Symantec NetBackup™ Appliance Troubleshooting Guide

Release 2.6.0.3

NetBackup 52xx, NetBackup 5030

Symantec™

Symantec NetBackup Appliance Troubleshooting 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.

Legal Notice

Copyright © 2014 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 About using the Troubleshooting Guide 11

About this guide 11
About the intended audience 12
About contacting Symantec Technical Support 12
About troubleshooting the NetBackup Appliance 13

Chapter 2 Best practices 17

About best practices 17
Locating the NetBackup Appliance serial number 19
Locating hardware serial numbers 21
Web browsers supported by Appliance 22
Disabling the Untrusted Connection page in Mozilla Firefox 24
About Fibre Channel HBA card configuration verification 25
About Notification settings 27
About the IPMI sub-system 27
About password management and recovery 28
About IPv4-IPv6-based network support 29
About enabling BMR options 30
Interpretation of some of the fields of `vxprint` output from NetBackup and PureDisk appliances 31
About deleting LDAP or Active Directory users 32

Chapter 3 About Software Troubleshooting Tools 34

Tools for troubleshooting the NetBackup Appliance 34
Troubleshooting and tuning Appliance from the Appliance Diagnostics Center 35
About NetBackup support utilities 40
NetBackup Domain Network Analyzer (NBDNA) 40
NetBackup Support Utility (nbsu) 42
About changing VxAT properties 42

Chapter 4 About the NetBackup appliance hardware 43

About the NetBackup 5230 appliance hardware 43
Specifications for the NetBackup 5230 Appliance 43
About the NetBackup 5230 appliance bezel 45
About the NetBackup 5230 Appliance front panel 46
About the NetBackup 5230 Appliance rear panel 48
About the NetBackup 5220 appliance hardware 53
Specifications for the NetBackup 5220 Appliance 53
NetBackup 5220 Appliance front panel 55
NetBackup 5220 Appliance rear panel 59
About the NetBackup 5030 Appliance hardware 60
About the NetBackup 5030 Appliance front panel 60
About the NetBackup 5030 Appliance bezel 62
About the cables 63
About rack mounting 63

Chapter 5 Working with log files 64

About working with log files 64
About using the Collect Log files wizard 67
Reviewing SCSP events 67
Viewing log files using the Support command 70
Locating NetBackup Appliance log files using the Browse command 71
Gathering device logs with the DataCollect command 72
Gathering information for NetBackup-Java applications 75
Enabling and disabling VxMS logging 76

Chapter 6 Troubleshooting the NetBackup Appliance setup and configuration issues 78

Troubleshooting the appliance setup and configuration issues 78
About NetBackup appliance and Symantec Storage Shelf matched pairs 79
About troubleshooting client installations 80
About troubleshooting appliance installation and upgrade problems 80
Troubleshooting appliance configuration problems 81
Resolving a boot order change problem 82
About a login error message that does not go away 87
Failure to complete role configuration when NetBackup Appliance Directory is down 87

Chapter 7 Troubleshooting generic issues 90

Troubleshooting generic issues 91
Troubleshooting target mode port from the client 92
About Fibre Transport media server verification 96
Troubleshooting failure to connect to a media server and create storage unit 96
Troubleshooting possible issues to enable or disable the SAN Client Fibre Transport 97
Troubleshooting self-test errors 97
About troubleshooting a corrupt storage partition 98
About troubleshooting FactoryReset problems 100
Discard RAID preserved cache after performing a factory reset 101
Crash analysis in case of kernel coredump 101
Troubleshooting IPv6 network problems 102
Reinstallation of the NetBackup Appliance software on a 5220 can fail 104
NetBackup deduplication disk pool or disk volume intermittently goes to a DOWN state 104
Failed to perform the Appliance Factory Reset operation on a media server 105
Failed to boot NetBackup 5220 appliance due to the missing embedded RAID controller information 106
Resolving an fsck test failure 107

Chapter 8 Troubleshooting Hardware Issues 111

Starting an appliance that does not turn on 111
Troubleshooting an amber drive status LED on the appliance 113
Troubleshooting a system drive that the management software does not identify 114
Troubleshooting appliance power supply problems 115
Troubleshooting system-induced shutdown 116
Troubleshooting system status LED issues 118

Chapter 9 Removing and replacing appliance hardware components 120

Overview 120
Removing and replacing the bezel 121
Removing and replacing NetBackup 5230 disk drives 122
Removing and installing a NetBackup 5030 or NetBackup 5230 power supply 124

Removing and replacing NetBackup 5220 Appliance storage drives 127
Removing and replacing a NetBackup 5220 Appliance power supply 128

Chapter 10 Disaster Recovery 129

About disaster recovery 129
Disaster recovery best practices 130
Disaster recovery scenarios 131
Appliance sustained power interruption 131
Appliance hardware failure 133
Appliance storage disk failure 136
Complete loss of appliance with recoverable operating system drives and attached storage disks 136
Complete loss of appliance with recoverable attached storage disks 138
Complete loss of appliance and attached storage disks 167
NetBackup appliance software corruption 168
NetBackup appliance database corruption 169
NetBackup appliance catalog corruption 172
NetBackup appliance operating system corruption 178

Chapter 11 NetBackup Appliance error messages 181

About NetBackup Appliance error messages 181
Error messages displayed during initial configuration 182
Error messages displayed on the NetBackup Appliance Web Console 183
Error messages displayed on the NetBackup Appliance Shell Menu 203
NetBackup status codes applicable for NetBackup Appliance 210

Index 212

Chapter 1

About using the Troubleshooting Guide

This chapter includes the following topics:

- About this guide
- About the intended audience
- About contacting Symantec Technical Support
- About troubleshooting the NetBackup Appliance

About this guide

This guide provides the information to troubleshoot the Symantec NetBackup Appliances with the appliance software version *2.6.0.x*. This guide provides steps to troubleshoot the NetBackup Appliance using the NetBackup Appliance Web Console and the NetBackup Appliance Shell Menu. It also provides detailed instructions on how to manage the 52xx appliance hardware. This guide helps you perform the following tasks:

- Diagnose an issue by using the available tools to diagnose a problem.
- Locate the relevant information to identify the core problem by referencing to the relevant logs.
- Resolve issues faced by implementing the best troubleshooting practices.
- Safely remove and replace the hardware components that are faulty and cause the issue to reoccur.

Note: We ensure that our documents are up-to-date with the latest information about the NetBackup Appliance hardware and software. You can refer to the DOC2792 for the most updated versions of the NetBackup Appliance documentation.

About the intended audience

This guide is intended for the end users that include system administrators and IT technicians who are tasked with maintaining theNetBackup Appliance.

About contacting Symantec Technical Support

The Symantec Technical Support website has a wealth of information that can help you solve NetBackup problems. You can access Technical Support at the following URL:

www.symantec.com/business/support/

You can also visit the Symantec TV website to view training videos about the features of NetBackup Appliance.

http://www.symantec.com/tv/allvideos/

When you report an issue to Symantec support, keep the following information at hand:

- Ensure that you register the appliance and your contact information using the **Settings > Notification > Registration** tab from the NetBackup Appliance Web Console. Registration of your NetBackup appliance helps to make sure that you are alerted to product updates and other important information about your appliance.
- Locate and note the serial number of your appliance, storage devices, and switches as applicable.
  See "Locating the NetBackup Appliance serial number" on page 19.
- Refer to the error messages section in the Troubleshooting guide and confirm the recommended action. You can refer to the following sections:
  See "Error messages displayed during initial configuration" on page 182.
  See "Error messages displayed on the NetBackup Appliance Web Console" on page 183.
  See "Error messages displayed on the NetBackup Appliance Shell Menu" on page 203.
  See "NetBackup status codes applicable for NetBackup Appliance" on page 210.
- Gathering device logs using the `Datacollect` command.

See "Gathering device logs with the DataCollect command" on page 72.

- Ensure that Call Home is enabled and the proxy settings provided are correct. You can use the **Settings > Notification > Alert Configuration** from the NetBackup Appliance Web Console to apply the Call Home settings. See "About Notification settings" on page 27.

For the complete list of best practices, See "About best practices" on page 17.

About troubleshooting the NetBackup Appliance

If you experience trouble with your appliance and cannot resolve the problem using the troubleshooting wizards available from the **Tools** icon, it is important that you can define the problem and collect any supporting information. When you reach this point, you should contact Symantec Technical Support. A technical support representative works with you to diagnose the problem and produce a satisfactory resolution.

The following steps offer general guidelines to help you resolve any problems you may encounter while you use NetBackup. The steps provide links to more specific troubleshooting information.

Table 1-1 Steps for troubleshooting NetBackup appliance problems

Step	Action	Description
Step 1	Note the error message	To note what has gone wrong with the appliance you can use the following options: ■ Error messages are usually the vehicle for telling you something went wrong. Refer to the error messages section in this guide and confirm the **recommended action**. You can refer to the following sections: ■ See "Error messages displayed during initial configuration" on page 182. ■ See "Error messages displayed on the NetBackup Appliance Web Console" on page 183. ■ See "Error messages displayed on the NetBackup Appliance Shell Menu" on page 203. ■ If you don't see an error message in an interface, but still suspect a problem, you can: ■ Use the **Monitor > Hardware** tab from the NetBackup Appliance Web Console to monitor the hardware, the storage devices, and all the components that are associated with them. ■ Execute a hardware self-test from theNetBackup Appliance Shell Menu using the `Support > Test` command. On completion of the hardware self test, a detailed hardware monitoring report is displayed on the NetBackup Appliance Shell Menu that can help you identify the exact issue with your appliance. ■ Check the NetBackup Appliance reports and logs. The logs show you what went wrong and the operation that was ongoing when the problem occurred. See "Locating NetBackup Appliance log files using the Browse command" on page 71. ■ If you can easily access the appliance hardware, you can identify the issues using LEDs. For more information about LED locations and interpreting them, refer to the *Symantec NetBackup 5230 Appliance Hardware Installation and Initial Configuration Guide*

Table 1-1 Steps for troubleshooting NetBackup appliance problems *(continued)*

Step	Action	Description
Step 2	Identify what you were doing, when the problem occurred	Ask the following questions: ■ What operation was tried? ■ What method did you use? For example, more than one way exists to install software on a client. Also more than one possible interface exists to use for many operations. Some operations can be performed with a script. ■ What type of server platform and operating system was involved? ■ If your site uses both the master server and the media server, was it a master server or a media server? ■ If a client was involved, what type of client was it? ■ Have you performed the operation successfully in the past? If so, what is different now? ■ What is the software version level? ■ Do you use operating system software with the latest fixes supplied,? ■ Is your device firmware at a level, or higher than the level, at which it has been tested according to the posted device compatibility lists?
Step 3	Record all information	Capture potentially valuable information: ■ Progress logs ■ Reports ■ Utility Reports ■ Debug logs ■ Check for error or status messages in the system log and Event Viewer application in case of a Windows computer. **Note:** To start the Event Viewer, from the **Start** menu, click **All Programs > Administrative Tools > Event Viewer**. ■ Error or status messages in dialog boxes See "Locating NetBackup Appliance log files using the Browse command" on page 71.

Table 1-1 Steps for troubleshooting NetBackup appliance problems *(continued)*

Step	Action	Description
Step 4	Correct the problem	If you define the issue as a NetBackup issue, you can use the following information to correct it: ■ Take the corrective action as recommended by the status code or message. See "NetBackup status codes applicable for NetBackup Appliance" on page 210. for the most common NetBackup errors or *NetBackup Status Code Reference Guide*. ■ If no status code or message exists, or the actions for the status code do not solve the problem, use additional troubleshooting procedures to isolate common problems. See "Troubleshooting generic issues" on page 91.
Step 5	Complete a problem report for Technical Support	If you can identify the logs that can help resolve the issue, collect the appropriate logs. If you cannot identify the required logs for resolving the problem, contact technical support to get advice on which logs to collect. Getting the 'support' log is the starting information to troubleshoot the issue, but other logs are required. If your troubleshooting is unsuccessful, prepare to contact Technical Support by filling out a problem report. See "About contacting Symantec Technical Support" on page 12. The `/usr/openv/netbackup/bin/goodies/support` script creates a file that contains data necessary for Technical Support to debug any problems you encounter. The support logs provide the starting point to troubleshoot the issue. You may need to collect other logs in case the issue cannot be resolved using the support logs. See "Viewing log files using the Support command" on page 70.
Step 6	Contact Technical Support	The Symantec Technical Support website has a wealth of information that can help you solve NetBackup problems. Access Technical Support at the following URL: www.symantec.com/business/support/ See "About contacting Symantec Technical Support" on page 12.

Chapter 2

Best practices

This chapter includes the following topics:

- About best practices
- Locating the NetBackup Appliance serial number
- Web browsers supported by Appliance
- About Fibre Channel HBA card configuration verification
- About Notification settings
- About the IPMI sub-system
- About password management and recovery
- About IPv4-IPv6-based network support
- About enabling BMR options
- Interpretation of some of the fields of vxprint output from NetBackup and PureDisk appliances
- About deleting LDAP or Active Directory users

About best practices

This section lists the best practices for working with the appliance hardware and software. It includes the following sections:

Table 2-1 Sections in the best practices chapter

Section	Description	Link
Locating the NetBackup Appliance serial number	This section provides the steps to obtain the serial number of your appliance.	See "Locating the NetBackup Appliance serial number" on page 19.
Web browsers supported by NetBackup Appliance Web Console	This section provides the guidelines to view the NetBackup Appliance Web Console your browsers.	See " Web browsers supported by Appliance" on page 22.
About Fibre Channel HBA card configuration verification	This section provides the steps to verify the installation and configuration of a SAN Client Fibre Channel HBA card.	See "About Fibre Channel HBA card configuration verification" on page 25.
About Notification settings	This section provides the importance for enabling the Notification and Registration setting.	See "About Notification settings" on page 27.
About the IPMI sub-system	This section provides a brief description on why IPMI sub-systems are vital and need to be configured for your appliance.	See " About the IPMI sub-system" on page 27.
About password management and recovery	This section provides the steps to be followed to recover your password.	See "About password management and recovery" on page 28.
About IPv4 and IPv6 network support	This section provides the guidelines for configuring the IPV4 and IPV6 addresses.	See "About IPv4-IPv6-based network support" on page 29.
About enabling BMR options	This section provides a brief description on the application and benefits of enabling the BMR options when the appliance is configured as a master server.	See "About enabling BMR options" on page 30.

Table 2-1 Sections in the best practices chapter *(continued)*

Section	Description	Link
Interpretation of some of the fields of `vxprint` output from NetBackup and PureDisk appliances	This section provides an explanation of how to interpret the vxprint output.	See "Interpretation of some of the fields of `vxprint` output from NetBackup and PureDisk appliances" on page 31.
About deleting LDAP or Active Directory users	This section provides the precautions you need to take while deleting LDAP or Active Directory users from the NetBackup Appliance.	See "About deleting LDAP or Active Directory users" on page 32.

In addition to these sections, you can also refer to the best practices specific to disaster recovery, for more information See "Disaster recovery best practices" on page 130.

Locating the NetBackup Appliance serial number

You need to note and refer to the NetBackup Appliance serial number when you report an issue to Symantec support.

You can use either of the following options to locate the NetBackup Appliance serial number.

- **Monitor > Hardware > Health details** from the NetBackup Appliance Web Console.
- `Monitor > Hardware ShowHealth Appliance [Item]` Command from the shell menu.

To locate the NetBackup Appliance serial number from the NetBackup Appliance Web Console:

1. Log on to the NetBackup Appliance Web Console using your user credentials.
2. Select **Monitor > Hardware**
3. From the left-pane, click on the appliance name.

   The appliance displays the **Hardware health details** page.
4. On the **Hardware health details** page, click the media server or master server icon. For example, if you want to locate the serial number of a media server, click on the media server icon.

The appliance displays the **Media Server Details** pop-up box, with the following information:

- NetBackup Appliance Hardware platform, for example - 5220 or 5230
- Version of the NetBackup Appliance installed on the appliance, for example - 2.6
- Serial number of the NetBackup Appliance

For more information, refer to the *Symantec NetBackup Appliance Administrator's Guide Release 2.6.0.2*

To locate the NetBackup Appliance serial number in a 52xx NetBackup appliance using the shell menu:

1. Log on to the administrative NetBackup Appliance Shell Menu.
2. Enter the `Monitor > Hardware ShowHealth Appliance [Product]` command, where `[Product]` is the value for the `[Item ]` parameter.

   The serial number of your appliance is displayed, as seen in the following example:

```
abc123.Monitor > Hardware ShowHealth Appliance Product

Gathering hardware information. It might take about a minute...

Compute Node abc123.engba.symantec.com

Time Monitoring Ran: Thu Mar 21 2013 04:47:09 PDT

Node does not have any errors.

+-----------------------------------------------------------------+
|                    Hardware monitor information                 |
|+----------------------------------------------------------------+|
||           name        |     manufacturer    |         serial   ||
||-----------------------+---------------------+------------------||
||NetBackup 5230         |Symantec             |abc123serno       ||
|+----------------------------------------------------------------+|
+-----------------------------------------------------------------+
```

For more information, refer to the *Symantec NetBackup Appliance Command Reference Guide*.

See “About best practices” on page 17.

Locating hardware serial numbers

If you cannot connect to the appliance or the storage shelf you can locate the serial numbers from the actual hardware.

The serial number of the NetBackup 5230 appliance is located in two places:

- On a tab that you pull out from the front left side of the appliance.

- On a vertical bar in the rear panel of the appliance.

The serial number of the NetBackup 5220 appliance is located on the rear panel of the appliance. The label is on a thin metal strip near the IPMI port.

The serial number of the Symantec Storage Shelf is located on the rear panel of the storage shelf. On the right side of the shelf pull the white tab from the storage shelf.

Earlier models may have two numbers. The HOST number applies to an appliance, which you can disregard. In these models the STORAGE number is the serial number for the storage shelf.

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 2-2 lists the Web browsers that Appliance supports.

Table 2-2 Web browsers supported by Appliance

Web browser	Supported Versions	Notes
Microsoft Internet Explorer	8.0 and higher **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 later in a compatible mode. From your browser, use the **Tools > Compatibility View Settings** menu and uncheck **Display all websites in Compatibility view** to see the Appliance Web Console.
Mozilla Firefox	21.0 and higher **Note:** If you try to access the NetBackup Appliance using earlier versions of Firefox and reset the password using Settings > Password, the page may hang.	Mozilla Firefox may display an **Untrusted Connection** page when you access the NetBackup Appliance Web Console. See "Disabling the Untrusted Connection page in Mozilla Firefox" on page 24.

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.

