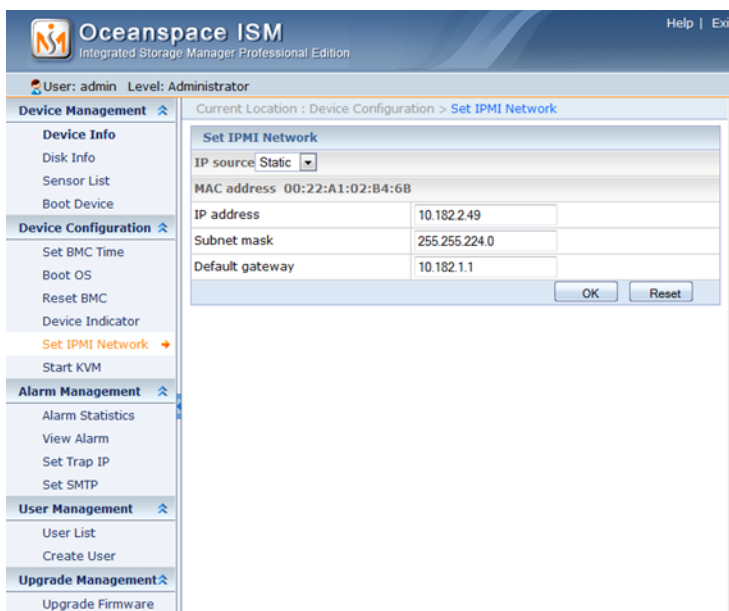
Boot OS

OS status: ON

Please select: ☐ Boot ☒ Shutdown ☐ Reset

OK

You can configure the network settings by clicking the **Set IPMI Network** link from the **Device Configuration** section.



Oceanspace ISM
Integrated Storage Manager Professional Edition

User: admin Level: Administrator

Current Location : Device Configuration > [Set IPMI Network](#)

Device Management

- Device Info
- Disk Info
- Sensor List
- Boot Device

Device Configuration

- Set BMC Time
- Boot OS
- Reset BMC
- Device Indicator
- Set IPMI Network**
- Start KVM

Alarm Management

- Alarm Statistics
- View Alarm
- Set Trap IP
- Set SMTP

User Management

- User List
- Create User

Upgrade Management

- Upgrade Firmware

Set IPMI Network

IP source: Static

MAC address: 00:22:A1:02:84:6B

IP address: 10.182.2.49

Subnet mask: 255.255.224.0

Default gateway: 10.182.1.1

OK Reset

When the IP address of the IPMI management network port is modified, you need to enter the username and password to re-log in to the ISM through the new IP address. On the **Set IPMI Network** interface, the **Reset** button is used to restore the content in the IP address, Subnet mask, and Default gateway text boxes as before being modified, or to empty the IP address, Subnet mask, and Default gateway text boxes without modifying the configuration of the IPMI management network port.

Managing settings using the NetBackup Appliance Shell Menu

The NetBackup Appliance Shell Menu enables you to manage IPMI settings using the following `Support` commands:

Table C-1 IPMI commands

Command	Description	Options and description	Example
IPMI Network Configure <IPAddress> <Netmask> <GatewayIPAddress>	You can use this command to change IPMI configuration.	<ul style="list-style-type: none">■ <IPAddress> - Specify the updated IP address of the remote management port.■ <Netmask> - Specify the updated Subnet mask.■ <GatewayIPAddress> - Specify the updated gateway IP address.	IPMI Network Configure 192.168.0.15 255.255.255.0 255.255.255.4
IPMI Network Show	You can use this command to view the remote management port information.	None	Support> IPMI Network Show IP Address Source : STATIC IP Address : 10.182.8.70 Subnet Mask : 255.255.240.0 Gateway IP Address : 10.182.1.1
IPMI User Add <USER_NAME>	You can use this command to add new users for accessing the remote management port.	<USER_NAME> - Specify the name of the user to be added.	IPMI User Add <i>New User</i>

Table C-1 IPMI commands *(continued)*

Command	Description	Options and description	Example
IPMI User Delete <USER_NAME>	You can use this command to delete existing users who no longer use the remote management port.	<USER_NAME> - Specify the name of the user to be deleted.	IPMI User Delete <i>Old User</i>
IPMI User List	You can use this command to list the users that have access to the remote management port.	None	Support> IPMI User List User name: abc User privilege: ADMIN User name : root User privilege: ADMIN

Note: For more information on the IPMI commands refer to the *Symantec NetBackup Appliance Command Reference Guide*.