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 Fibre Channel HBA card configuration verification

After you install and configure a Fibre Channel HBA card on the appliance as Fibre Transport media server to use with SAN clients, you may want to verify that at it is configured properly. To do that, use the `Main_Menu > Manage > FibreChannel > Show` command from the command line interface. When you run the `Main_Menu`

`> Manage > FibreChannel > Show` command and the HBA card was configured properly, you see an output that is similar to the following:

```
Testsys.FC> Show
FC HBA card(s) are configured correctly.

**** FC HBA Cards ****
02:00.0 Fibre Channel: QLogic Corp. ISP2432-based 4Gb Fibre Channel
to PCI Express HBA (rev 03)
02:00.1 Fibre Channel: QLogic Corp. ISP2432-based 4Gb Fibre Channel
to PCI Express HBA (rev 03)
03:00.0 Fibre Channel: QLogic Corp. ISP2532-based 8Gb Fibre Channel
to PCI Express HBA (rev 02)
03:00.1 Fibre Channel: QLogic Corp. ISP2532-based 8Gb Fibre Channel
to PCI Express HBA (rev 02)
06:00.0 Fibre Channel: QLogic Corp. ISP2532-based 8Gb Fibre Channel
to PCI Express HBA (rev 02)
06:00.1 Fibre Channel: QLogic Corp. ISP2532-based 8Gb Fibre Channel
to PCI Express HBA (rev 02)

**** Drivers ****
qla2xxx     is loaded
windrvr6    is loaded

**** Ports ****
Bus ID Slot  Port WWN     Status     Mode       Speed  Remote Ports
2:00.0 Slot3 21:00:...:07 Linkdown   Initiator  4 gb/s
2:00.1 Slot3 21:01:...:07 Linkdown   Initiator  4 gb/s
3:00.0 Slot2 21:00:...:30 Disconnect Target     8 gb/s
3:00.1 Slot2 21:00:...:31 Online     Initiator  2 gb/s 0x21000024...
6:00.0 Slot1 21:00:...:82 Fabric     Target     8 gb/s
6:00.1 Slot1 21:00:...:83 Online     Initiator  8 gb/s 0x21000024...

*** Devices ****
Device   Vendor    Host         Type               Remote Port
/dev/sg0 SYMANTEC  10.182.0.209 FCPIPE  (NBU 50x0) 0x21000024ff232438
/dev/sg2 SYMANTEC  10.182.0.209 FCPIPE  (NBU 50x0) 0x21000024ff3162be

*** Notes ****
(NOTE: Ports in mode "Initiator*" are configured for target mode
When SAN Client FT Media Server is active, however, are currently
running in initiator mode, i.e. SAN Client is disabled or inactive.)
```

About Notification settings

You can use the **Settings > Notification > Alert Configuration** from the NetBackup Appliance Web Console to apply the Call Home settings. 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 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 there is a problem with a piece of hardware, you might want to contact Symantec Technical Support. The Technical Support engineer uses the serial number of your appliance and assesses the hardware status from the Call Home data.

Note: 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.

NetBackup Appliance supports all the SNMP servers in the market. However, the following SNMP servers are tested and certified for using with version 2.6.0.x:

- ManageEngine™ SNMP server
- HP OpenView SNMP server

Also ensure that you register the appliance and your contact information using the **Settings > Notification > Registration** menu. Registering your NetBackup appliance helps to make sure that you are alerted to product updates and other important information about your appliance.

See “About best practices” on page 17.

See “Locating the NetBackup Appliance serial number” on page 19.

About the IPMI sub-system

Ensure that the IPMI sub-system is configured 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 using the IPMI port, located on the rear panel of the appliance.

An IPMI lets you monitor and manage your appliance from a remote location by using the Integrated Storage Manager (ISM) 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.

Some of the main uses of IPMI are the following:

- Manage a system remotely in the absence of an operating system
- Change BIOS settings
- Turn on, turn off, or recycle the system
- Situations where local access using a 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.

Note: You can also use the IPMI sub-system to reimage your NetBackup Appliance.

For the detailed steps on configuring the IPMI sub-system, refer to the *IPMI Configuration* section from the *Symantec NetBackup 52xx Appliance Administrator's Guide*.

See "About best practices" on page 17.

About password management and recovery

Symantec understands that there may be situations where you need to recover your administrator (admin) password. Password recovery for users can be approached based on the following approaches:

Table 2-3 Password recovery for local and LDAP users

User Type	Steps to change password	Steps to recover password
Local Users	Use the **Settings > Password Management** tab from the NetBackup Appliance Web Console.	Contact the Symantec Technical Support for changing the password. An employee that maintains the password may leave the company, or you may lose or forget the password. If any of these situations occur, contact Symantec Technical Support for assistance.

Table 2-3 Password recovery for local and LDAP users *(continued)*

User Type	Steps to change password	Steps to recover password
LDAP Users	Use the following steps to reset or change the password for an LDAP user: ■ Update the user password in the Active Directory of your LDAP server. ■ Use the **Settings > Password Management** tab from the NetBackup Appliance Web Console.	Considering the example when an LDAP user leaves the company, or may lose or forget the password. Use the following steps to reset or change the password for an LDAP user: ■ Recover the password using the Active Directory of your LDAP server. ■ Contact the Symantec Technical Support for changing the password.

See "About best practices" on page 17.

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*.

About enabling BMR 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. BMR is the server recovery option of NetBackup that automates and streamlines the server recovery process. Thus making it unnecessary to manually reinstall the operating systems or configure hardware. 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)

For more information about the recovery process using BMR, refer to the *BMR Administrator's Guide*.

See "About best practices" on page 17.

Interpretation of some of the fields of `vxprint` output from NetBackup and PureDisk appliances

The output of the `vxprint` command displays the layout and configuration of NetBackup appliances, including volumes, disks, and subdisks. This section explains the different columns in `vxprint` output from all versions of NetBackup and PureDisk appliances. This helps the field engineers, support engineers, consultants, the customers, and the partners understand the volumes layout and how much spaces are allocated to different volumes for configuration and troubleshooting purposes.

Let us consider an example of a `vxprint` output from a NetBackup 5220 appliance running version 2.0.2 where a Symantec Storage Shelf is attached to the Base Unit:

```
# vxprint
Disk group: nbuapp

TY NAME       ASSOC      KSTATE   LENGTH       PLOFFS  STATE    TUTIL0  PUTIL0
dg nbuapp     nbuapp     -        -            -       -        -       -

dm disk_1     disk_1     -        9755774656   -       -        -       -
dm disk_2     disk_2     -        76171777984  -       -        -       -

v  advol      fsgen      ENABLED  1560281088   -       ACTIVE   -       -
pl advol-01   advol      ENABLED  1560281088   -       ACTIVE   -       -
sd disk_1-02  advol-01   ENABLED  1560281088   0       -        -       -

v  catvol     fsgen      ENABLED  1951154176   -       ACTIVE   -       -
pl catvol-01  catvol     ENABLED  1951154176   -       ACTIVE   -       -
sd disk_1-01  catvol-01  ENABLED  2097152      0       -        -       -
sd disk_1-03  catvol-01  ENABLED  1949057024   2097152 -        -       -

v  pdvol      fsgen      ENABLED  6243221504   -       ACTIVE   -       -
pl pdvol-01   pdvol      ENABLED  6243221504   -       ACTIVE   -       -
sd disk_1-04  pdvol-01   ENABLED  6243221504   0       -        -       -
```

Row/Column	Description
`dm rows`	These rows list two disks named `disk_1` and `disk_2`. The `disk_1` is the base 5220 unit, `disk_2` is the storage from the Storage Shelf attached to the Base unit. The storage belonging to the Storage Shelf may be disk_2, or disk_3, or disk_0 or any other number.
`Volume names`	The volume names are in the 2nd columns in rows starting with 'v' (abbreviation for volumes). For example, `advol` - displays AdvancedDisk volume, `catvol` - displays for catalog volume, and `pdvol` - displays for PureDisk volume In the 3rd columns in rows starting with `pl` (plexes) subdisk names are listed in 2nd column in rows starting with 'sd' (subdisk). If the name of the subdisk and volume is followed, it can be identified which disk a particular volume resides in. For example, `catvol` is on `disk_1`.
`Length`	The `LENGTH` column provides information in 512 bytes. To get the size in KB, divide the `LENGTH` value by 2. Then keep dividing the result by 1024 to get to GB or TB For example, the catvol`LENGTH` column displays the value is 1951154176 which is 930 GB.

See “About best practices” on page 17.

About deleting LDAP or Active Directory users

When you delete an LDAP or Active Directory user, ensure that you delete the user from the NetBackup Appliance. If you delete a user from the LDAP or Active Directory before deleting it from the NetBackup Appliance results in an error condition.

Note: If the user is removed from the LDAP directory (and not removed from appliance allowed to log in list), though the user is listed as LDAP authorized user, the user will not be able to log in. So, these users poses no security threat.

For example, you want to delete user John Doe from the LDAP server and the NetBackup Appliance. You delete the user entry for John Doe from your LDAP server. Then you log into the NetBackup Appliance Shell Menu and to remove a user using the `LDAP > Users Remove` *`John Doe`* command. The appliance does not recognize the user and displays the following error:

```
The user name that you have entered is not valid. Enter a valid user name.
```

See “About best practices” on page 17.

Chapter 3

About Software Troubleshooting Tools

This chapter includes the following topics:

- Tools for troubleshooting the NetBackup Appliance
- Troubleshooting and tuning Appliance from the Appliance Diagnostics Center
- About NetBackup support utilities
- About changing VxAT properties

Tools for troubleshooting the NetBackup Appliance

This chapter describes the tools and commands used to diagnose the issues faced by your NetBackup Appliance, it includes the following sections:

Table 3-1 Sections in the Software Troubleshooting Tools chapter

Section	Description	Link
Troubleshooting and tuning your appliance using the Appliance Diagnostics Center	This section describes the Appliance Diagnostics Center used to troubleshoot multiple failures and resolve issues in the NetBackup Appliance by using some interactive self-repair wizards.	See "Troubleshooting and tuning Appliance from the Appliance Diagnostics Center" on page 35.
About NetBackup support utilities	This section describes the NetBackup support utilities supported by the NetBackup Appliance.	See "About NetBackup support utilities" on page 40.

Table 3-1 Sections in the Software Troubleshooting Tools chapter *(continued)*

Section	Description	Link
About changing VxAT properties	This section describes the script used to configure the Symantec Product Authentication Service (AT) Server parameters	See "About changing VxAT properties" on page 42.

See "About this guide" on page 11.

Troubleshooting and tuning Appliance from the Appliance Diagnostics Center

You can troubleshoot multiple failures and resolve issues in the NetBackup Appliance by using some interactive self-repair wizards in the Appliance Diagnostics Center. Each wizard helps you perform specific diagnostic tasks. Some of the wizards also guide you through system optimization and tuning. These wizards can be accessed by clicking the Appliance Diagnostics Center icon on theNetBackup Appliance Web Console. The icon is located on the upper-right corner of the NetBackup Appliance Web Console and looks like the following:

When you click this icon, the Appliance Diagnostics Center page appears where you can see the **Available** and the **Running Wizard Jobs** tab. You can return to theNetBackup Appliance Web Console by closing this page.

All the troubleshooting wizards are listed under the **Available** tab.

Figure 3-1 shows a sample view of the **Available** tab.

Figure 3-1 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 3-2 shows a sample view of the **Running Wizard Jobs** tab.

Figure 3-2 Running Wizard Jobs tab

You can do the following to run the wizards from the **Available** tab:

Click **Test Call Home functionality**	Use this wizard to troubleshoot Call Home failures. The wizard checks if Call Home is enabled, the Call Home proxy server (or proxy server) is enabled, and if Appliance, proxy server, and the Symantec Call Home server can communicate.
Click **Check Disk Configuration**	Use this wizard to troubleshoot disk storage issues, tuning, and availability. The wizard checks the storage partitions like AdvancedDisk, etc., and does the following: ■ 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**	Use this wizard to collect log files from an Appliance. You can do any of the following: ■ Collect log files for a 52x0 appliance. 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. Table 3-2 lists details about the log files that are collected by the wizard. You can choose to email the log files to recipients, download to your computer, or upload them to Symantec Support. Review the following points if you want to email the log files: ■ SMTP must be configured for emailing the logs. You can configure SMTP from **Settings > Notification > Alert Configuration** in the NetBackup Appliance Web Console. ■ To email the logs, the collected log size must be 10 MB or less.
Click **Perform a hardware health check**	Use this wizard to perform a hardware health check of your environment. The wizard helps you determine if hardware components like CPU, Disk, Fan, RAID, are working fine.
Click **Test and diagnose network issues**	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.

Table 3-2 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 3-2 Log files collected by the Collect Logs Wizard

Log Type	What is collected?
NetBackup	Logs created by the NetBackup Copy Logs tool (`nbcplogs`). These include the following: ■ NetBackup legacy logs ■ NetBackup VxUL (Unified) logs ■ NetBackup OpsCenter logs ■ NetBackup PureDisk logs ■ Windows Event logs (Application, System, Security) ■ PBX logs ■ NetBackup database logs ■ NetBackup database error logs ■ NetBackup database trylogs ■ Vault session logs ■ Volume Manager debug logs ■ VxMS logs, if enabled **Note:** The legacy logs and the VXlogs are collected based on the time frame that you specify.

Table 3-2 Log files collected by the Collect Logs Wizard *(continued)*

Log Type	What is collected?

Appliance	Appliance logs including upgrade, hardware, event logs and so on. The following Appliance logs are collected:
	■ `hostchange.log`, `selftest_report*`
	■ Logs created by the `CallhomeDataGather` utility.
	■ `config_nb_factory.log`, `iso_postinstall.log`, `sf.log`
	■ `patch_*`, `upgrade_* logs`
	■ NetBackup Appliance VxUL (Unified) logs, which include:
	  ■ `All`
	  ■ `CallHome`
	  ■ `Checkpoint`
	  ■ `Common`
	  ■ `Config`
	  ■ `Database`
	  ■ `Hardware`
	  ■ `HWMonitor`
	  ■ `Network`
	  ■ `RAID`
	  ■ `Seeding`
	  ■ `SelfTest`
	  ■ `Storage`
	  ■ `SWUpdate`
	  ■ `Commands`
	  ■ `CrossHost`
	  ■ `Trace`
	Note: The NetBackup Appliance unified logs are not the same as the NetBackup unified logs, such as `nbpem` or `nbjm`. NetBackup Appliance has its own set of unified logs. To collect the NetBackup unified logs, select **NetBackup** in the Collect Logs Wizard.

Operating system	Operating system logs that include the following: ■ `boot.log` ■ `boot.msg` ■ `boot.omsg` ■ `messages`

Table 3-2 Log files collected by the Collect Logs Wizard *(continued)*

Log Type	What is collected?
Deduplication (Media Server Deduplication Pool or PureDisk)	All logs related to Media Server Deduplication Pool (MSDP) are collected under the following directories: <DIR> PD ■ `/var/log/puredisk` ■ `/disk/log`
NetBackup Appliance Web Console	All logs related to NetBackup Appliance Web Console logs are collected under the following directories: `/log/webgui`
NetBackup support utility (`nbsu`)	Diagnostic information about NetBackup and the operating system.
DataCollect	Hardware and storage device logs. The logs created by the `DataCollect` utility are collected.

About NetBackup support utilities

The NetBackup 52xx provides the following support utilities to help diagnose NetBackup problems:

- NetBackup Domain Network Analyzer (NBDNA)
- NetBackup Support Utility (nbsu)

NetBackup Domain Network Analyzer (NBDNA)

You can run the NBDNA utility on a NetBackup primary or secondary appliance to perform the following tasks:

- Identifying the NetBackup domain configuration to resolve network-related issues
- Identifying the NetBackup performance issues
- Ensuring the behavior with regards to the host name lookup is functional
- Ensuring that the connectivity between NetBackup hosts and the appliance is established and functional based on their role within the NetBackup domain
- Generating the reports that are meant for Symantec Technical Support.

The NBDNA utility provides the following types of information in its output:

```
Running audit as Media Server.

Collection Version: x.x
   Collection Time: Tuesday, October 7, 2010 at 19:17:11 PM
       NBU Release: NetBackup-SuSE2.6.16 7.0.1.5
       NBU Version: 7.0.1.5
 NBU Major Version: 7.0
 NBU Minor Version: 1
    NBU Patch Type: GA
   NBU GlobDB Host: "host name"
    Is GlobDB HOST? No
             UNAME:
          Hostname: sample.name.symantec.com
  Host's  Platform: Linux
 Perl Architecture: Linux

Initialization completed in 14.040101 seconds.


Brief Description of What It Does (for type 1):
----------------------------------------------------
 1) Perform basic self checks.
 2) Check connectivity to Master (and EMM) server.
 3) If SSO configured, get list of media servers sharing devices.
 4) Get list of all clients which could send data here for backup.
 5) Test NBU ports for basic connectivity between media servers
    sharing devices.
 6) Test NBU ports for basic connectivity between media server and
    clients it backs up.
 7) Perform service level tests for phase 2
 8) Capture data for reports; save reports.
 9) Save data to report files.
----------------------------------------------------

Discovering and mapping the NetBackup domain network for analysis
by extracting data from current system's configuration.
 (To see more details, consider using '-verbose' switch.)

Probing Completed in 4.695464 seconds.

Initiating tests...

COMPLETED.  Thank you for your patience.
```

```
/log/dna/sample.name.symantec.com.NBDNA.20100907.191711.zip
Archive created successfully!
Return /log/dna/sample.name.symantec.com.NBDNA.20100907.191711.zip
to Symantec Support upon request.
```

NetBackup Support Utility (nbsu)

You can use the `nbsu` utility to gather appropriate diagnostic information about NetBackup and the operating system. The *Symantec NetBackup Troubleshooting Guide* describes when you would use this utility, as well as how to run it.

See "Tools for troubleshooting the NetBackup Appliance" on page 34.

About changing VxAT properties

When troubleshooting your appliance, you may need to configure the Symantec Product Authentication Service (AT) Server parameters. You can update these parameters using the `changeVxATProperties` script.

Enter the following command to configure the AT parameters on UNIX:

```
/opt/SYMCOpsCenterServer/bin/changeVxATProperties.sh
```

The `changeVxATProperties` script prompts you to enter the following details:

- **Authentication Service Host Name**
- **Authentication Service Port Number**
- **Authentication Service Domain Name**
- **Authentication Service Domain Name**
- **Authentication Service Password**

See "Tools for troubleshooting the NetBackup Appliance" on page 34.

Chapter 4

About the NetBackup appliance hardware

This chapter includes the following topics:

- About the NetBackup 5230 appliance hardware
- About the NetBackup 5220 appliance hardware
- About the NetBackup 5030 Appliance hardware
- About the cables
- About rack mounting

About the NetBackup 5230 appliance hardware

This section provides information about the NetBackup 5230 appliance.

See "Specifications for the NetBackup 5230 Appliance" on page 43.

See "About the NetBackup 5230 appliance bezel" on page 45.

See "About the NetBackup 5230 Appliance front panel" on page 46.

See "About the NetBackup 5230 Appliance rear panel" on page 48.

See "*About the NetBackup appliance hardware*" on page 43.

Specifications for the NetBackup 5230 Appliance

This section provides information about types of specifications for the NetBackup 5230.

See "NetBackup 5230 Appliance dimensions" on page 44.

See "NetBackup 5230 Appliance environmental specifications" on page 44.

See "NetBackup 5230 Appliance hardware components" on page 45.

See "About the NetBackup 5230 appliance bezel" on page 45.

See "About the NetBackup 5230 Appliance front panel" on page 46.

See "About the NetBackup 5230 Appliance rear panel" on page 48.

See "*About the NetBackup appliance hardware*" on page 43.

NetBackup 5230 Appliance dimensions

This section provides information about the physical specifications for NetBackup 5230 appliances.

- 3.45 inches (87.60 mm) high
- 19.13 inches (486 mm) wide
- 28.82 inches (732.2 mm) deep
- 52 pounds (23.58 kg) - maximum chassis weight

See "NetBackup 5230 Appliance environmental specifications" on page 44.

See "NetBackup 5230 Appliance hardware components" on page 45.

See "Specifications for the NetBackup 5230 Appliance" on page 43.

NetBackup 5230 Appliance environmental specifications

This section provides information about the environmental specifications for NetBackup 5230 appliances.

- Operating temperature: 50° F to 95° F (10° C to 35° C) with maximum rate of change not to exceed 10° C per hour
- Non-operating temperature: -40° F to 140° F(-40° C to 60° C)
- Operating humidity: 8% to 80% non-condensing
- Non-operating humidity: 90% non-condensing @ 35°C
- Operating shock: Half sine, 2g peak, 11ms duration
- Non-operating shock: 10g amplitude, 11ms duration
- Altitude: 0 FT to 7000 FT (2100 m) or 0 FT to 10,000 FT (3000 m) @ less than 95° F (35° C)

You can find additional specification information for the NetBackup 5230 at the following:

See "NetBackup 5230 Appliance dimensions" on page 44.

See "NetBackup 5230 Appliance hardware components" on page 45.

See "Specifications for the NetBackup 5230 Appliance" on page 43.

NetBackup 5230 Appliance hardware components

This section provides information about the hardware that is used in NetBackup 5230 appliances.

- Two Intel® Sandy Bridge® processors
- Memory
  - 64 GB RDIMM @ 1333Hz without Symantec Storage Shelf
  - 128 GB RDIMM @ 1333Hz with Symantec Storage Shelf
- Two 1-TB system-disk drives (hot-swappable)
- Eight 1-TB storage disk drives (hot-swappable)
- One 1 Gb Ethernet ports (eth0) for administrative use
- Three 1 Gb Ethernet ports (eth1 thru eth3) for public use
- Two 10 Gb Ethernet ports (eth4 and eth5)
- Remote Management interface support
- Three USB 2.0 connectors
- RJ-45 serial port A connector
- DB-15 video connector
- Two 750W hot-swappable power supplies
- Five fans (internal)
- Maintenance free battery unit (MFBU)

See "NetBackup 5230 Appliance dimensions" on page 44.

See "NetBackup 5230 Appliance environmental specifications" on page 44.

See "Specifications for the NetBackup 5230 Appliance" on page 43.

About the NetBackup 5230 appliance bezel

Symantec provides a bezel that attaches to the front of the NetBackup 5230 appliance. The bezel is designed to maximize the air flow through the unit. The bezel should be installed to enhance ventilation and to protect the disk drives.

See "Specifications for the NetBackup 5230 Appliance" on page 43.

See "About the NetBackup 5230 Appliance front panel" on page 46.

See "About the NetBackup 5230 Appliance rear panel" on page 48.

You can find additional information about appliance hardware at the following:

See "*About the NetBackup appliance hardware*" on page 43.

About the NetBackup 5230 Appliance front panel

The front panel of the servers of NetBackup Appliances house drives and a control panel. This section describes the server front panel.

See "About drive slots in the NetBackup 5230" on page 46.

See "About LEDs for the drive slot" on page 47.

See "About the NetBackup 5230 Appliance control panel" on page 47.

About drive slots in the NetBackup 5230

The NetBackup 5230 Appliance front panel contains 12 drive slots and a control panel. Ten of the drive bays are used. The drives in slots 0 and 1 are the system drives. These drives are mirrored to provide RAID 1 parity. The drives in slots 4 through 11 provide the RAID-enabled storage. The drive in Slot 11 is the hot spare. Slots 2 and 3 are not used. Blank carriers are installed in slots 2 and 3 to maintain proper airflow within the appliance.

Figure 4-1 shows the drive layout for NetBackup 5230 Appliances. System drives are shown in section 1. Storage drives are shown in section 2.

Note: Additional storage can be added to the NetBackup 5230 using Symantec Storage Shelves.

Figure 4-1 NetBackup 5230 Appliance front panel

All NetBackup 5230 Appliance drives are hot-swappable. However, at least one of the system drives (slots 0 and 1) must operate at all times. The appliance cannot function without an operating system.

See “About LEDs for the drive slot” on page 47.

See “About the NetBackup 5230 Appliance control panel” on page 47.

See “About the NetBackup 5230 Appliance front panel” on page 46.

About LEDs for the drive slot

Each drive slot has two LEDs. The LEDs are located on the edge of the drive facade to the left of the handle. See Figure 4-2 on page 47..

Figure 4-2 LEDs for the disk drive

The LEDs provide the following information:

- The top LED is solid green when power is supplied to the drive. This LED flashes green when the disk drive is active.
- The bottom LED is solid amber when a drive fault occurs. This LED is not lit when there are no disk drive faults.
- The bottom LED flashes amber during the following conditions:
  - The drive is involved in a copyback operation.
  - When an identify command is issued that allows the drive to be located.

Warning: Removing the drive from the slot when it is not in a safe state can cause equipment damage, loss of data, and data corruption. The drive is in a safe state when the bottom LED is solid amber or the drive power and activity LED is off.

See “About drive slots in the NetBackup 5230” on page 46.

See “About the NetBackup 5230 Appliance front panel” on page 46.

See “About the NetBackup 5230 Appliance front panel” on page 46.

About the NetBackup 5230 Appliance control panel

The appliance control panel is located on the right-hand side of the front panel and lets you monitor server activity. Figure 4-3 shows the elements in the control panel. Table 4-1 describes the elements in the control panel.

Figure 4-3 LEDs for the appliance control panel

Table 4-1 NetBackup 5230 control panel LEDs

Label	Description
1	AC power button
2	Disk drive activity LED
3	Appliance ID button
4	Cold reset button
5	NIC4 activity LED
6	NIC3 activity LED
7	Not used
8	NIC1 activity LED
9	NIC2 activity LED
10	Appliance status LED

See "About drive slots in the NetBackup 5230" on page 46.

See "About LEDs for the drive slot" on page 47.

See "About the NetBackup 5230 Appliance front panel" on page 46.

About the NetBackup 5230 Appliance rear panel

The NetBackup 5230 Appliance rear panel provides access to the communication ports and the hot-swappable power supplies. How the appliance is provisioned and configured at the factory determines the number and type of communication ports

available on an appliance. This section provides the information about the rear panel of different appliance configurations.

1. A single FC HBA card is installed. You can connect the FC ports to Fibre Transport data transfer clients or other devices. This appliance configuration is not used with a storage shelf.

Number	Port
1	1Gb Ethernet (NICs 1-4 (eth0 to eth3) from left to right) ■ NIC 1 is used for administrative purposes only ■ NIC 2, NIC 3, and NIC 4 are used for public networks only
2	Video Graphics Array (VGA)
3	Serial port
4	Three USB ports
5	Administrative port
6	Two 10Gb Ethernet ports
7	Two Fibre Channel (FC) ports

2. In configuration two, a single RAID controller is installed into Slot 1. The SAS ports on the RAID controller connect to the SAS_IN ports on the storage shelf. The SAS_OUT ports are used to connect additional storage shelves.

   One FC HBA card is installed. You can connect the FC ports to Fibre Transport data transfer clients or other devices.

Number	Port
1	1Gb Ethernet (NICs 1-4 (eth0 to eth3) from left to right) ■ NIC 1 is used for administrative purposes only ■ NIC 2, NIC 3, and NIC 4 are used for public networks only
2	Video Graphics Array (VGA)
3	Serial port
4	USB (qty 3)
5	Administrative port
6	10Gb Ethernet (qty 2)
7	SAS RAID controller (qty 2)
8	Fibre Channel (FC) (qty 2)

3. In configuration three, a single RAID controller is installed into Slot 1. The SAS ports on the RAID controller connect to the SAS_IN ports on the storage shelf. The SAS_OUT ports are used to connect additional storage shelves.

   One 10Gb Ethernet card is installed. You can connect the Ethernet ports to other devices that are connected to your network.

Number	Port
1	1Gb Ethernet (NICs 1-4 (eth0 to eth3) from left to right) ■ NIC 1 is used for administrative purposes only ■ NIC 2, NIC 3, and NIC 4 are used for public networks only
2	Video Graphics Array (VGA)
3	Serial port
4	Three USB ports
5	Administrative port
6	Two 10Gb Ethernet ports
7	Two 10Gb Ethernet ports
8	Two SAS RAID controller ports
9	Two Fibre Channel (FC) ports

4. In configuration four, a single RAID controller is installed into Slot 1. The SAS ports on the RAID controller connect to the SAS_IN ports on the storage shelf. The SAS_OUT ports are used to connect additional storage shelves.

   Four FC HBA cards are installed. You can connect the FC ports to Fibre Transport data transfer clients or other devices.

   One 10Gb Ethernet card is installed. You can connect the Ethernet ports to other devices that are connected to your network.

Number	Port
1	1Gb Ethernet (NICs 1-4 (eth0 to eth3) from left to right) ■ NIC 1 is used for administrative purposes only ■ NIC 2, NIC 3, and NIC 4 are used for public networks only
2	Video Graphics Array (VGA)

Number	Port
3	Serial port
4	Three USB ports
5	Administrative port
6	Two 10Gb Ethernet ports
7	Two 10Gb Ethernet ports
8	Two SAS RAID controller ports
9	Eight Fibre Channel (FC) ports

5. In configuration five, a single RAID controller is installed into Slot 1. The SAS ports on the RAID controller connect to the SAS_IN ports on the storage shelf. The SAS_OUT ports are used to connect additional storage shelves.

   Five FC HBA cards are installed. You can connect the FC ports to Fibre Transport data transfer clients or other devices.

   No Ethernet cards are included in this configuration.

Number	Port
1	1Gb Ethernet (NICs 1-4 (eth0 to eth3) from left to right) ■ NIC 1 is used for administrative purposes only ■ NIC 2, NIC 3, and NIC 4 are used for public networks only
2	Video Graphics Array (VGA)
3	Serial port
4	Three USB ports
5	Administrative port
6	Two 10Gb Ethernet ports

Number	Port
7	Two SAS RAID controller ports
8	Ten Fibre Channel (FC) ports

Other configurations or other cards in the PCIe slots of the NetBackup 5230 are not supported.

See "Specifications for the NetBackup 5230 Appliance" on page 43.

See "About the NetBackup 5230 Appliance front panel" on page 46.

See "NetBackup 5230 Appliance hardware components" on page 45.

See "*About the NetBackup appliance hardware*" on page 43.

About the NetBackup 5220 appliance hardware

This chapter provides information about NetBackup 5220 appliance hardware.

See "Specifications for the NetBackup 5220 Appliance" on page 53.

See "NetBackup 5220 Appliance front panel" on page 55.

See "NetBackup 5220 Appliance rear panel" on page 59.

Specifications for the NetBackup 5220 Appliance

This section provides information about types of specifications for the NetBackup 5220.

See "NetBackup 5220 Appliance physical dimensions" on page 53.

See "NetBackup 5220 Appliance environmental specifications" on page 54.

See "NetBackup 5220 Appliance hardware" on page 54.

NetBackup 5220 Appliance physical dimensions

This section provides information about the physical specifications for NetBackup 5220 appliances.

- 3.44 inches (87.30 mm) high
- 16.93 inches (430 mm) wide
- 27.75 inches (704.8 mm) deep
- 65 pounds (29.5 kg) - maximum chassis weight

Note: Weight is without drives installed.

See "NetBackup 5220 Appliance environmental specifications" on page 54.

See "NetBackup 5220 Appliance hardware" on page 54.

See "Specifications for the NetBackup 5220 Appliance" on page 53.

NetBackup 5220 Appliance environmental specifications

This section provides information about the physical specifications for NetBackup 5220 appliances.

- Operating temperature: 50° F to 95° F (10° C to 35° C) with maximum rate of change not to exceed 10° C per hour
- Non-operating temperature: -40° F to 140° F(-40° C to 60° C)
- Non-operating humidity: 90% non-condensing @ 28°C
- Operating shock: Half sine, 2g peak, 11ms duration
- Vibration: 5Hz to 500 Hz, 2.2g RMS random

See "NetBackup 5220 Appliance physical dimensions" on page 53.

See "NetBackup 5220 Appliance hardware" on page 54.

See "Specifications for the NetBackup 5220 Appliance" on page 53.

NetBackup 5220 Appliance hardware

This section provides information about the physical specifications for NetBackup 5220 appliances.

- Support for one or two Intel® Xeon® processors in FC-LGA 1366 Socket B package with up to 95 W Thermal Design Power (TDP)
- Memory:
  - 48 GB RDIMM @ 1066Hz without Symantec Storage Shelf
  - 96 GB RDIMM @ 1066Hz without Symantec Storage Shelf
- Two 1-TB system-disk drives
- Eight 1-TB storage disk drives (hot-swappable)
- One 1 Gb Ethernet ports (eth0), private network port
- One 1 Gb Ethernet ports (eth1), service network port
- Remote Management interface support

- Four USB 2.0 connectors
- RJ-45 serial port A connector
- VGA connector
- Two 750W hot-swappable power supplies
- Six fans (internal)

See "NetBackup 5220 Appliance physical dimensions" on page 53.

See "NetBackup 5220 Appliance environmental specifications" on page 54.

See "Specifications for the NetBackup 5220 Appliance" on page 53.

NetBackup 5220 Appliance front panel

The front panel of the NetBackup 5220 houses the storage drives and the local control panel. This section provides information about these features.

See "Appliance front bezel" on page 55.

See "NetBackup 5220 Appliance drive slots" on page 55.

See "Appliance local control panel" on page 56.

Appliance front bezel

The optional front bezel is made of molded plastic. The snap-on design allows for maximum airflow through the server system. The bezel provides a lock to secure the hard drives, peripheral devices, and the control panel. A cut-out section of the bezel lets you view the LEDs and the data that displays on the control panel.

See "NetBackup 5220 Appliance drive slots" on page 55.

See "Appliance local control panel" on page 56.

See "NetBackup 5220 Appliance front panel" on page 55.

NetBackup 5220 Appliance drive slots

The NetBackup 5220 Appliance front panel houses seven storage drives, the system drives, and the local control panel. Figure 4-4 shows the front panel. Table 4-2 describes the elements that appear in the front panel.

Figure 4-4 Front panel for the NetBackup 5220 appliance

Table 4-2 Elements in the NetBackup 5220 appliance front panel

Number	Description
1	Drive tray containing two SATA disk drives (not hot swappable). The appliance must be turned off to insert or remove these drives.
2	USB ports (qty 2).
3	Control panel with system LED indicators, on/off button, and a scroll mechanism to obtain system messages.
4	Slimline drive bay (functionality not available with NetBackup 5220).
5	Drive slot #7 is used as the hot spare.
6	Disk modules containing one SAS disk drive and one disk carrier each (qty 8, labeled 0 through 7 from left to right) (hot-swappable). Each drive can consume up to 17 watts of power.

See "Appliance front bezel" on page 55.

See "Appliance local control panel" on page 56.

See "NetBackup 5220 Appliance front panel" on page 55.

Appliance local control panel

The NetBackup 5220 appliance uses a local control panel that provides traditional control panel functions and includes an LCD display. Figure 4-5 shows the local control panel that is used in the NetBackup 5220 appliance. Table 4-3 provides the information about the elements in the local control panel.

Figure 4-5 Local control panel

Table 4-3 Local control panel elements

Number	Element	Description
1	USB port	Supports USB devices.
2	LCD display	Displays system information.
3	Menu button - Scroll up	Scroll up one option at a time.
4	Menu button - Scroll down	Scroll down one option at a time.
5	Menu button - Scroll left	Move to the previous option.
6	Menu button - Enter	Select option.
7	System identification LED	■ Solid blue indicates that system identification is active. ■ No light indicates that system identification is not active.

Table 4-3 Local control panel elements *(continued)*

Number	Element	Description
8	Power LED	■ Solid green indicates that power is applied to the system. ■ Continuous green blink indicates the system is in S1 sleep state. ■ No light indicates that the power is off or the system is in ACPI S4 or S5 state.
9	Power button	■ Solid green indicates that the system is connected to the network. ■ Continuous green blink indicates that there is network activity.
10	System status LED	■ Solid green indicates normal operation. ■ Continuous green blink indicates degraded performance. ■ Solid amber indicates a critical or non-recoverable condition. ■ Continuous amber blink indicates a non-critical condition. ■ No light indicates that POST is running or the system is off.
11	NIC 2 Activity LED	■ Solid green indicates that the system is connected to the network. ■ Continuous green blink indicates network activity.
12	NIC 1 Activity LED	■ Solid green indicates that the system is connected to the network. ■ Continuous green blink indicates network activity.
13	Disk drive activity LED	■ Continuous green blink indicates disk drive activity. ■ No light indicates no disk drive activity.
14	Reset button	Restarts and initializes the system.
15	USB port	Supports USB devices.

See “Appliance front bezel” on page 55.

See “NetBackup 5220 Appliance drive slots” on page 55.

See "NetBackup 5220 Appliance front panel" on page 55.

NetBackup 5220 Appliance rear panel

Figure 4-6 shows the rear panel of a NetBackup 5220 appliance. Table 4-4 provides information about the components in the rear panel.

Figure 4-6 Rear panel for the NetBackup 5220 appliance

Table 4-4 Components in the NetBackup 5220 appliance rear panel

Number	Description
1	Low Profile PCIe Add-in Card Slots (qty 2)
2	Full-height PCIe Add-in Card Slots (qty 3)
3	Upper Power Supply Module
4	Upper Power Receptacle
5	Lower Power Receptacle
6	Lower Power Supply Module
7	I/O Expansion Module (optional)
8	Remote Management (RMM) IPMI port
9	NIC2/eth1 Ethernet port Service network port provides I/O access to the device. See Table 4-5 on page 60.
10	NIC1/eth0 Ethernet port Private network port provides for device management. See Table 4-5 on page 60.
11	USB port
12	USB port
13	DB-9 Serial B connector
14	Video connector

Table 4-4 Components in the NetBackup 5220 appliance rear panel *(continued)*

Number	Description
15	RJ-45 Serial A connector

Table 4-5 LED indications for NIC1 and NIC2 port

LED	State	Indications
Left	Off	No network connection.
	Solid amber	Network connection in place.
	Flashing amber	Transmit/receive activity.
Right	Off	10-Mbps connection (if left LED is on or flashing)
	Solid amber	100-Mbps connection.
	Solid green	1000-Mbps connection.

See "Specifications for the NetBackup 5220 Appliance" on page 53.

See "NetBackup 5220 Appliance front panel" on page 55.

About the NetBackup 5030 Appliance hardware

This section provides information about the NetBackup 5030 appliance hardware.

See "About the NetBackup 5030 Appliance bezel" on page 62.

See "About the NetBackup 5030 Appliance front panel" on page 60.

See "*About the NetBackup appliance hardware*" on page 43.

For additional information about the NetBackup 5030 refer to TECH145661.

About the NetBackup 5030 Appliance front panel

This section provides information about the NetBackup 5030 Appliance front panel.

See "About drive slot LEDs" on page 61.

See "About the NetBackup 5030 appliance control panel" on page 61.

See "*About the NetBackup appliance hardware*" on page 43.

About drive slot LEDs

Each drive slot has two LEDs. The LEDs are located on the edge of the drive facade to the left of the handle. Figure 4-7 shows the LEDs. The LEDs provide the following information:

- The top LED is solid green when power is supplied to the drive. This LED flashes green when the disk drive is active.
- The bottom LED is solid amber when a drive fault occurs. This LED is not lit when there are no disk drive faults.
- The bottom LED flashes amber during the following conditions:
  - The drive is involved in a copyback operation.
  - When an identify command is issued that allows the drive to be located.

Warning: Removing the drive from the bay when it is not in a safe state can cause equipment damage, loss of data, and data corruption. The drive is in a safe state when the bottom LED is solid amber or the drive power and activity LED is off.

Figure 4-7 Disk drive LEDs

Note: LEDs are also present for the drive slots that do not contain disk drives. These LEDs have color but are not illuminated.

About the NetBackup 5030 appliance control panel

The hardware control panel is located on the right-hand side of the front panel. It lets you monitor server activity at a glance and perform some tasks. Figure 4-8 shows the elements in the hardware control panel. Table 4-6 describes the elements in the hardware control panel.

Figure 4-8

Table 4-6

Label	Description
1	AC power button with integrated LED
2	Disk drive activity LED
3	
4	Cold reset button
5	NIC4 activity LED
6	NIC3 activity LED
7	Not used
8	NIC1 activity LED
9	NIC2 activity LED
10	

About the NetBackup 5030 Appliance bezel

Symantec provides a bezel that attaches to the front of the NetBackup 5030 Appliance. The bezels are designed to maximize the air flow through the appliance. The bezel should be installed to enhance ventilation and to protect the disk drives.

See "About the NetBackup 5030 Appliance front panel" on page 60.

See "*About the NetBackup appliance hardware*" on page 43.

About the cables

Country-specific AC power cords are shipped for each power supply that is installed in NetBackup hardware.