Index

Symbols

- 52xx appliances
 - card slots on 293
- 52xx master server appliance
 - initial configuration from NetBackup Appliance Shell Menu 268
 - reconfigure from USB and NetBackup Appliance Shell Menu 268
- 52xx media server appliance
 - reconfigure from USB and NetBackup Appliance Shell Menu 275

A

- about
 - appliance restore 144
 - backup to tape support for appliances 317
 - checkpoint creation status 152
 - creating appliance checkpoint 146, 149
 - decommissioning an appliance 245
 - Email notification from NetBackup appliance 92
 - factory reset 163
 - Fibre Channel port configuration options 298
 - license key management 175
 - master server role 15
 - media server role 16
 - NetBackup appliances 12
 - NetBackup documentation 31
 - reconfiguring the appliance 258
 - rollback to checkpoint 154
 - software release updates 192
 - supported tape devices and tapes 106
- About BMR 116
- acknowledge
 - hardware 91
- add external robots 107
- add user
 - LDAP 77
 - local 77
- add user group 78
- alert notification
 - call home 37

- alert notification (*continued*)
 - SMTP 37
 - SNMP 37
- Appliance console
 - description 21
- appliance FT target ports
 - guidelines for multiple SAN Client FC initiator ports 309
- appliance media server
 - configure master server to communicate with 273
- appliance password
 - change after initial configuration 63
- appliance registration
 - initial configuration for 46
- Appliance Restore
 - management on the NetBackup appliance 144
- appliance support
 - for backup to tape 317
- Appliance Web Console
 - enable BMR 117
- Auto Image Replication 239
 - between appliances and deduplication appliances 244
- AutoSupport
 - customer registration 48

B

- backup to tape
 - appliance support for 317
- bandwidth
 - expanding on NetBackup appliance 220
- BMR
 - enable 117
 - option 116
- bookmarks
 - using with Appliance 23

C

- Call Home
 - alerts 41
 - workflow 45

- call home
 - information uploaded 284
- Call Home proxy server
 - configuring 44
- card slots
 - on 52xx appliances 293
- change
 - Date and Time Configuration 64
 - settings for Fibre Transport 53
- change appliance password 63
- change settings
 - for DNS Configuration 55
 - for Network Configuration 50
- changing host configuration 54
- clients used with appliances
 - install client software on 212
- common tasks
 - Appliance 29
- configuration
 - of maximum transmission unit size 221
- configure master server
 - to communicate with appliance media server 273

D

- dashboard 28
- data buffer
 - parameters 109
- datacollect
 - device logs 256
- Date and Time Configuration
 - change 64
- decommissioning an appliance
 - about 245
- deduplication
 - parameters 115
 - solutions 113
- deduplications 5230 113
- delete user
 - LDAP 77
 - local 77
- delete user group 79
- disable security warnings
 - on Mozilla 18
- disk information
 - viewing 140
- disks
 - storage 130
- DNS Configuration
 - change settings 55

- documentation 31
- download software updates
 - Manage > Software Updates tab 194

E

- Email notification
 - from NetBackup appliance 92
- expand bandwidth
 - on NetBackup appliance 220
- external robots
 - adding to the NetBackup 5200 107

F

- Fibre Channel
 - port configuration options 298
- Fibre Transport
 - change settings 53

G

- grant permissions 79
- guidelines for changing appliance FT target ports
 - for multiple SAN Client FC initiator ports 309

H

- hardware
 - monitor 87
 - monitoring and alerts on the appliance 82
- hardware monitoring and alerts 82
- HBA WWPN
 - how to determine for appliance 315
- home page 28
- host reconfiguration 54

I

- initial configuration
 - for appliance registration 46
- initial configuration of 52xx master server appliance
 - from NetBackup Appliance Shell Menu 268
- install
 - openstorage plugin 223
- install client software
 - on clients used with appliances 212
- install software updates
 - Manage > Software Updates tab 194
- IPMI configuration
 - about 319
- IPv4 and IPv6 support 61