Symantec provides the SFP connectors for the systems that ship with FC HBA cards installed. Customers can order approved 10Gb E connectors separately. Only the connectors that Symantec supports should be used. In general, Symantec does not provide Ethernet or fibre cables.

See "*About the NetBackup appliance hardware*" on page 43.

About rack mounting

Warning: NetBackup system components can weigh more than 68 lbs (30.84 kg). Lifting and moving these components can result in bodily injury. Use appropriate tools and technique when lifting and moving NetBackup system components.

Caution: To ensure rack stability, install the heaviest NetBackup units at the bottom of the rack. Always install storage subsystems (RAID-enabled and Expansion-enabled systems) first and start at the bottom of the rack. When maintenance requires sliding a unit forward on the rails, make sure that doing so does not destabilize the rack.

You can find additional information about appliance hardware at the following:

See "*About the NetBackup appliance hardware*" on page 43.

Chapter 5

Working with log files

This chapter includes the following topics:

- About working with log files
- About using the Collect Log files wizard
- Reviewing SCSP events
- Viewing log files using the Support command
- Locating NetBackup Appliance log files using the Browse command
- Gathering device logs with the DataCollect command
- Gathering information for NetBackup-Java applications
- Enabling and disabling VxMS logging

About working with log files

As you define and troubleshoot a problem, always try to capture potentially valuable information. NetBackup Appliance has the ability to capture hardware-, software-, system-, and performance-related data. These log files capture information such as how the appliance has been running, whether there are any issues such as unconfigured volumes or arrays, temperature issues, batteries not being found, etc. These log files are stored in specific directories and can be accessed using the following methods:

Table 5-1 lists the methods you can use to access the various appliance logs.

Table 5-1 Viewing log files

From...	Using...	Logs collected..
NetBackup Appliance Web Console	You can use the **Collect Log files** wizard from the NetBackup Appliance Web Console to collect log files from an appliance. See "About using the Collect Log files wizard" on page 67. See "Troubleshooting and tuning Appliance from the Appliance Diagnostics Center" on page 35.	▪ Logs created by the NetBackup Copy Logs tool (`nbcplogs`) ▪ Appliance logs including high availability, hardware, and event logs ▪ Operating system logs ▪ All logs related to Media Server Deduplication Pool (MSDP) ▪ All logs related to the NetBackup Appliance Web Console ▪ Diagnostic information about NetBackup and the operating system ▪ Hardware and storage device logs
NetBackup Appliance Web Console	You can use the **Monitor > SCSP Audit View** screen from the NetBackup Appliance Web Console to retrieve the audit logs of an appliance. See "Reviewing SCSP events" on page 67.	NetBackup appliance's audit logs
NetBackup Appliance Shell Menu	You can use the `Main > Support > Logs > Browse` commands to open the `LOGROOT/>` prompt. You can use commands like `ls` and `cd` to work with the appliance log directories and obtain the various logs. See "Viewing log files using the Support command" on page 70.	▪ NetBackup appliance configuration log ▪ NetBackup logs, Volume Manager logs, and the NetBackup logs that are contained in the `openv` directory ▪ NetBackup appliance operating system (OS) installation log ▪ NetBackup administrative web user interface log and the NetBackup web server log ▪ NetBackup 52xx appliance device logs

Table 5-1 Viewing log files *(continued)*

From...	Using...	Logs collected..
NetBackup Appliance Shell Menu	You can use the `Main > Support > Logs > VxLogView Module` *`ModuleName`* commands to access the NetBackup Appliance VxUL (unified) logs. You can also use the `Main > Support > Share Open` commands and use the desktop to map, share, and copy the VxUL logs.	NetBackup Appliance unified logs: ■ `All` ■ `CallHome` ■ `Checkpoint` ■ `Commands` ■ `Common` ■ `Config` ■ `CrossHost` ■ `Database` ■ `Hardware` ■ `HWMonitor` ■ `Network` ■ `RAID` ■ `Seeding` ■ `SelfTest` ■ `Storage` ■ `SWUpdate` ■ `Trace`
NetBackup Appliance Shell Menu	You can use the `Main > Support > DataCollect` commands to collect storage device logs. See "Gathering device logs with the DataCollect command" on page 72.	NetBackup 5xxx storage device logs
NetBackup-Java applications	If you encounter problems with the NetBackup-Java applications, you can use the scripts in this section to gather the required information for contacting support. See "Gathering information for NetBackup-Java applications" on page 75.	Logs relating to the NetBackup-Java applications

About using the Collect Log files wizard

You can use the **Collect Log files** wizard from the NetBackup Appliance Web Console to collect log files from an Appliance. The wizard lets you collect different types of log files like NetBackup, Appliance, operating system, PureDisk, GUI, NBSU (NetBackup Support Utility), DataCollect and so on.

You can collect log files from a 52x0 Appliance.

After you have generated the log files you can email them to recipients, download them to your computer, or upload them to Symantec Support. For information about the Appliance Diagnostics Center, See "Troubleshooting and tuning Appliance from the Appliance Diagnostics Center" on page 35.

See "About working with log files" on page 64.

Reviewing SCSP events

You can use the **Monitor > SCSP Event View** menu to view the Symantec Critical System Protection (SCSP) logs.

These audit logs can help detecting security breach or abnormal activity on your appliance. An event in the audit log includes the following details:

- When - Displays the timestamp of the logged event.
- Who - Displays which user had logged on when the event took place.
- What - Displays the description of the event and the resource involved.
- How - Displays the Process Name, Process ID, Operation Permissions, Sandbox Details.
- Severity - Displays the severity of the log.
- Enforcement Action - Displays whether the event was allowed or denied.

The SCSP logs are retrieved and are represented using the following severity types:

Severity types	Description	Events example

Information	Events with a severity as Info contain information about normal system operation.	For example the following message provides the basic information relating to a generic event.
		`general CLISH message`
		`Event source:`
		`SYSLOG PID: 30315`
		`Complete message:`
		`May 21 06:58:55`
		`nb-appliance`
		`CLISH[30315]:`
		`User admin`
		`executed Return`

Notice	Events with a severity as Notice contain information about normal system operation.	An event that helps confirm the successful execution of an event is recorded as a Notice. For example the following message helps the user to understand that the event has been successfully executed.
		`successful SUDO to root`
		`Event source: SYSLOG`
		`[sudo facility]`
		`Command: /bin/su From`
		`Username: AppComm To`
		`Username: root`
		`Port: unknown`

Severity types	Description	Events example
Warning	Events with a severity as 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.	For example, the following event helps to identify and unexpected activity, like the inbound connection from a local IP address. `Inbound connection allowed from <IPaddress> to local address.`
Major	Events with a severity as Major imply a more serious effect than Warning and less effect than Critical.	For example, the following event helps to identify unauthorized access. `General luser message Event source:SYSLOG Complete message: Feb 5 21:57 luser Unauthorized user by luser Denying access to system.`
Critical	Events with a severity as Critical indicate activity or problems that might require administrator intervention to correct.	For example, the following event can help to identify critical events that can affect the appliance in an unexpected manner. `Group Membership for "group1" CHANGED from 'admin1' to 'admin2'`

For more information about retrieving SCSP audit logs, refer to the **Monitor > SCSP Events**section in the *Symantec NetBackup 52xx Appliance Administrator's Guide*.

For information about the Operating System logs, such as syslogs and other NetBackup Appliance logs, See "About working with log files" on page 64.

Viewing log files using the Support command

You can use the following section to view the log file information.

To view logs using the `Support > Logs > Browse` command:

1. Enter browse mode using the `Main_Menu` > `Support` > `Logs` followed by the `Browse` command in the NetBackup Appliance Shell Menu. The `LOGROOT/>` prompt appears.
2. To display the available log directories on your appliance, type `ls` at `LOGROOT/>` prompt.
3. To see the available log files in any of the log directories, use the `cd` command to change directories to the log directory of your choice. The prompt changes to show the directory that you are in. For example, if you changed directories to the `GUI` directory, the prompt appears as `LOGROOT/GUI/>`. From that prompt you can use the `ls` command to display the available log files in the `GUI` log directory.
4. To view the files, use the `less <FILE>` or `tail <FILE>` command. Files are marked with `<FILE>` and directories with `<DIR>`.

See "Locating NetBackup Appliance log files using the Browse command" on page 71.

To view NetBackup Appliance unified (VxUL) logs using the `Support > Logs` command:

1. You can view the NetBackup Appliance unified (VxUL) logs with the `Support > Logs > VXLogView` command. Enter the command into the shell menu and use one of the following options:
   - `Logs VXLogView JobID` *`job_id`*
     Use to display debug information for a specific job ID.
   - `Logs VXLogView Minutes` *`minutes_ago`*
     Use to display debug information for a specific timeframe.
   - `Logs VXLogView Module` *`module_name`*
     Use to display debug information for a specific module. The available module names are: `All`, `CallHome`, `Checkpoint`, `Common`, `Config`, `Database`, `Hardware`, `HWMonitor`, `Network`, `RAID`, `Seeding`, `SelfTest`, `Storage`, `SWUpdate`, `Commands`, `CrossHost`, and `Trace`.
2. If you want, you can copy the unified logs with the `Main > Support > Share Open` command. Use the desktop to map, share, and copy the logs.

Note: The NetBackup Appliance unified logs are not the same as the NetBackup unified logs, such as `nbpem` or `nbjm`. NetBackup Appliance has its own set of unified logs. To collect the NetBackup unified logs, use the Collect Logs Wizard and select **NetBackup**.

See "Troubleshooting and tuning Appliance from the Appliance Diagnostics Center" on page 35.

You can also use the `Main_Menu` > `Support` > `Logs` commands to do the following:

- Upload the log files to Symantec Technical Support.
- Set log levels.
- Export or remove CIFS and NFS shares.

Note: The NetBackup Appliance VxUL logs are no longer archived by a cron job, or a scheduled task. In addition, log recycling has been enabled, and the default number of log files has been set to 50.

Refer to the *NetBackup Appliance Command Reference Guide* for more information on the above commands.

See "About working with log files" on page 64.

Locating NetBackup Appliance log files using the Browse command

Table 5-2 provides the location of the logs and the log directories that are accessible with the `Support > Logs > Browse` command.

Table 5-2 NetBackup Appliance log file locations

NetBackup appliance logs	Log file location
NetBackup appliance configuration log	`<DIR> APPLIANCE config_nb_factory.log`
NetBackup appliance selftest report	`<DIR> APPLIANCE selftest_report`
NetBackup appliance host change log	`<DIR> APPLIANCE hostchange.log`

Table 5-2 NetBackup Appliance log file locations *(continued)*

NetBackup appliance logs	Log file location
NetBackup logs, Volume Manager logs, and the NetBackup logs that are contained in the `openv` directory	`<DIR> NBU` ■ `<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` ■ `<DIR> gui` ■ `<DIR> webserver`
NetBackup 52xx appliance device logs	`/tmp/DataCollect.zip` You can copy the `DataCollect.zip` to your local folders using the `Main > Support > Logs > Share Open` command.

See "About working with log files" on page 64.

Gathering device logs with the DataCollect command

You can use the `DataCollect` command from the `Main > Support` shell menu to gather device logs. You can share these device logs with the Symantec Support team to resolve device-related issues.

Along with the operating system, IPMI, and storage logs, the DataCollect command now collects the following logs as well:

- Patch logs
- Veritas File System logs
- Test hardware logs
- CPU information
- Disk performance logs

- Memory information
- Hardware information

To gather device logs with the DataCollect command

1. Log on to the administrative NetBackup Appliance Shell Menu.
2. Open the Support menu. To open the support menu, use the following command:

   ```
   Main > Support
   ```

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

3 Enter the `DataCollect` command to gather storage device logs.

The appliance initiates the following procedure:

```
appliance123.Support > DataCollect
Gathering release information
Gathering dmidecode logs
Gathering ipmitool sel list logs
Gathering fwtermlog logs
Gathering AdpEventLog logs
Gathering smartctl logs
Gathering disk performance logs
Gathering ipmiutil command output
Gathering cpu information
Gathering memory information
Gathering sdr logs
Gathering adpallinfo logs
Gathering encinfo logs
Gathering cfgdsply logs
Gathering ldpdinfo logs
Gathering pdlist logs
Gathering fru logs
Gathering adpbbucmd logs
Gathering os logs
Gathering adpalilog logs
Gathering dfinfo logs
Gathering vxprint logs
Gathering Test Hardware logs
Gathering patch logs


All logs have been collected in /tmp/DataCollect.zip
Log file can be collected from the appliance shared folder
 - \\appliance123\logs\APPLIANCE
Share can be opened using Main->Support->Logs->Share Open

=======================End of DataCollect=================
All logs have been collected in /tmp/DataCollect.zip
```

The appliance generates the device log in the `/tmp/DataCollect.zip` file.

4 Copy the `DataCollect.zip` to your local folders using the `Main > Support > Logs > Share Open` command.

5 You can send the `DataCollect.zip` file to the Symantec Support team to resolve your issues.

See "About working with log files" on page 64.

Gathering information for NetBackup-Java applications

If you encounter problems with the NetBackup-Java applications, use the following methods to gather data for support.

The following scripts are available for gathering information:

`jnbSA` (NetBackup-Java administration application startup script)	Logs the data in a log file in `/usr/openv/netbackup/logs/user_ops/nbjlogs`. At startup, the script tells you which file in this directory it logs to. Normally, this file does not become very large (usually less than 2 KB). Consult the file `/usr/openv/java/Debug.properties` for the options that can affect the contents of this log file.
NetBackup-Java administration application on Windows	Logs the data in a log file if NetBackup is installed on the computer where the application was started. It logs on *install_path*`\NetBackup\logs\user_ops\nbjlogs`. If NetBackup was not installed on this computer, then no log file is created. To produce a log file, modify the last "java.exe" line in the following to redirect output to a file: `install_path\java\nbjava.bat`.
`/usr/openv/java/get_trace`	Provides a Java Virtual Machine stack trace for support to analyze. This stack trace is written to the log file that is associated with the instance of execution.
`/usr/openv/netbackup/bin/goodies/support`	Creates a file containing data necessary for customer support to debug any problems you encounter. For more details, consult the usage information of the script by using `support -h`.

The following example describes how you can gather troubleshooting data for Symantec Technical Support to analyze.

An application does not respond.	Wait for several minutes before you assume that the operation is hung. Some operations can take quite a while to complete, especially operations in the Activity Monitor and Reports applications.
Still no response after several minutes.	Run `/usr/openv/java/get_trace` under the account where you started the Java application. This script causes a stack trace to write to the log file. For example, if you started `jnbSA` from the root account, start `/usr/openv/java/get_trace` as root. Or else, the command runs without error, but fails to add the stack trace to the debug log. This failure occurs because root is the only account that has permission to run the command that dumps the stack trace.
Get data about your configuration.	Run `/usr/openv/netbackup/bin/goodies/`support. Run this script after you complete the NetBackup installation and every time you change the NetBackup configuration.
Contact Symantec Technical Support	Provide the log file and the output of the `support` script for analysis.

See "About working with log files" on page 64.

Enabling and disabling VxMS logging

The following procedures explain how to enable or disable VxMS logging from the NetBackup Appliance Shell Menu.

Note: Due to the size of the VxMS logs, Symantec recommends that you only enable VxMS logging when it is necessary to troubleshoot an issue. Disable VxMS logging again when the issue is resolved.

Use the `Support > Logs > GetLevel` command to check your current VxMS log setting.

To enable VxMS logging

1. From the `Support > Logs` view of the NetBackup Appliance Shell Menu, run the following command:

   ```
   SetLevel VxMS 1
   ```

2. Verify that VxMS logging has been enabled with the `GetLevel` command. If the VxMS logs are enabled, the `GetLevel` command output displays the following:

   ```
   VxMS debug level is TRC_TOP|PARAM_IN|PARAM_OUT|DEBUG|PARAM_FULL
   ```

To disable VxMS logging

1. From the `Support > Logs` view of the NetBackup Appliance Shell Menu, run the following command:

   ```
   SetLevel VxMS 0
   ```

2. Verify that VxMS logging has been disabled with the `GetLevel` command. If the VxMS logs are disabled, the `GetLevel` command output displays the following:

   ```
   VxMS debug level is disabled
   ```

See "About working with log files" on page 64.

Chapter 6

Troubleshooting the NetBackup Appliance setup and configuration issues

This chapter includes the following topics:

- Troubleshooting the appliance setup and configuration issues
- About NetBackup appliance and Symantec Storage Shelf matched pairs
- About troubleshooting client installations
- About troubleshooting appliance installation and upgrade problems
- Troubleshooting appliance configuration problems
- Resolving a boot order change problem
- About a login error message that does not go away
- Failure to complete role configuration when NetBackup Appliance Directory is down

Troubleshooting the appliance setup and configuration issues

This chapter provides the procedures to troubleshoot issues faced during setup and configuration of your appliance. This chapter includes the following sections:

Table 6-1 Sections in troubleshooting the appliance setup and configuration issues

Section	Description	Links
About NetBackup appliance and Symantec Storage Shelf matched pairs	The section provides the instructions to work with Symantec Storage Shelf matched pairs.	See "About NetBackup appliance and Symantec Storage Shelf matched pairs" on page 79.
About troubleshooting client installations	The section provides the reson and resolution when an error occurs during client installation.	See "About troubleshooting client installations" on page 80.
About troubleshooting appliance installation and upgrade problems	This section provides the steps to troubleshoot appliance installation and upgrade problems.	See "About troubleshooting appliance installation and upgrade problems" on page 80.
Troubleshooting appliance configuration problems	This section provides the steps to check for problems after an initial configuration or after changes are made to an existing configuration.	See "Troubleshooting appliance configuration problems" on page 81.
Resolving a boot order change problem	This section provides the steps to resolve problems arising from a boot order change problem.	See "Resolving a boot order change problem" on page 82.
About a login error message that does not go away	This section provides the steps to resolve a loging error message.	See "About a login error message that does not go away" on page 87.
Failure to complete initial configuration when CMDB is down	This section provides the reason and resolution if the initial configuration fails when the CMDB is down.	See "Failure to complete role configuration when NetBackup Appliance Directory is down" on page 87.

About NetBackup appliance and Symantec Storage Shelf matched pairs

The NetBackup 5220 appliance ships with zero to four storage shelves. The NetBackup 5030 appliance ships with one storage shelf. When you order a NetBackup 5220 appliance or a NetBackup 5030 appliance with a Symantec Storage

Shelf, these units are initialized together at the factory. The initialization creates a matched pair that provides optimum performance. The pair should always be used together to help ensure successful installation and configuration.

Each storage shelf contains two numbers that show the matched set. The HOST number refers to the appliance to which a particular storage shelf is matched. The HOST and the STORAGE numbers are located in either of the following locations:

- On a white plastic panel that pulls out from the right, rear panel of the storage shelf.
- On a label that is located under the two SAS ports on the right, rear I/O module of the storage shelf.

If your NetBackup 5220 system includes more than one Symantec Storage Shelf, you do not need to match the other shelves.

Starting with appliance version 2.6.0.2, the NetBackup 5230 appliance does not require a match to a storage shelf. You can use any approved Symantec Storage Shelf with a NetBackup 5230 appliance. Therefore, any storage shelves that ship with a NetBackup 5230 appliance with version 2.6.0.2 no longer have the yellow labels that identify a matched unit.

About troubleshooting client installations

When you install client software on a Windows system, the installation process displays an, "`Install complete`" message. This message appears even if an error occurs during the installation. To ensure that the installation completed correctly, look at the script in the installation dialog and verify that a failure did not occur. If a failure occurs, you can identify the failure by searching for a failure exit code.

About troubleshooting appliance installation and upgrade problems

Use the following steps to troubleshoot appliance installation and upgrade problems.

Table 6-2 Steps for troubleshooting installation problems.

Step	Action	Description
Step 1	Determine if you can install the software on the appliance by using the release media.	Some reasons for failure are as follows: ■ Not logged on as an administrator. ■ Bad media (contact Technical Support) ■ Defective drive (replace the drive or refer to vendor's hardware documentation) ■ Improperly configured drive (refer to the system and the vendor documentation)
Step 2	Resolve network problems.	Determine if the problem is related to general network communications.

The following topics describe the specific problems that you may encounter.

Troubleshooting appliance configuration problems

Use the following steps to check for problems after an initial configuration or after changes are made to an existing configuration.

Table 6-3 Steps for troubleshooting configuration problems

Step	Action	Description
Step 1	Check the appliance configuration parameters	Begin, by verifying the parameters that you entered during the initial configuration process are correct. Refer to Chapter on Initial Configuration, in the *NetBackup Appliance Hardware Installation and Initial Configuration Guide* and review the "Performing initial configuration" topic. This topic steps you through the required IP addresses, firewall port usage, licenses, and so forth, to successfully configure your appliance.
Step 2	Retry the operation and check for status codes and messages.	If you found and corrected any configuration problems, retry the operation and check for status codes or messages in the following: ■ Check the log files. The contents of the logs can provide specific information, that is useful when the error can result from a variety of problems. If you find a error message, perform the recommended corrective actions. See "Error messages displayed during initial configuration" on page 182. ■ Check the appropriate enabled debug logs. Correct any problems you detect. If these logs are not enabled, enable them before your next try.

Table 6-3 Steps for troubleshooting configuration problems *(continued)*

Step	Action	Description
Step 3	Retry the operation and do additional troubleshooting.	If you performed corrective actions, retry the operation. If you did not perform corrective actions or the problem persists, go to one of the following procedures. ■ If the NetBackup installation directory fills up, such as with logging files, a number of problems can result. NetBackup may become unresponsive. For example, NetBackup jobs may remain queued for long periods, even though all NetBackup processes and services are running. See, "Resolving full disk problems" in the *Symantec NetBackup Troubleshooting Guide*. ■ If the backup jobs or restore jobs are running slowly, verify that the network interface cards (NIC) are set to full duplex. Half duplex often causes poor performance. See, "Troubleshooting network interface card performance" in the *Symantec NetBackup Troubleshooting Guide*.

Resolving a boot order change problem

The following situations can cause the boot order to change, which can prevent the appliance from booting up.

- A new Symantec Storage Shelf is connected to an appliance that is currently in use.
- An appliance is restarted or turned on after the Symantec Storage Shelf is disconnected.
- Power outage causes a restart of both components and the appliance is turned on before the Symantec Storage Shelf.

  If you are logged in to the appliance during any of these situations, you may experience either a blank screen with a blinking cursor or a screen that displays **GRUB**.

  The following procedure describes how to clear the current condition so that the appliance can boot successfully.

Note: The boot order can change only for a 5220 appliances. The 5030 and 5230 appliances have static boot order and will never change in any of the listed conditions.

To resolve a boot order change problem

1. Connect a monitor to the VGA port on the appliance.
2. Connect a keyboard to one of the USB ports on the appliance.
3. Make sure that the Symantec Storage Shelf is connected to the appliance and is turned on.
4. Restart the appliance by turning off the power, then turn it on again.
5. When the following **Version** screen appears, immediately press **F2** to enter setup.

6. On the setup screen, press the right arrow key until the **Boot Options** tab is highlighted, then press **Enter**.

7 On the **Boot Options** screen, press the down arrow key until **Hard Disk Order** is highlighted, then press **Enter**.

8 On the following screen, press the up or down arrow key until **Boot Option #1** is highlighted, then press Enter.

9 When the **Boot Option #1** popup appears, select **ICHx/ESB2 Embedded RAID** and press **Enter**.

10 Return to the **Boot Options** tab by pressing **ESC**.

The correct boot order should now appear with the **ICHx/ESB2 Embedded RAID** set as **Boot Option #1**.

11 Press **F10** to save this configuration and exit from the setup.

The appliance restarts automatically and should boot successfully.

About a login error message that does not go away

You may encounter a login error message that states the following, "Please try after 5 minutes". If you receive this error message, and it does not disappear after five minutes, then you can use the following procedure to diagnose the issue.

To determine why an error message does not go away after a period of time

1. Open the command-line shell on the appliance.
2. Use the following sequence of commands to navigate to the **Processes** view.

   `Main > Support > Processes`

3. Enter the following command to review the status of the current processes.

   `AdminConsole Show`

   You can see that the **Appliance Console Server** service is down.

4. Check the following log to determine if a service authentication has failed.

   `/opt/SYMCOpsCenterServer/logs/OpsCenterServer_out.log`

5. If the log shows, **Service user authentication failed**, perform the following steps:
   - Check the state of the VxAT service. If the service is down, bring it up.
     - You can check the state of the VxAT service from the root as, `/opt/VRTSat/bin/vxatd`.
     - Enter `AdminConsole Stop` and then enter `AdminConsole Start`.
   - From the root, check for the VxAT domain, `/opt/VRTSat/bin/vssat listpd --pdrtype ab`.
   - Check the host name in the domain and compare it with the host name of the system:
     - If they are not the same, then your Initial configuration might have been broken.
     - To resolve this issue, edit the `vxss.hostname` with the host name of the system and restart the OpsCenter using the following command: `/opt/SYMCOpsCenterServer/bin/opsadmin.sh stop/start`

Failure to complete role configuration when NetBackup Appliance Directory is down

The role configuration tends to fail when:

- The NetBackup Appliance Directory is down
- There is an unexpected error in connecting with the NetBackup Appliance Directory

---

Note: This error can be observed for the media server Deduplication appliance as well.

When role configuration fails and displays the following message:

```
Appliance> Master
- [Info] Checking current state of the appliance
- [Info] Initializing storage configuration...
- [Info] Acquired lock on the storage.
- [Info] Looking for existing storage configurations...
- [Info] No existing storage configurations found.
- [Info] Looking for existing storage configurations...
- [Info] Creating a new storage configuration now...
- [Info] Storage partitions are not present.
- [Info] 'Configuration' storage partition does not exist. Creating it now...
- [Info] Creating the 'Configuration' partition '0'...
- [Info] Mounting the 'Configuration' partition '0'...
- [Info] 'Catalog' storage partition does not exist. Creating it now...
- [Info] Creating the 'Catalog' partition '0'...
- [Info] Mounting the 'Catalog' partition '0'...
- [Info] Moving appliance configuration database to the Configuration partition.
- [Info] Updating hostname in the NetBackup Authentication Service configuration
                                                                                .
- [Info] Checking storage capacity of the appliance

Enter storage configuration properties.
You have the opportunity to configure AdvancedDisk and dedupe storage pools.
You can view a summary of the storage settings and edit them, if desired.

1. To configure a storage pool, you must enter the following:
   The size, the diskpool name, and the storage unit name.
2. To skip configuration, enter 0 (zero) when prompted for the size.
   This also deletes any existing data.
3. To keep the storage pool intact, choose the default size, if applicable.

 >> NetBackup Catalog volume size in GB [250..4096]: (250)
 >> AdvancedDisk storage pool size in GB/TB (e.g., 50 GB) [0 GB..4.2 TB]: 1
- [Error] You must enter a valid value. For example, 512 GB or 8 TB.
```

```
 >> AdvancedDisk storage pool size in GB/TB (e.g., 50 GB) [0 GB..4.2 TB]: 1 TB
 >> AdvancedDisk diskpool name: (dp_adv_nbuappliance)
 >> AdvancedDisk storage unit name: (stu_adv_nbuappliance)
 >> MSDP storage pool size in GB/TB (e.g., 40 TB) [0 GB..3.2 TB]: 0

- [Info] Summary of storage configuration.
  -> NetBackup Catalog volume size:       250 GB
  -> AdvancedDisk storage pool size:      1 TB
  -> AdvancedDisk storage diskpool name:  dp_adv_nbuappliance
  -> AdvancedDisk storage unit name:      stu_adv_nbuappliance
  -> Dedupe storage configuration:        None

The estimated time to configure storage is 3 minutes. The greater total storage size
you specify, the longer it takes to complete the storage configuration.
 >> Do you want to edit the storage configuration? [yes,no]: no
- [Info] Removing existing NetBackup configuration on appliance 'nbuappliance'
- [Info] Stopping NetBackup processes.
- [Info] Removing current NetBackup configuration.
- [Info] Performing Deduplication Engine cleanup.
- [Info] Configuring appliance 'nbuappliance' as NetBackup master appliance
- [Info] Creating basic NetBackup configuration on appliance 'nbuappliance'
- [Info] Reconfiguring NetBackup databases
- [Info] Configuring NetBackup logging on appliance 'nbuappliance'
- [Info] Starting NetBackup processes on appliance 'nbuappliance'
- [Info] Waiting for NetBackup processes to start
- [Info] Configuring storage partitions for appliance 'nbuappliance'
- [Error] Failed to save the AdvancedDisk disk pool name in the NetBackup Appliance
Directory. Retry this operation. If the issue persists, see the NetBackup Appliance
Troubleshooting Guide.
- [Error] Could not configure the appliance.
```

To resolve the issue restart the appliance and try again. If the issue is not resolved, perform a factory reset and try again. If the issue persists contact Symantec Technical Support.

Note: Always ensure that the NetBackup processes are up and running before you perform a Role Configuration.

See "About best practices" on page 17.

See "Troubleshooting the appliance setup and configuration issues" on page 78.

Chapter 7

Troubleshooting generic issues

This chapter includes the following topics:

- Troubleshooting generic issues
- Troubleshooting target mode port from the client
- Troubleshooting failure to connect to a media server and create storage unit
- Troubleshooting possible issues to enable or disable the SAN Client Fibre Transport
- Troubleshooting self-test errors
- About troubleshooting a corrupt storage partition
- About troubleshooting FactoryReset problems
- Discard RAID preserved cache after performing a factory reset
- Crash analysis in case of kernel coredump
- Troubleshooting IPv6 network problems
- Reinstallation of the NetBackup Appliance software on a 5220 can fail
- NetBackup deduplication disk pool or disk volume intermittently goes to a DOWN state
- Failed to perform the Appliance Factory Reset operation on a media server
- Failed to boot NetBackup 5220 appliance due to the missing embedded RAID controller information
- Resolving an fsck test failure

Troubleshooting generic issues

This chapter includes sections to help you troubleshoot Low Priority, High Priority, and Critical issues. The following types of issues are included in this chapter:

Table 7-1 Low priority issues

Section	Link
Troubleshooting target mode port from the client	See "Troubleshooting target mode port from the client" on page 92.
Troubleshooting failure to connect to a media server and create storage unit	See "Troubleshooting failure to connect to a media server and create storage unit" on page 96.
Troubleshooting possible issues to enable or disable the SAN Client Fibre Transport	See "Troubleshooting possible issues to enable or disable the SAN Client Fibre Transport " on page 97.
Troubleshooting self-test errors	See "Troubleshooting self-test errors" on page 97.

Table 7-2 High priority issues

Section	Link
About troubleshooting a corrupt storage partition	See "About troubleshooting a corrupt storage partition" on page 98.
About troubleshooting FactoryReset problems	See "About troubleshooting FactoryReset problems" on page 100.
Discard RAID preserved cache after performing a factory reset	See "Discard RAID preserved cache after performing a factory reset" on page 101.
Crash analysis in case of kernel coredump	See "Crash analysis in case of kernel coredump" on page 101.
Troubleshooting IPv6 network problems	See "Troubleshooting IPv6 network problems" on page 102.
Reinstallation of the NetBackup Appliance software on a 5220 can fail	See "Reinstallation of the NetBackup Appliance software on a 5220 can fail " on page 104.

Table 7-3 Critical issues

Section	Link
NetBackup deduplication disk pool or disk volume intermittently goes to a DOWN state	See "NetBackup deduplication disk pool or disk volume intermittently goes to a DOWN state" on page 104.
Failed to boot NetBackup 5220 appliance due to the missing embedded RAID controller information	See "Failed to boot NetBackup 5220 appliance due to the missing embedded RAID controller information" on page 106.
Resolving an fsck test failure	See "Resolving an fsck test failure" on page 107.

Troubleshooting target mode port from the client

Once the target ports are operational, you may need to continue your troubleshooting efforts from the client. You can use the NetBackup Administrator's console or use the `nbftconfig` command from the command-line interface. From the administrator's console select, **Device Management** > **Devices** > **SAN Clients**. From the command line, run the following command, where *appsanclient1* is the name of the SAN Client:

```
nbftconfig -listclients -verbose -C appsanclient1
```

```
Testsys:~ # nbftconfig -listclients -verbose -C appsanclient1
SAN Client Name       : appsanclient1
SAN Client Version    : 7.0
SAN Client State      : disabled
Master Server Name    : nbuappliance1
FT Server Connections: 1
Client Ports/Server   : 2
Usage Preference      : always
SAN Client HBA Port   : 16
        SAN Client Device State: active
        Media Server Name       : Testsys
        Media Sever State       : active
        Media Server HBA Port   : 1
        Media Server Port Mode  : FABRIC
        Media Server LUN        : 1

        SAN Client Device State: active
        Media Server Name       : Testsys
        Media Sever State       : active
```

```
Media Server HBA Port  : 1
Media Server Port Mode : FABRIC
Media Server LUN       : 0
```

If the output does not display correctly, you can use the `nbftconfig -rescanclient client` command. Wait a few minutes and attempt to list the clients again. If running this command fails, go to the client system and verify that the operating system can detect the SCSI devices. You can see a list of devices in the `/proc/scsi/scsi` directory.

```
appsanclient1:~ # cat /proc/scsi/scsi
Attached devices:
Host: scsi0 Channel: 00 Id: 08 Lun: 00
  Vendor: DP       Model: BACKPLANE        Rev: 1.00
  Type:   Enclosure                        ANSI SCSI revision: 05
Host: scsi0 Channel: 02 Id: 00 Lun: 00
  Vendor: DELL     Model: PERC 5/I         Rev: 1.00
  Type:   Direct-Access                    ANSI SCSI revision: 05
Host: scsi0 Channel: 02 Id: 01 Lun: 00
  Vendor: DELL     Model: PERC 5/I         Rev: 1.00
  Type:   Direct-Access                    ANSI SCSI revision: 05
Host: scsi2 Channel: 00 Id: 00 Lun: 00
  Vendor: Dell     Model: Virtual  CDROM   Rev: 123
  Type:   CD-ROM                           ANSI SCSI revision: 02
Host: scsi3 Channel: 00 Id: 00 Lun: 00
  Vendor: Dell     Model: Virtual  Floppy  Rev: 123
  Type:   Direct-Access                    ANSI SCSI revision: 02
```

Note: If the `nbftconfig -rescanclient client` command works, Symantec recommends that you still go to the client system and verify that the operating system can detect the SCSI devices. It's possible that the output that is received after the `nbftconfig -rescanclient client` command is run can contain stale information.

From the example, the expected SCSI devices are missing. You should have seen two devices from the vendor, **ARCHIVE**, and the model **Python**. In this situation, you should look at the `/sys/class/fc_remote_ports` directory. This directory shows you the remote FC ports that the operating system can see.

```
appsanclient1:~ # ls -la /sys/class/fc_remote_ports/
total 0
drwxr-xr-x  2 root root 0 Apr 25 11:06 .
drwxr-xr-x 24 root root 0 Apr 24 17:55 ..
```

Again, the expected entries are missing. At this time, Symantec recommends that you reload the FC HBA driver, `qla2xxx` with `rmmod qla2xxx` and then `modprobe qla2xxx`. Reloading the driver may correct your issue. In this example, reloading the driver corrected the issue because the driver had not been previously loaded. From the following output you can see the entries, and you can see that the remote **port_name** matches the appliance **Port WWN**):

```
appsanclient1:~ # modprobe qla2xxx
appsanclient1:~ # ls -la /sys/class/fc_remote_ports/
total 0
drwxr-xr-x  3 root root 0 Apr 27 14:48 .
drwxr-xr-x 24 root root 0 Apr 24 17:55 ..
drwxr-xr-x  2 root root 0 Apr 27 14:48 rport-4:0-0
appsanclient1:~ # cat /sys/class/fc_remote_ports/rport-4\:0-0/port_name
0x21000024ff232782
appsanclient1:~ # cat /proc/scsi/scsi
Attached devices:
Host: scsi0 Channel: 00 Id: 08 Lun: 00
  Vendor: DP       Model: BACKPLANE        Rev: 1.00
  Type:   Enclosure                        ANSI SCSI revision: 05
Host: scsi0 Channel: 02 Id: 00 Lun: 00
  Vendor: DELL     Model: PERC 5/I         Rev: 1.00
  Type:   Direct-Access                    ANSI SCSI revision: 05
Host: scsi0 Channel: 02 Id: 01 Lun: 00
  Vendor: DELL     Model: PERC 5/I         Rev: 1.00
  Type:   Direct-Access                    ANSI SCSI revision: 05
Host: scsi2 Channel: 00 Id: 00 Lun: 00
  Vendor: Dell     Model: Virtual  CDROM   Rev: 123
  Type:   CD-ROM                           ANSI SCSI revision: 02
Host: scsi3 Channel: 00 Id: 00 Lun: 00
  Vendor: Dell     Model: Virtual  Floppy  Rev: 123
  Type:   Direct-Access                    ANSI SCSI revision: 02
Host: scsi4 Channel: 00 Id: 00 Lun: 00
  Vendor: ARCHIVE  Model: Python           Rev: V000
  Type:   Sequential-Access                ANSI SCSI revision: 02
Host: scsi4 Channel: 00 Id: 00 Lun: 01
  Vendor: ARCHIVE  Model: Python           Rev: V000
  Type:   Sequential-Access                ANSI SCSI revision: 02
```

If you still do not see anything in the `/sys/class/fc_remote_ports` directory or you do not see any SCSI devices, then the root cause is most likely a zoning issue. You may need to contact Technical Support for assistance if you come to this determination.

It's possible for you to see expected entries in the `/proc/scsi/scsi` directory and yet have the information be stale. To ensure that the information is not stale, use the `sg_inq` command to query the current status.

```
appsanclient1:~ # sg_inq -I /dev/sg3
VPD INQUIRY: Device Identification page
  Designation descriptor number 1, descriptor length: 55
    id_type: T10 vendor identification,  code_set: ASCII
    associated with the addressed logical unit
      vendor id: SYMANTEC
      vendor specific: FATPIPE 1.0     Testsys.enx1.symantec.com
appsanclient1:~ # sg_inq -I /dev/sg4
VPD INQUIRY: Device Identification page
  Designation descriptor number 1, descriptor length: 55
    id_type: T10 vendor identification,  code_set: ASCII
    associated with the addressed logical unit
      vendor id: SYMANTEC
      vendor specific: FATPIPE 1.1     Testsys.enx1.symantec.com
```

If these commands fail then it is likely that there is stale information in the operating system . You can run the `rescan-scsi-bus util` (`/bin/rescan-scsi-bus.sh`) to force a refresh. Run it first with the `-r` option to remove the stale entries. If that does not work, try the following:

- If you do not see the entries you expect after you run the `rescan-scsi-bus util -r` command, try it with the `-I` option. That forces the FC link to be renegotiated.
- Restart the FT media server on the appliance (enable and then disable it). Then rescan with the `rescan-scsi-bus util` command.