L

- LDAP
 - user management 76
- LDAP authentication 65
- license key
 - management on the NetBackup appliance 175
- lifecycle
 - parameters 110, 113

M

- Manage
 - license keys 177
- manage
 - appliance restore 146, 149, 152–155, 157–158, 161, 163, 167, 170–171
 - license keys 176
- Management Information Base (MIB) 41
- master server
 - about role 15
- maximum transmission unit size
 - about configuration for 221
- media server role 16
- menu
 - settings 34
- menus 19
- Microsoft Internet Explorer 17
- migration
 - check job status 185
 - Policy Conversion tab 188
 - Selection Criteria tab 181
- Migration Job Status tab 185
- Migration Utility
 - about 179
- monitor
 - hardware summary 82
 - NetBackup 52XX configuration 81
- monitor storage tasks 137
- move dialog
 - storage 129
- Mozilla Firefox 17

N

- NetBackup
 - about documentation for 31
- NetBackup 5200
 - adding external robots 107
- NetBackup appliance
 - about appliance restore 144

- NetBackup appliance (*continued*)
 - about Email notification 92
 - about license key management 175
 - appliance factory reset 167, 171
 - appliance rollback validation 157
 - checkpoint rollback status 161
 - expanding bandwidth on 220
 - factory reset status 170
 - managing appliance restore 146
 - managing license keys 176
 - monitoring and alerts 82
 - reconfigure 258
 - rollback appliance 155, 158, 161
- NetBackup Appliance Web Console login 23
- NetBackup commands
 - Auditing accounts 237
 - Best practices 233
 - Creating touch files 232
 - creating users 234
 - deleting users 237
 - Known limitations 234
 - Logging in as administrator 235
 - manage users 229
 - Managing passwords 236
 - OS commands 232
 - Running commands 231
 - viewing current users 238
- NetBackup parameters 107
- Network Configuration
 - change settings 50
- network settings 49
- NFS mount
 - mount a remote NFS drive 226
 - mount list 225
 - unmount 225
 - Unmount a remote NFS drive 228
- notifications 41

O

- openstorage plugin 221
 - installing plugins 223
 - uninstalling plugins 224
- OST plugin
 - installing plugins 223
 - uninstalling plugins 224

P

- parameters
 - data buffer 109
 - deduplication 115
 - lifecycle 113
- partition distribution
 - on disks 142
- partitions
 - storage 120
- Policy Conversion
 - change policy for migration 188
- port configuration options
 - for Fibre Channel 298

R

- reconfiguration of 52xx master server appliance
 - from USB and NetBackup Appliance Shell Menu 268
- reconfiguration of 52xx media server appliance
 - from USB and NetBackup Appliance Shell Menu 275
- reconfigure
 - NetBackup appliance 258
- remove
 - storage disk 135
- resize dialog
 - storage 126
- revoke permissions 80
- role
 - about master server 15
 - about media server 16

S

- scan
 - storage device 137
- SCSP
 - connecting 101
 - documentation 102
 - filtering audit logs 98
 - log retention 100
- SCSP integration
 - about 94
- Selection Criteria tab
 - migration 181
- settings
 - sub menus 34
- show
 - disks 138

show *(continued)*

- distribution 138
- partitions 138
- Simple Network Management Protocol (SNMP) 40
- SNMP server options 40
 - options 40
- software release updates 192
- software updates
 - Manage > Software Updates tab 194
- storage 82
 - viewing 139
- storage configuration
 - about 117
- storage device
 - scan 137
- storage disk
 - removing 135
- storage partition
 - moving 128
 - resizing 124
- storage partitions
 - viewing 142
- Symantec NetBackup Appliance
 - settings menu 34

T

- tape devices and tapes
 - about appliance supported 106
- trusted master servers
 - adding 240

U

- uninstall
 - openstorage plugin 224
- upgrade appliance 200

W

- WAN optimization
 - disable 56
 - enable 56
 - status 56
 - traffic 56
- web browser
 - book marks 23
 - support 17