  If that command fails, the most likely root cause is a zoning issue. You should contact Support to help identify the zoning on the appliance.
- Finally, if you have had to rescan the SCSI devices or there are new SCSI devices, restart the FT client daemon. Once it has been restarted, you can look at the VxUL log for originator 200 to check that it sees the SCSI devices correctly:

  ```
  appsanclient1:~ # /usr/openv/netbackup/bin/vxlogview -p nb -o 200
  04/27/11 13:58:25.736 [FATClientMgrService::init] Client
  successfully started (FATClientMgrService.cpp:277)
  04/27/11 13:58:25.822 [DiscoveryTaskThread]  DiscoveryTask Thread
  1094740288 Startup
  04/27/11 13:58:25.822 [AddDevice] /dev/sg3
   Inquiry "SYMANTECFATPIPE 1.0     nbapp36.engba.symantec.com"
   TargetHBA:LUN:InitiatorHBA = 1:0:0x40 State = 1 RefCount = 0
  ```

```
04/27/11 13:58:25.822 [AddDevice] /dev/sg4
 Inquiry "SYMANTECFATPIPE 1.1     nbapp36.engba.symantec.com"
 TargetHBA:LUN:InitiatorHBA = 1:1:0x40 State = 1 RefCount = 0
```

About Fibre Transport media server verification

After you install and configure a Fibre Transport (FT) media server, you can use the `Settings` > `FibreTransport SANClient Show` command to show the status of the SAN Client feature. When you run the `FibreTransport SANClient Show` command and the Fibre Transport (FT) media server is configured properly, you see an output similar to the following:

```
Testsys.Settings> FibreTransport SANClient Show
Fibre Transport server installed and running.
```

You can also use the `Manage > FC Show` command to verify and confirm the status of the SAN Client feature. From the output that you receive after you have run the `Manage > FC Show` command, you can verify the following:

- The `qla2xxx` and `windrvr6` drivers are loaded.
- The target ports are in `Target` mode and not `initiator` mode.
- Under the **Status** column, the target mode ports should have a status of **Fabric** if the port is physically connected to something such as a switch
  Nothing ever appears under the **Remote Ports** column for target mode ports.
  To find more information about the target mode ports, you must look at the VxUL logs for the originator 199 (`nbftsvr`).

Troubleshooting failure to connect to a media server and create storage unit

Ensure that both the short name and long name of the media server are pingable from master server. If you cannot access the media server, using the short name, do the following:

- Use the fully-qualified name as the DNS suffix
- Clear the host cache on the master server.

After you have performed these two steps you can access the media server from the master server and then create the storage unit from the media server.

See “Troubleshooting generic issues” on page 91.

Troubleshooting possible issues to enable or disable the SAN Client Fibre Transport

If you enable or disable the SAN Client Fibre Transport on a 5220 appliance, you may need to do the following to ensure that your tape devices are recognized and the SAN Client daemons are running:

- If you enable or disable the SAN Client Fibre Transport on a 5220 appliance, you must rescan for tape devices unless you have persistent device paths configured. That is necessary because the enable and disable operations cause the Fibre Channel HBA driver to be reloaded. The reloading causes the tape device paths on the appliance to be renumbered unless you have persistent paths configured. Thus, to use the tape devices, you must perform a rescan so that the appliance can discover tape device paths again.
- If you disable SAN Client Fibre Transport on a 5220 appliance and then enable it again at some later time, you must restart any SAN Client daemons that are running on the client systems. For example, you must enable the SAN Client on the 5220 appliances before the SAN Client daemon is started on the client because it only discovers targets on startup.

See "Troubleshooting generic issues" on page 91.

Troubleshooting self-test errors

This section talks about the possible errors that you may come across when a self test fails and the recommended action to resolve these errors.

Self-test may fail when it tests if NetBackup is configured and running

The self-test may fail with the following error message when it tests if NetBackup is configured and running:

```
....cannot connect on socket - CORBA transient error(3000001)
```

To resolve the self-test failure when NetBackup configuration and operation are tested:

1. Stop all of the NetBackup services.
2. Stop the Symantec Private Branch Exchange (PBX).
3. Start the Symantec Private Branch Exchange (PBX).
4. Start the NetBackup daemons.

Self-test may fail when backup and restore operations are tested

The self-test may fail when backup and restore operations are tested. The following error may appear:

```
Error:
[10-21-2011 00:33:17] [10882]
Debug (/opt/NBUAppliance/scripts/self_test.pm 812):
"Trying restore attempt number <1>"
[10-21-2011 00:34:50] [10882] cmd:
" /usr/openv/netbackup/bin/bprestore
-00:03:00 /tmp/test_backup.txt"( 10 )
stderr: EXIT STATUS 10: allocation failed
```

The system memory allocation fails because of an insufficient amount of available system memory. A possible cause is that the system is overloaded with too many processes and not enough physical or virtual memory.

Symantec recommends that you stop any unnecessary processes that consume memory and add more swap space or physical memory.

For more information about this issue, see the following tech note on the Symantec Support website:http://www.symantec.com/docs/TECH87179

See “Troubleshooting generic issues” on page 91.

About troubleshooting a corrupt storage partition

There can be a rare instance where a storage partition might be corrupt. The issue can appear as configuration failures, backup failures, and status and monitoring failures. The error messages, in most cases, do not directly point to a corrupt storage partition. The software stack masks the actual error and presents a different error.

Note: In most cases, the storage partitions are generally VxFS file systems.

One symptom that you may encounter that can help you recognize a problem is if a backup fails with the following error message.

```
1: (213) no storage units available for use.
```

You can then use either of the following methods to check the partition size. If the partition size status is shown as **Degraded** it indicates that one or more partitions are not mounted. Also, if appliance is already configured, and the partition status is shown as **Not Accessible**.

Symantec recommends that you contact Symantec Technical Support for your appliance as this type of issue is a Storage Foundation escalation. Symantec recommends that you do not attempt to remove or reformat the volumes because that can render the file system unrecoverable.

Symantec needs different information from what the Appliance DataCollect tool can gather. The Storage Foundation team have utilities to gather extensive troubleshooting information from the appliance to do a "Root Cause Analysis". Refer to the following tech notes for more information about these utilities:

- Symantec Root Cause Analysis description page, (TECH61403)

- Symantec VRTSexplorer tool reference page, (TECH17676)
- How to Download and run Metasave, (HOWTO36957)

About troubleshooting FactoryReset problems

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.

The FactoryReset function is used to return an appliance to its default state. The following issues may occur when you use this function:

- You may encounter one of the following issues when you perform a `FactoryReset` function on an appliance that has network issues:
  - The network may timeout.
    This situation is likely to occur if the appliance is a media server appliance and it cannot communicate with the master server.
  - Any configured storage units on the master server may not get cleaned properly.

  If you encounter any of these situations, you must ensure that you clean up the storage units properly, before you reconfigure the appliance.
- If you choose the Storage Reset option during a factory reset, the data or storage may not be deleted. This situation happens if one of 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 will need to clear the preserved cache of the RAID controller.
  See "Discard RAID preserved cache after performing a factory reset" on page 101.

Note: For NetBackup 5200 appliances that are upgraded to version 2.5.1, you cannot factory reset or reimage directly back to version 2.5.1. You must reset or reimage the appliance to version 2.5 and then reinstall the version 2.5.1 release update.

See "About contacting Symantec Technical Support" on page 12.

Discard RAID preserved cache after performing a factory reset

If you remove any attached disk storage before performing a factory reset, you will need to discard the preserved cache of storage disks in the RAID BIOS console.

Discarding the preserved cache

1. Once the appliance has restarted, press any key when prompted. The RAID configuration utility opens.
2. Select the RAID controller, then click **Start**.
3. A message appears starting that the controller lost access to one or more drives. Click **Discard Cache** to discard the preserved cache of the virtual drives.
4. When prompted, click **Yes** to discard the preserved cache.
5. Restart the appliance to continue the factory reset process.

See "Troubleshooting generic issues" on page 91.

Crash analysis in case of kernel coredump

In case a kernel coredump has occurred, use the following procedure to perform a crash analysis:

To perform a crash analysis in case of kernel coredump

1. As the `debuginfo.rpm` is not installed in the v2.6 installation, you need to manually install the `debuginfo.rpm` file.
2. You can find the `debuginfo.rpm` in the following location on the appliance:

   ```
   /inst/client/.packages/from_dvd/netbackup_addon/suse/x86_64
   ```

   The complete name of the rpm file is
   `kernel-default-devel-debuginfo-2.6.32.59-0.7.1.fsl.x86_64.rpm`
3. Use the following command to install the rpm file.

   ```
   # rpm -ivh
   kernel-default-devel-debuginfo-2.6.32.59-0.7.1.fsl.x86_64.rpm
   ```

   The following output is displayed:

   ```
   Preparing...    ########################### [100%]
   1:kernel-default-devel-de############################### [100%]
   ```

The `vmlinux gzip` is then available in `/boot`
`/boot/vmlinux-2.6.32.59-0.7-default-fsl.gz` for use.

See "Troubleshooting generic issues" on page 91.

Troubleshooting IPv6 network problems

You can use the following procedure to troubleshoot problems with IPv6 networks. If you need further assistance at any point, contact Symantec Technical Support.

Possible issues include:

- The IPv6 network is not configured properly.
- IP routing cannot locate one or more hosts.
- The default gateway is not reachable.
- The network host is not reachable.
- A NetBackup feature still points to an IPv4 address.

To troubleshoot an IPv6 network error

1. Verify that the IPv6 interface has a global address.

   Run the following command in the NetBackup Appliance Shell Menu:

   `Main_Menu > Network > Show Configuration`

   In the output, under one of the `eth` headings (`eth0`, `eth1`, etc.), look for an entry similar to the following:

   ```
   inet6 addr: 2001:db8::2/64 Scope: Global
   ```

   The scope of at least one address must be global. If a global scope address does not appear in the command output, reconfigure the IPv6 address.

2. Verify the network routing path with the `Main_Menu > Network > Gateway Show IPv6` command. Check the routing table for any errors. If any of the network path information is incorrect, enter the correct information. You can use the `Network` view commands in the shell menu or the **Settings > Network** page of the NetBackup Appliance Web Console.

   See the *NetBackup Appliance Command Reference Guide* and the *NetBackup Appliance Administrator's Guide* for more information.

3. Check communication with the default gateway. The gateway IP address is shown in the routing table that displayed in the previous step.

   Use the `Main_Menu > Network > Ping Host` command to test communication with the gateway. In this case, *`Host`* is the IPv6 address of the gateway.

   If the gateway is not reachable, contact your network administrator to check the gateway status.

4. Check communication with the host with the `Main_Menu > Network > Ping Host` command, where *`Host`* is the host name or the host IPv6 address.

   If the host is not reachable, run the `Network > TraceRoute Host` command to check for problems along the network path.

5. If you experience an IPv6 issue with a feature that previously worked over an IPv4 network, ensure that NetBackup now associates an IPv6 address with the host name or host names.

   Add a host name to the IPv6 network with the following command:

   `Main_Menu > Network > Hosts Add IP_Address FQHN Short_Name`

   where *`IP_Address`* is the IPv6 address, *`FQHN`* is the fully qualified host name, and *`Short_Name`* is the short host name.

See "About IPv4-IPv6-based network support" on page 29.

Reinstallation of the NetBackup Appliance software on a 5220 can fail

A reinstallation of the NetBackup Appliance software on a 5220 appliance may fail. The issue occurs because the database is backed up before the operating system is reinstalled.

If you encounter this issue, contact your Symantec Support representative and have them reference DOC6035 to help resolve this issue.

See "Troubleshooting generic issues" on page 91.

NetBackup deduplication disk pool or disk volume intermittently goes to a DOWN state

The deduplication disk pool or disk volume for yourNetBackup Appliance, configured as a media server, intermittently goes to a `DOWN` state. As a result the backups or duplication jobs can fail with status **213** no storage units is available and **2074** respectively. This can occur in case of a NetBackup 52xx appliance using a deduplication disk pool is writing to a media server Deduplication storage server.

The NetBackup Disk Polling Service (DPS) is responsible for telling NetBackup whether a disk pool or disk volume is functioning fine. The DPS extracts this information from the MSDP storage server using `bpstsinfo`. The DPS The default timeout limit for DPS is set to 1 minute, so if the DPS is not able to receive a reply with the current status from the MSDP within a minute, it automatically treats it as an error and considers the disk pool or the disk volumes as down. A deplay in the reply to the DPS can be due to the depletion of system resources. You can use the following procedure to resolve this error:

To resolve the DOWN state of the NetBackup deduplication disk pool or disk volume:

1. Increase the DPS proxy timeouts to 3600 seconds (max) in the `DPS_PROXYNOEXPIRE` file from the following location:

   `/usr/openv/netbackup/db/config/DPS_PROXYNOEXPIRE`

2. Create the `DPS_PROXYDEFAULTSENDTMO` file with the value of 1800 inside:

   `/usr/openv/netbackup/db/config/DPS_PROXYDEFAULTSENDTMO`

3. Create the `DPS_PROXYDEFAULTRECVTMO` file with the value of 1800 inside:

   `/usr/openv/netbackup/db/config/DPS_PROXYDEFAULTRECVTMO`

4 Log on to the NetBackup Appliance media server using theNetBackup Appliance Shell Menu.

5 You can use the following command to restart `nbrmms` process.

```
Main > Support > Processes NetBackup Start
```

Note: If the issue reoccurs, uncomment or configure the `CR_STATS_TIMER`line in `pd.conf` on the affected media server for 300-seconds change`CR_STATS_TIMER = 300`

See "Troubleshooting generic issues" on page 91.

Failed to perform the Appliance Factory Reset operation on a media server

When a media server contains SLP (Storage Lifecycle Parameter) based backup images, it is vital that you perform a cleanup of these images and policies, before running a **Appliance Restore > Factory Reset** operation. This is because when you try to perform a factory reset on a media server that has SLP-based backup images stored on its storage devices, the following error may appear:

```
- [Warning] Found some storage units in Storage Lifecycle Policies:
- [Warning] SLP: slp, storage units: stu_adv_applabc stu_disk_applabc
- [Warning] The factory reset will not be able to remove the
above storage units
as part of the reset. Please manually remove the storage units from the
above Storage Lifecycle Policies using the NetBackup Administration Console
before running a factory reset.
 >> Factory reset validation found some minor issues.
Continue with factory reset shell menu? [yes/no]
```

To resolve this error, select **No**, and manually cleanup the SLP-based storage images using the NetBackup Administration Console. After you have removed all the SLP backup images, perform the factory reset operation.

For more information on manually cleaning up the SLP-based storage, refer to the *SLP Parameters properties* section in the *Symantec NetBackup™ Administrator's Guide* and tech note TECH150431.

If you select **Yes**, and continue with the factory reset, the reconfiguration of the same media server may fail.

See "Troubleshooting generic issues" on page 91.

Failed to boot NetBackup 5220 appliance due to the missing embedded RAID controller information

This section troubleshoot the issue when a NetBackup 5220 Appliance does not boot with the following message:

```
Waiting for /dev/disk/by-id/scsi-46000805E0000000-part2
```

The issue is caused when the embedded RAID controller information is not detected and presented to the BIOS.

To troubleshoot the error `Waiting for /dev/disk/by-id/scsi-46000805E0000000-part2`:

1. Connect a monitor and keyboard to your 5220 appliance.
2. Turn on the appliance.
3. Press **F2** to enter the BIOS Main menu.
4. Use the arrow keys to move right and select the **Boot Order** tab.
5. Select the **Hard Disk Order** and press **Enter**.

   A pop-up window is displayed, in the three Boot Option numbers verify if you see the option **ICHx/ESB2 Embedded RAID**. If you do not see this option proceed to the next step.
6. Press **ESC** to exit and return to the main BIOS menu options.
7. Select the **Advanced** tab at the top.
8. Arrow down to **Mass Storage Controller Configuration** which will take you to the **Mass Storage Controller Configuration** options.
9. From the **Mass Storage Controller Configuration** options, arrow down to **Intel (R) SAS RAID Module** and press **Enter**.
10. A pop-up window is displayed, set the selection to **Enabled**.
11. From the **Mass Storage Controller Configuration** options, arrow down to **SATA Mode** and press **Enter**.
12. A pop-up window is displayed, set the selection to **SW RAID** to enable it.
13. Now that SW RAID is enabled, Press **F10** .
14. Restart the appliance go back into BIOS and see if you can see the **ICHx device**.

See “Troubleshooting generic issues” on page 91.

Resolving an fsck test failure

If the appliance runs a file system check (`fsck`) and the test fails, it asks the user to fix the file system with more advanced `fsck` options. Before you can fix the issue, you may be asked for a root password. In NetBackup Appliance 2.6.0.2 and later, however, the root account is locked. Therefore, do the following to resolve the issue:

To resolve an `fsck` test failure:

1. Restart the appliance.
2. When the following GRUB boot screen appears, press **e** to edit the boot commands:

3 Select the second line and press **e** again.

4 Add the word **single** to the end of the command that appears on the next screen. Press **Enter** and then **b** to boot the system in single-user mode.

5 Once the prompt is available, run `fsck` on the affected file system with the `fsck -pv FileSystem` command, where `FileSystem` is the file system that encountered the error.

For example, `fsck -pv /dev/system/log`

6 If the operation fails, the following error message appears:

```
UNEXPECTED INCONSISTENCY; RUN fsck MANUALLY
```

If you encounter this message, run the `fsck -yv FileSystem` command to run `fsck` manually.

For example, `fsck -yv /dev/system/log`

You may see several messages similar to the following

7 When the file system has been repaired, restart the appliance with the `shutdown -r now` command.

See "Troubleshooting generic issues" on page 91.

Chapter 8

Troubleshooting Hardware Issues

This chapter includes the following topics:

- Starting an appliance that does not turn on
- Troubleshooting an amber drive status LED on the appliance
- Troubleshooting a system drive that the management software does not identify
- Troubleshooting appliance power supply problems
- Troubleshooting system-induced shutdown
- Troubleshooting system status LED issues

Starting an appliance that does not turn on

This section provides suggestions you can use to ensure that the appliance is on. Possible causes include the following:

- The AC power plug is not inserted properly.
- AC power is not supplied from the power source.
- Appliance is not turned on.

To ensure that the power is on, do the following

1. Check the AC power LED and the system status LED on the control panel.
   - If the AC power LED is off and the system status LED is green, push the AC power button to turn on the power.

- If the system status indicator is off, the system is not on. Proceed to the next step.

2. Connect the AC power cables for the unit to another external power source.
3. Check the power plug and cables as follows:
   - Remove and reinsert the power plug from the power supply sockets in the rear panel.
   - Check the status of the power-on and alarm indicator on the control panel for the following:
     - If the power indicator flashes green, power to the unit is active. The fault is removed.
     - If the power indicator is amber, one of the two power supplies may be faulty.
     - If the power supply is blinking green, the power supply is in standby mode. Press the power button and LED on the control panel on the front panel to turn on the unit.
     - If the power is still off, check the LEDs on the power supplies on the rear panel of the unit.
       - If a power supply LED is green, power is supplied. The LED on the control panel may be faulty. Contact Symantec Technical Support.
       - If a power supply LED is off or amber, power is not supplied to that power supply.
4. If the power is off to a power supply, check the LEDs on the power supplies on the rear panel of the unit. Do the following:
   - Verify that AC power source works. Attach a different unit to the power source and verify that power is on.
   - Access the hardware monitor in the NetBackup Appliance Web Console or the appliance shell menu to obtain information about errors. Refer to your Symantec NetBackup Appliance administrator guide for more information about using the hardware monitor and the NetBackup Appliance Shell Menu. For information about CLI commands, refer to the *NetBackup 52xx Series Command Reference Guide*.
   - Contact Symantec Technical Support.

You can find additional troubleshooting topics at the following:

See "*Troubleshooting Hardware Issues*" on page 111.

Troubleshooting an amber drive status LED on the appliance

Each NetBackup 5230 appliance drive has two LEDs along the left edge near the drive release latch. The top LED indicates the drive status. The bottom LED indicates drive activity. Table 8-1 describes the LED states.

Each NetBackup 5220 appliance drive has two LEDs along the top edge of the drive above the release latch. The LED on the right indicates the drive status. The LED on the left indicates drive activity. Table 8-1 describes the LED states.

Table 8-1 System disk status LEDs indications

LED	Behavior	Indication
Status	Off	No access and no fault.
	Solid amber	Disk drive fault has occurred.
	Blinking amber	RAID rebuild in progress (1-Hz), Identify (2-Hz).
Activity	Solid green	Power is on with no drive activity.
	Blinking green	Power is on and the drive is active.
	Off	Drive has no power.

To verify that a drive is faulty

Caution: The drive status LED must be solid amber before you remove a drive from the appliance. Data loss and corruption can occur when a drive is disconnected inappropriately.

1. Make sure that the drive status LED is amber.
2. Pull open the green handle on the drive cover to disengage the drive from the slot.

   Note: You can gently pull the drive forward about an inch (2.4 cm) to ensure that the drive is disengaged.

3. Remove the disk drive completely.

4 Install a new drive from Symantec.

Caution: You must use a drive that is properly set up for the NetBackup RAID.

5 After the new drive spins up, wait for approximately three minutes.

6 Check the disk drive LEDs and do the following:

- If the activity LED is green, the fault is resolved.
- If the status LED is still amber, contact Symantec Technical Support.

You can find additional troubleshooting topics at the following:

See "*Troubleshooting Hardware Issues*" on page 111.

Troubleshooting a system drive that the management software does not identify

You can use this procedure to troubleshoot a system disk drive that is not identified in any of the following management tools:

- NetBackup Appliance Web Console
- NetBackup Appliance Shell Menu
- Symantec Remote Management tool

Some possible reasons that the system drive does not appear include the following:

- Improperly installed disk drive. The connector on the drive is not properly mated with the connector inside the chassis.
- Drive or drive slot connector that is damaged or obstructed.
- The drive is faulty.

To determine that a disk drive is properly inserted

1 Locate the system drive that does not register in the monitoring interface.

2 Inspect the drive cover and the bay. Look for signs of damage, loose particles, twisted parts or other abnormalities.

3 Check the activity LED (the bottom LED) on the left side of the drive cover.

4 Verify that the drive is properly inserted in the bay. Reinsert the drive if necessary.

5 If the activity LED is still amber, replace with a new drive from Symantec.

6 Make sure that the new drive fits correctly.

7 Wait approximately three minutes for the drive to spin up.

8 Check to see if the drive is scannable by the NetBackup Appliance Web Console, NetBackup Appliance Shell Menu, or the Symantec Remote Management tool.

- If both disk drives can be seen, the fault is removed.
- If the fault persists, contact Symantec Technical Support.

You can find additional troubleshooting topics at the following:

See "*Troubleshooting Hardware Issues*" on page 111.

Troubleshooting appliance power supply problems

NetBackup appliances have two, modular power supplies for high availability operation. During normal operation, the power supplies are configured for active standby operation. In this configuration, one power supply is used to provide power for the entire system and the other is held in reserve. Should the active power supply fail, the system automatically shifts the load to the power supply that is held in reserve.

Caution: To ensure power to the system in not interrupted, periodically check the reserve power supply. Make sure that the unit is turned on and operating properly.

Power supply modules are easily accessed from the rear of the unit. They are installed side-by-side on the left-hand side of the unit. Each contains an AC socket, switch, LED, and fan. The LED on the power supply provides information about the power supply status.

Note: The power supplies are designed to enter protection mode when an electrical event that is potentially catastrophic occurs. Such events include short-circuits, voltage overloads, and power surges. In protection mode, the power supply shuts down or locks up to protect itself and the component in the system.

You can remotely gain information about the current status of an appliance power supply using one of the following Symantec user interfaces:

- In the NetBackup Appliance Web Console use **Monitor > Hardware** page to view the power supply information.
- In the NetBackup Appliance Shell Menu use `Main_Menu > Monitor > Hardware`.

- You can also gather information about the power supply by viewing the LEDs on the front and the rear panels of the unit. If the power button and LED on the front control panel is amber, one or both power supplies may be faulty. Check the LEDs on the power supplies on the back of the unit to determine which power supply is faulty. You can use the following procedure to verify that the power supply is faulty.

To determine if one, or both, power supplies are faulty

1. On the rear panel, locate the power supply that has the amber LED.
2. Make sure that the other power supply functions properly.
3. Unplug the power cord from the power supply that has the amber LED.
4. Wait for 2 minutes or for 3 minutes, then plug in the power cord.
5. If the LED is still amber, replace the power supply.

Caution: The unit functions normally with one power supply. However, data and operation is at risk if the second power supply fails. The faulty power supply should be replaced as soon as possible.

Warning: To ensure that the unit does not overheat, do not operate the unit with the power supply bay empty for more than a few minutes. Leave the failed power supply in the bay until the replacement power supply is available.

If both power supplies have amber LEDs, shut down the unit and obtain replacements.

You can find additional troubleshooting topics at the following:

See "*Troubleshooting Hardware Issues*" on page 111.

Troubleshooting system-induced shutdown

The power supplies are designed to enter protection mode when an electrical event that is potentially catastrophic occurs. Such events include short-circuits, voltage overloads, and power surges. In protection mode, the power supply shuts down or locks up to protect itself and the component in the system.

When the unit is running, it may be turned off incorrectly or inadvertently. The control panel in front of the unit may show a fault. The LEDs on the power supplies in the rear of the unit may show a fault.

Possible causes include the following:

- AC power input to the power supplies is incorrect.
- The power supply is faulty or in protection mode.
- The CPU is in over-temperature protection mode.

To determine if the AC input to the power supplies is correct

1. Check to see if the power button/LED on the control panel and the LED near each AC power socket are off.
2. If an LED is off, remove and reinsert the AC power cable to the power supply at the power source. Do the following:
   - If the power button LED flashes green, the abnormal lock-up is due to a loose plug connection. Operations should continue normally.
   - If the LEDs are still off, it is possible that AC power to the equipment room is faulty. In this case, contact the customer for resolution.
   - If the equipment room power is normal, replace the power supply.
3. If the power button is amber, check other components such as fans and CPUs for further analysis.

To determine if a power supply is faulty or in protection mode

1. For each power supply, check the power button LED and the power supply LED.
2. If both the LEDs are amber, replace the power supply.
3. If only one LED is amber, check other components such as fans and CPUs for further analyses.

To determine if the CPUs are in over-temperature mode

1. Access the NetBackup web Appliance console and click **Monitor > Hardware**.
2. Check the alarm list.

   Review the list for temperature- and fan- related alerts such as the following:

Alert information	Description
Overtemperature	Temperature is not critical yet but approaches the upper limit of the range.
Absence	A component such as a fan is absent.

3. If an alarm about the CPU overtemperature appears, several problems may be the cause including the following:
   - Improper installation or damage of the air duct inside the chassis.
   - Fan and or air intake or output problems.
   - Excessive equipment room temperature (room temperature should be between 10° C and 35° C (50° F - 95° F).
4. Inspect the fans in the power supplies on the rear left-hand side of the unit. Verify that there are no obstructions or damage.
5. Inspect the air intake and output vents in the front panel and rear panel of the unit. Verify that there are no obstructions or damage.
6. If the room temperature is too high, reduce the temperature at a rate of no more than 10° C per hour until an acceptable temperature is reached.
7. Access the NetBackup Appliance Web Console and verify that the CPU temperature has decreased.
8. If CPU temperature does not return to normal, escalate as necessary. The unit may require replacement.

See "*Troubleshooting Hardware Issues*" on page 111.

Troubleshooting system status LED issues

Color/action	Description
Solid green	Normal operation.
Flashes green	Degraded performance.
Solid amber	Critical or non-recoverable condition.
Flashes amber	Non-critical condition.
Not lit	POST (Power On Self Test) is running, or the unit is off.

If the system status LED is anything other than solid green, you must investigate. Environmental or component issues such as the following can trigger a status change:

- An excessively hot or an excessively cold equipment room.
- AC current too high.
- AC current too low.

- Current surge from the AC power source affects operation.
- Open or damaged chassis cover can cause overheating.
- Components drifting out of specifications.

To determine why the system status LED shows issues

1. Access the NetBackup Appliance Web Console and click **Monitor > Hardware**.
2. Review the alerts page. If CPU-related alerts are shown, do the following:
   - Turn off the unit immediately.
   - Contact Symantec Technical Support and arrange for a replacement unit.
   - Keep system intact until the new unit arrives.
3. If power supply module alerts are shown, check the power supply section. See "Troubleshooting appliance power supply problems" on page 115.
4. If memory (DIMM) related alerts are shown, contact Symantec Technical Support.
5. If Over temperature or current alerts are shown, go to the equipment room where the unit is installed. Do the following:
   - Check the room for temperature abnormalities.
   - Make sure that other sources of heat do not heat the unit. Check equipment that is installed on, under, or next to the unit.
   - Check the unit for loose or unplugged power cables.
   - Make sure that the air vents are not blocked (minimum 3 inches of clearance). Check the front and back of the unit.
   - Check the unit exterior for damage.

You can find additional troubleshooting topics at the following:

See "*Troubleshooting Hardware Issues*" on page 111.

Chapter 9

Removing and replacing appliance hardware components

This chapter includes the following topics:

- Overview
- Removing and replacing the bezel
- Removing and replacing NetBackup 5230 disk drives
- Removing and installing a NetBackup 5030 or NetBackup 5230 power supply
- Removing and replacing NetBackup 5220 Appliance storage drives
- Removing and replacing a NetBackup 5220 Appliance power supply

Overview

This chapter provides information that describes how to remove and replace faulty components from NetBackup appliance. Some components are hot-swappable. Care must be taken to ensure that hot-swappable components are in a safe state before they are removed. Inappropriate removal of a hot-swappable component can disrupt system operation and result in data loss and data corruption. Contact Symantec Technical Support immediately if a component is removed inappropriately or the replacement part does not resolve the fault.

When handling electrical components, be sure to always apply appropriate ESD preventative measures. Do the following:

- Wear an appropriately grounded wrist strap, ESD-compliant gloves, or ESD-compliant clothing.
- Place the components on which you are working on a properly grounded, ESD-compliant surface.
- Leave replacement components in the ESD-compliant shipping material until you are ready to use them.

The effects of electrostatic damage are invisible and, often, do not appear immediately. Nonetheless, electrostatic damage can affect the performance and shorten the life of sensitive components.

See "*Removing and replacing appliance hardware components*" on page 120.

Removing and replacing the bezel

This section describes how to remove and replace the bezel on the front of the media server.

To remove the bezel

1. Depress and push in the left side (the side nearest the Symantec logo) of the bezel to dislodge the tabs that hold it in place.
2. Swing the dislodged side forward slightly and pull bezel out of the chassis.

To replace the bezel

1. Locate the notches in the inside edge of the bar that contains front panel LEDs and buttons.
2. Align the tabs on the right side of the bezel (side farthest from the Symantec logo) with the notches and insert.
3. Align the tabs on the left side of the bezel (side nearest the Symantec logo) with the notches in the bar.
4. Press the bezel down until the tabs snap into place. You may need to flex the bezel slightly.

See "*Removing and replacing appliance hardware components*" on page 120.

Removing and replacing NetBackup 5230 disk drives

Warning: A drive bay must not be open for longer than three minutes. The media server is constructed to optimize cooling. If a bay is empty for too long, the system will over heat and fail. If you cannot swap the failed drive within three minutes, place a drive cover over the bay until a drive can be installed.

To remove a disk drive:

1. Use the control panel on the front of the media server to identify the faulty disk drive. The system ID LED (second large LED from the top) is amber.
2. Put on an ESD wrist strap or take other ESD precautions.

   Note: An ESD wrist strap is shipped with replacement drives.

3. Remove the bezel. See "Removing and replacing the bezel" on page 121.
4. Locate and identify the faulty disk drive. The drive fault LED is solid amber and the bottom of the two.

5 Press the green button on the left side of the drive. The front panel pivots forward and the drive carrier ejects. The front panel also serves as a latch for the drive carrier. The following figure shows the drive latch.

6 Slide the drive carrier out of the bay.

To install a replacement drive

1 Put on a wrist strap or take other ESD precautions.

2 Grasp the replacement drive carrier by the sides or metal surfaces only and remove it from the shipping container.

Warning: Grasping and pinching any part of the printed circuit board on the drive can damage the drive.

---

3 Remove the drive carrier from the antistatic bag.

4 Press the green button on the left side of the carrier front panel to release the latch.

5 Slide the drive carrier into the slot until it makes contact with the back of the bay. Do not force the drive into place.

6 Close the front panel latch. The drive should click into place.

7 Replace the bezel.

See "*Removing and replacing appliance hardware components*" on page 120.

Removing and installing a NetBackup 5030 or NetBackup 5230 power supply

NetBackup Appliances have two power supplies to ensure high availability operation. If one power supply fails, you can replace it while the other supply provides power to the appliance (hot-swap).

Caution: A power supply is only hot-swappable when two power supplies are installed. At least one power supply must be in service to power the unit.

Note: The system periodically polls the power supplies to ensure that they operate. When a power supply does not respond, an error message is posted on the hardware monitor and an alert is sent to the designated party.

To remove a power supply

1 Put on a grounded ESD wrist strap or take other precautions against ESD damage.

2 Check the LEDs for both power supplies in the unit. If one is green, you can hot-swap the faulty power supply. If both are amber or one is amber and the other is off, perform the shutdown procedure on the unit.

3 On the faulty power supply, unplug the power cord.

4 Locate the green lever on the right side of the power cord socket and push it toward the socket to release the power supply. The following figure shows the green lever on the power supply.

5 Use the handle that is folded beneath the fan to pull the power supply out of the bay.

To replace a power supply

1. Put on a grounded ESD wrist strap or take other precautions against ESD damage.
2. Insert the replacement power supply into the power supply bay and push it all the way until it clicks into place.

Caution: To maintain adequate cooling within the appliance, both power supplies must be install. If you cannot replace the failed power supply, leave the failed unit in the bay until you have a replacement or install a filler panel. The filler panel allows the air to circulate as designed and keeps the unit from overheating. The following figure shows the filler panel.

See "*Removing and replacing appliance hardware components*" on page 120.

Removing and replacing NetBackup 5220 Appliance storage drives

The NetBackup 5220 Appliance has eight disk drives that are used for storage. The drives are located in slots behind the bezel in the front panel. The slots are identified in numerical order Slot 0 through Slot 7 starting with Slot 0 in the left corner of the appliance. Slot 7 is the designated hot spare. These drives are hot-swappable.

Proper air flow must be maintained within the chassis at all times. Drive slots must be covered when the appliance is in operation. If you have a faulty disk drive, leave it in the slot until you have a replacement.

Requirements

- Replacement disk drive from Symantec. The drive must be compatible with the other storage drives in the appliance.
- Take ESD precautions.

To remove a storage disk drive:

1. Wear a grounded wrist strap or take other ESD precautions.
2. Locate the failed disk drive in the appliance. The drive status LED on the right at the top of the drive is amber.
3. Press the green button at the top drive to release the black lever.
4. Pull down the black lever completely. This releases the drive from the slot.
5. Pull the drive forward slightly to ensure that it is disengaged, but do not remove it from the slot.
6. Wait one or two minutes for the disk to spin down (stop spinning). You can hear when it has stopped.
7. Completely remove the disk drive from the slot.

To install a storage disk drive:

1. Remove the replacement disk drive from Symantec from the ESD-protective package.
2. Press the green button on the replacement disk drive to release the black lever. in the fully open position and insert the disk drive into the slot.
3. Pull the lever down completely.
4. Orient the disk drive so that the green button is at the top of the appliance.
5. Insert the disk drive into the slot and carefully push the disk drive all of the way into the slot. The disk drive clicks when it is in place.

6 Close the lever.

7 Make sure that the drive status LED turns green.

See "*Removing and replacing appliance hardware components*" on page 120.

Removing and replacing a NetBackup 5220 Appliance power supply

The NetBackup 5220 Appliance has two power supplies to provide fault-tolerant operation. If one power supply fails, the other provides power to the appliance until the faulty power supply is replaced.

Power supplies are hot swappable. You can replace one while the appliance is in operation. At least one power supply must be functioning for the appliance to operate.

Caution: Do not leave a power supply bay empty for longer than 3 minutes. The NetBackup 5220 appliance is constructed for optimum air circulation when the unit is in operation. The appliance can overheat and damage vital components if a power supply bay is empty for longer than three minutes while the appliance is in operation.

Requirements

- Replacement NetBackup 5220 power supply from Symantec.

To remove and replace a NetBackup 5220 power supply:

1 Locate the replacement power supply module and remove the protective packaging. Set the power supply near the appliance requiring repair so that it can be installed quickly.

2 Disconnect the power cable from the faulty power supply.

3 Press in and hold the green lever on the right side of the power supply to release the module.

4 Grasp the handle between the two fans in the power supply module and pull the module out of the slot.

5 Orient the replacement power supply so that the green lever is on the right side of the appliance.

6 Insert a new power supply module until it clicks into place.

7 Plug the power cable into the power socket in the module.

See "*Removing and replacing appliance hardware components*" on page 120.

Chapter 10

Disaster Recovery

This chapter includes the following topics:

- About disaster recovery
- Disaster recovery best practices
- Disaster recovery scenarios

About disaster recovery

Disasters can strike your appliance at any time. Unfortunately, the definition of a disaster can change by region and be interpreted in different ways. An event such as a power supply failure, to an entire site loss are both in the realm of disaster recovery.

This chapter describes the following topics:

- Disaster recovery best practices
  You can implement strategies to help aid your recovery process in case a disaster strikes your appliance.
- Disaster recovery scenarios
  Look at high-level examples of failure scenarios and the steps that are needed to perform a recovery, minimizing data loss.

Before attempting any type of disaster recovery on your appliance, it is highly recommended to contact Symantec Technical Support for assistance. Symantec's support engineers work with you to ensure that the appropriate recovery steps are performed. 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.

Disaster recovery best practices

NetBackup offers a few different configuration options that can help aid in a disaster recovery process if a disaster strikes.

Note: Use the following topology configurations as a general guide. Contact your Symantec account representative to establish what topology configuration best fits your particular environment.

Single domain configuration:

- Create backups of the MSDP catalog. The backup protects the critical MSDP information about the contents of the backup data that exists on the NetBackup appliance.

  A policy is automatically created when configuring the NetBackup appliance for the first time as well as when adding MSDP storage during a Storage > Resize operation.

  Review the policy configuration and make changes to its schedules, backup window, and residence as required. Make sure to activate the policy to protect the catalog.

  See "MSDP catalog backup policy creation during initial configuration" in the *Symantec NetBackup Appliance Hardware Installation and Initial Configuration Guide* for more information.

- Create the appliance Master as a virtual machine, using Site Recovery Manager to replicate data from the protected site to the recovery site.

- Store catalog backups at an off-site location in case a recovery is necessary. You can use tape or cloud for restoration to a rebuilt master server at the disaster recovery site.

- Configure a setup using VCS Global Cluster Option. Global Cluster Option to VCS enables linking clusters from separate locations together and connecting applications across clusters. This connection provides complete service level protection against an entire site failure by providing applications failover to the remote site.

  An application is installed and configured on both clusters-local and remote, but is online on a system in local cluster and is configured to fail over globally on the remote cluster. The data is located on shared disks within each cluster and is replicated across clusters to ensure data concurrency.

  In an event of a disaster affecting an entire region, one can create a comprehensive Disaster Recovery solution by combining the capabilities of application clustering with data replication.

Note: Clustering environments are not supported on the NetBackup appliance.

Multi-domain configuration:

- Configure Auto Image Replication to replicate backups that are generated in one NetBackup domain to storage in another NetBackup domain.

Disaster recovery scenarios

The following disaster scenarios are provided as a guide to help you get your appliance running after a disaster.

Hardware-related scenarios

- See "Appliance sustained power interruption" on page 131.
- See "Appliance hardware failure" on page 133.
- See "Appliance storage disk failure" on page 136.
- See "Complete loss of appliance with recoverable operating system drives and attached storage disks" on page 136.
- See "Complete loss of appliance with recoverable attached storage disks" on page 138.
- See "Complete loss of appliance and attached storage disks" on page 167.

Software-related scenarios

- See "NetBackup appliance software corruption" on page 168.
- See "NetBackup appliance database corruption" on page 169.
- See "NetBackup appliance catalog corruption" on page 172.
- See "NetBackup appliance operating system corruption" on page 178.

Appliance sustained power interruption

If you have lost power at the site of your NetBackup appliance and storage systems for a sustained amount of time, use the following steps as a guide to help get your hardware turned on.

Note: The appliance continues to operate normally once the power is restored after a power outage.

Table 10-1 Steps for restoring power to an appliance following a power interruption

Step	Action	Description
Step 1	Initialize the storage systems and appliance hardware.	Initialize the hardware in the following order: ■ Storage systems ■ Master server ■ Media server **Note:** Always turn on the storage shelf that is furthest away from the main appliance first, then move to the next closest shelf until you reach the main appliance. See the section called "Power restoration procedures" on page 133. For more information on the hardware initialization process, see "Verifying the operation of the appliance and storage hardware" in the *Symantec NetBackup 5230 Appliance Hardware Installation Guide*.
Step 2	Verify the status of the hardware components.	Once the appliance and attached storage systems have initialized, verify the health status of all the hardware components. ■ Run the **Appliance Diagnostics Center** from the NetBackup Appliance Web Console, then choose **Perform a hardware health check**. See "Troubleshooting and tuning Appliance from the Appliance Diagnostics Center" on page 35. ■ Download the DataCollect log to check any logs associated with the hardware. See "*Working with log files*" on page 64.

Table 10-1 Steps for restoring power to an appliance following a power interruption *(continued)*

Step	Action	Description
Step 3	Verify that all NetBackup services have started.	Once you have verified that the status of the appliance hardware is healthy, check to make sure that all NetBackup services have resumed. All backup jobs resume once the appliance is turned on. You can check the NetBackup services through the Command Line Interface or the maintenance shell menu. **Note:** If a backup was in process when the power interruption occurred, the backup job likely failed.

Power restoration procedures

Use the following procedures as a guide to walk through restoring power to your hardware:

Appliance hardware failure

While failure of the NetBackup appliance hardware is rare, a failure can still strike the appliance for a number of reasons. Use the following steps as a guide to recovering your appliance from a hardware failure.

Symptoms of an appliance that has experienced a hardware failure:

- A warning message is displayed on the hardware monitor page or via email if configured for SNMP.
- The appliance does not boot or turn on. The system disk could be in a failed state.
- The appliance boots and turns on but shows hardware errors for components from the main appliance or the storage shelves.
- Virtual disks are degraded.

Table 10-2 Steps for recovering the appliance from a hardware failure

Step	Action	Description
Step 1	Turn on the appliance.	Press the power button and LED on the control panel on the front panel to turn on the unit. ■ If the unit does not turn on, make sure that the unit has power. See "Starting an appliance that does not turn on" on page 111. ■ If the unit still does not turn on, contact Symantec Technical Support for further assistance. ■ If the unit does turn on but with issues, proceed to the next step. ■ If the unit turns on with no issues, verify that all NetBackup services resume successfully.
Step 2	Determine the faulty hardware.	Perform the following actions to determine the faulty hardware: ■ Use the LED status indicators on the appliance to help determine if the hard disks and power supplies function correctly. See "Troubleshooting system status LED issues" on page 118. ■ Run the **Appliance Diagnostics Center** from the NetBackup Appliance Web Console, then choose **Perform a hardware health check**. See "Troubleshooting and tuning Appliance from the Appliance Diagnostics Center" on page 35. For more detailed procedures not covered in this guide, see the "Troubleshooting the system status LED faults" chapter of the *Symantec NetBackup™ 5230 Appliance Hardware Troubleshooting and Parts Replacement Guide*.

Table 10-2 Steps for recovering the appliance from a hardware failure *(continued)*

Step	Action	Description
Step 3	Replace the faulty hardware.	Once you have determined the hardware that needs replacement, remove the faulty hardware and replace with a new unit. User-replaceable hardware includes: ■ Power supplies ■ Hard disks See "Removing and replacing NetBackup 5230 disk drives" on page 122. For more detailed procedures not covered in this Guide, see the "Removing and replacing hardware" chapter of the *Symantec NetBackup™ 5230 Appliance Hardware Troubleshooting and Parts Replacement Guide*. **Note:** If you find that non-user replaceable hardware is faulty, contact Symantec Technical Support for further assistance.
Step 4	Verify that the hardware replacement is successful.	Perform the following actions to verify the status of the new hardware: ■ Use the LED status indicators on the appliance to help determine if the hard disks and power supplies are functioning correctly. See "Troubleshooting system status LED issues" on page 118. ■ Run the **Appliance Diagnostics Center** from the NetBackup Appliance Web Console, then choose **Perform a hardware health check**. See "Troubleshooting and tuning Appliance from the Appliance Diagnostics Center" on page 35.
Step 5	Verify that all NetBackup services have started.	Once you have verified that the status of the appliance hardware is healthy, check to make sure that all NetBackup services have resumed. All backup jobs resume once the appliance is turned on. **Note:** If a backup was in process when the power interruption occurred, the backup job likely failed.

Appliance storage disk failure

If you have encountered a failed disk or disks within the appliance, use the following steps as a guide to replacing the disks and verify there is no data loss.

Note: Multiple disk failures in an appliance can lead to loss of the entire file system.

Table 10-3 Steps for replacing a hard disk within the appliance after a hard disk failure

Step	Action	Description
Step 1	Remove the failed hard disk and replace with a new hard disk.	Remove and replace the hard disk in the appliance. See "Removing and replacing NetBackup 5230 disk drives" on page 122.
Step 2	Verify that all NetBackup services have started.	Once you have verified that the status of the appliance hardware is healthy, check to make sure that all NetBackup services have resumed. All backup jobs resume once the appliance is turned on.

Complete loss of appliance with recoverable operating system drives and attached storage disks

If the location your appliance resides has encountered a catastrophic event that requires an entire appliance replacement, but the operating system drives and attached storage disks are still operational, use the following steps as a guide to replace the appliance.

Note: Please contact Symantec Technical Support to assist you in replacing and reconfiguring your appliance. The steps provided in this procedure serve as a general guide for replacing the appliance with functioning attached disk storage.

Table 10-4 Steps for replacing an appliance with recoverable operating system drives and attached disk storage

Steps	Action	Description
Step 1	Remove the operating system and storage disks from the damaged appliance.	Symantec Technical Support dispatches service personnel to you who remove the drives from the appliance.

Table 10-4 Steps for replacing an appliance with recoverable operating system drives and attached disk storage *(continued)*

Steps	Action	Description
Step 2	Remove the damaged appliance and replace with a new appliance.	Symantec Technical Support dispatches service personnel to you who then help you get your new appliance installed and configured.
Step 3	Install the operating system and storage disks into the new appliance.	Symantec Technical Support dispatches service personnel to you who install the drives into the new appliance.
Step 4	Turn on the components.	Turn on the components in the following order: ■ Turn on the storage shelf that is the furthest away from the appliance and wait until the initialization completes. ■ Turn on the storage shelf that is nearest to the appliance and wait until the initialization completes. ■ Turn on the main appliance. **Note:** If your environment contains multiple appliances, recover the master server appliance first, then the media server second.
Step 5	Verify that all NetBackup services have started.	Once you have verified that the status of the appliance hardware is healthy, check to make sure that all NetBackup services have resumed. All backup jobs resume once the appliance is turned on.

Complete loss of appliance with recoverable attached storage disks

If the location your appliance resides has encountered a catastrophic event that requires an entire appliance replacement, but the attached storage disks are still operational, use the following steps as a guide to replace the appliance. This scenario assumes that your appliance hardware and operating system drives are not recoverable.

Note: Please contact Symantec Technical Support to assist you in replacing and reconfiguring your appliance. The steps provided in this procedure serve as a general guide for replacing the appliance with functioning attached disk storage.

Table 10-5 Steps for replacing an appliance after it has been rendered non-operational but the attached disk storage is still operational

Steps	Action	Description
Step 1	Remove the damaged appliance and replace with a new appliance.	Symantec Technical Support dispatches service personnel to you who then help you get your new appliance installed and configured.
Step 2	Export all data.	If you have data on your disks, you may have to export this data and move it to the new appliance. If the failed appliance was a master server, a catalog recovery is required.

Table 10-5 Steps for replacing an appliance after it has been rendered non-operational but the attached disk storage is still operational *(continued)*

Steps	Action	Description
Step 3	Turn on the components.	Turn on the components in the following order: ■ Turn on the storage shelf that is the furthest away from the appliance and wait until the initialization completes. ■ Turn on the storage shelf that is nearest to the appliance and wait until the initialization completes. ■ Turn on the main appliance. **Note:** If your environment contains multiple appliances, recover the master server appliance first, then the media server second.

Table 10-5 Steps for replacing an appliance after it has been rendered non-operational but the attached disk storage is still operational *(continued)*

Steps	Action	Description
Step 4	Reconfigure the new appliance with the existing storage disk systems.	Perform a reconfiguration of the new appliance. The reconfiguration process determines whether NetBackup storage objects have been detected. You have the option of preserving the following: ■ NetBackup catalog. ■ Pre-existing storage partitions and objects. Refer to the following topics for steps to reconfigure your appliance: ■ See "Reimaging a NetBackup appliance from the USB drive" on page 141. ■ See "Reconfiguring a 52xx master server appliance from the USB drive using the NetBackup Appliance Shell Menu" on page 149. ■ See "Configuring a master server to communicate with an appliance media server" on page 155. ■ See "Reconfiguring a 52xx media server appliance from the USB drive using the NetBackup Appliance Shell Menu" on page 157. **Note:** If you want to add an additional storage expansion shelf to your configuration, you can add it after the reconfiguration process is complete.

Appliance reconfiguration procedures

Use the following procedures as a guide to walk through reconfiguring your appliance:

Reimaging a NetBackup appliance from the USB drive

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 (`nnnnnnn.pfx`). If you select `no` for no password, a period precedes the file name (`.nnnnnnn.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.

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 (`P@ssw0rd`). 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.

---

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 149.

See "Reconfiguring a 52xx media server appliance from the USB drive using the NetBackup Appliance Shell Menu" on page 157.

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 (`nnnnnnn.pfx`). If you select `no` for no password, a period precedes the file name (`.nnnnnnn.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 *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 29.

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 29.

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 29.

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 In addition to the above network configuration settings, you may also use the **Main_Menu** > **Network** view to create a bond and to tag a VLAN during the initial configuration of your appliance network.

- Use the `Network > LinkAggregation Create` command to create a bond between two or more network interfaces.
- Use the `Network > VLAN Tag` command to tag a VLAN to a physical interface or bond interface.

For detailed information about the `LinkAggregation` and the `VLAN` command options, refer to the *NetBackup Appliance Command Reference Guide*.

10 From the **Main_Menu** > **Network** view, use the following commands to set the time zone, the date, and the time for this appliance:

- Set the time zone by entering the following command:

  ```
  TimeZone Set
  ```

  Select the appropriate time zone from the displayed list.

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

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

Where *Month* is the name of the month.
Where *Day* is the day of the month from 0 to 31.
Where *HHMMSS* is the hour, minute, and seconds in a 24-hour format. The fields are separated by semi-colons, for example, HH:MM:SS.
Where *Year* is the calendar year from 1970 through 2037.

11 From the **Main_Menu > Settings > Alerts > Email** 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 Server [Account] [Password]` The *Server* variable is the host name of the target SMTP server that is used to send emails. The [Account] option identifies the name of the account that was used or the authentication to the SMTP server. The [Password] option is the password for authentication to the SMTP server.
Enter email addresses	`Email Software Add Addresses` Where Addresses is the user's email address. To define multiple emails, separate them with a semi-colon.

12 Set the role for the appliance to a master server.

From the **Main_Menu** > **Appliance** view, run the following command:

```
Master
```

13 After you set the role configuration, the disk storage prompts appear for the Catalog, AdvancedDisk, and Deduplication (MSDP) partitions.

To configure storage partitions, you must do the following:

- Enter a size for the NetBackup catalog on the master server.
  To skip the configuration for the NetBackup catalog partition, enter **0** when prompted for its size. To keep the partition at its current size, press **Enter**.
- Enter a storage pool size in GB or TB.
  To skip the storage pool size configuration for any partition, enter **0** when prompted for its size. To keep the storage pool at its current size, press **Enter**.
- Enter a disk pool name.
  The default names are *dp_adv_<hostname>* for AdvancedDisk and *dp_disk_<hostname>* for Deduplication. To keep the default names, press **Enter**.

- Enter a storage pool name.
  The default names are *stu_adv_<hostname>* for AdvancedDisk and *stu_disk_<hostname>* for Deduplication. To keep the default names, press **Enter**.

The storage prompts appear in the following order:

```
NetBackup Catalog volume size in GB [default size]:
AdvancedDisk storage pool size in GB/TB [default size]:
AdvancedDisk diskpool name:
AdvancedDisk storage unit name:
MSDP storage pool size in GB/TB [default size]:
MSDP diskpool name:
MSDP storage unit name:
```

After you configure the storage partitions, a summary of the storage configuration appears with the following prompt:

```
Do you want to edit the storage configuration? [yes, no]
```

Type **yes** to make any changes, or type **no** to keep the current configuration.

14 Disconnect the laptop from the **NIC1** appliance port.

Note: If your network uses the 192.168.x.x IP address range, refer to the following topic for important information:

---

15 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 155.

See "Reconfiguring a 52xx media server appliance from the USB drive using the NetBackup Appliance Shell Menu" on page 157.

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 NetBackup Appliance Shell Menu: ■ From the **Main_Menu** > **Settings** view, run the following command: `Settings > NetBackup AdditionalServers Add media-server` Where *media-server* is the fully qualified host name (FQHN) of the appliance media server that is not yet configured. If the appliance has more than one host name, you must add all of the names.

For a traditional NetBackup 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 157.

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 theNetBackup 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 theNetBackup 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 (`nnnnnnn.pfx`). If you select `no` for no password, a period precedes the file name (`.nnnnnnn.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 *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 29.

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 29.

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 29.

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 In addition to the above network configuration settings, you may also use the **Main_Menu** > **Network** view to create a bond and to tag a VLAN during the initial configuration of your appliance.

- Use the `Network > LinkAggregation Create` command to create a bond between two or more network interfaces.
- Use the `Network > VLAN Tag` command to tag a VLAN to a physical interface or bond interface.

For detailed information about the `LinkAggregation` and the `VLAN` command options, refer to the *NetBackup Appliance Command Reference Guide*.

10 From the **Main_Menu** > **Network** view, use the following commands to set the time zone, the date, and the time for this appliance:

- Set the time zone by entering the following command:

  ```
  TimeZone Set
  ```

  Select the appropriate time zone from the displayed list.

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

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

Where *Month* is the name of the month.

Where *Day* is the day of the month from 0 to 31.

Where *HHMMSS* is the hour, minute, and seconds in a 24-hour format. The fields are separated by semi-colons, for example, HH:MM:SS.

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

11 From the **Main_Menu > Settings > Alerts > Email** 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 Server [Account] [Password]` The *Server* variable is the host name of the target SMTP server that is used to send emails. The [Account] option identifies the name of the account that was used or the authentication to the SMTP server. The [Password] option is the password for authentication to the SMTP server.
Enter email addresses	`Email Software Add Addresses` Where Addresses is the user's email address. To define multiple emails, separate them with a semi-colon.

12 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.

13 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
```

---

14 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.

15 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
```

16 Disconnect the laptop from the **NIC1** appliance port.

Note: If your network uses the 192.168.x.x IP address range, refer to the following topic for important information:

Complete loss of appliance and attached storage disks

If the location your appliance resides has encountered a catastrophic event that requires an entire appliance replacement, use the following steps as a guide to replace the appliance. This scenario assumes that your appliance, operating system drives, and attached storage disks are not recoverable.

Note: Please contact Symantec Technical Support to assist you in replacing your appliance. The steps provided in this procedure serve as a general guide for performing a disaster recovery.

Table 10-6 Steps for replacing an appliance and attached storage disk units after they have been rendered non-operational

Steps	Action	Description
Step 1	Remove the damaged appliance and replace with a new appliance.	Symantec Technical Support will dispatch service personnel to you who will then help you get your new appliance installed.
Step 2	Remove the damaged storage systems and replace with new storage systems.	All damaged storage systems must be replaced at the same time the appliance hardware is replaced so a proper configuration can be achieved. Symantec Technical Support will assist you in replacing the storage systems.

Table 10-6 Steps for replacing an appliance and attached storage disk units after they have been rendered non-operational *(continued)*

Steps	Action	Description
Step 3	Power on the new components.	Power on the components in the following order: ■ Storage systems ■ Master server ■ Media server
Step 4	Configure the appliance and storage systems.	Configure the appliance as you would a new configuration. See the "Initial Configuration" chapter of the *Symantec NetBackup 52xx Appliance Hardware Installation and Initial Configuration Guide* for more information on setting up your appliance and attached storage systems.
Step 5	Recover the data from a secondary backup site.	If you have a secondary backup site, Symantec Technical Support will help you work through recovering your data from a secondary backup site.

NetBackup appliance software corruption

Use the following steps as a guide to determine the type of software corruption you are experiencing and where you can get more information on your specific scenario

Table 10-7 Steps for determining the type of software corruption

Steps	Action	Description
Step 1	Determine the software corruption that has occurred on the appliance.	The following are types of software corruption that can happen on the appliance due to many factors: ■ Database corruption: A change you made is not being displayed or nothing is being displayed at all. ■ Catalog corruption: You lose the ability to perform backups or restores or you are not seeing images being backed up. ■ Operating system corruption: You are not able to log in or you are not able to perform any of NetBackup and NetBackup appliance operations. **Note:** If you have more severe software corruption than what is listed here, contact Symantec Technical Support with your specific scenario for further assistance.
Step 2	Perform disaster recovery for your specific software corruption case.	See See "NetBackup appliance database corruption" on page 169. for database corruption disaster recovery. See See "NetBackup appliance catalog corruption" on page 172. for catalog corruption disaster recovery. See See "NetBackup appliance operating system corruption" on page 178. for operating system corruption disaster recovery.

NetBackup appliance database corruption

Database corruption may have occurred if you have made changes to the configuration, or your appliance is not displaying anything when booted up.

Use the following steps as a guide to recover a corrupt database on the appliance.

Table 10-8 Steps for recovering a corrupt database on the appliance

Steps	Action	Description
Step 1	Roll back the appliance to a previously created checkpoint.	If you have determined your database is corrupt, you can rollback your appliance to an existing checkpoint. See "Rollback to an appliance checkpoint from the appliance shell menu" on page 170.
Step 2	Verify that the rollback is successful.	Verify that the rollback has reverted 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 rollback: ■ The NetBackup catalog on the master server appliance is not included. ■ The backup data is not included. See "About appliance rollback validation" on page 171.

Appliance rollback procedures

Use the following procedures as a guide to performing a rollback on an appliance:

Rollback to an appliance checkpoint from the appliance shell menu

The following procedure describes how to roll back an appliance to a checkpoint from the appliance shell menu.

To roll back to an existing checkpoint from the appliance shell menu

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

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

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

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

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

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

6 Enter **Yes** to begin the rollback to a checkpoint operation.

The following status is provided once the rollback operation is started.

```
Rollback to checkpoint? (yes/no) yes
- [Info] Stopping NetBackup Services...please wait.
- [Info] PERFORMING REVERT TO USER CHECKPOINT
- [Info] This takes approx. 15 to 20 mins. Please wait...
- [Info] Rollback to Appliance Checkpoint (User directed
         checkpoint) successful.

A reboot of the appliance is required to complete the
checkpoint rollback. Reboot now? (Type REBOOT to continue) REBOOT
Rebooting the appliance now...
- [Info] Rebooting app2.symantec.com

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

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

About appliance rollback validation

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

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

Rolling back to an appliance checkpoint reverts the following components:

- The appliance operating system
- The appliance software
- The NetBackup software
- The network configuration

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

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

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

NetBackup appliance catalog corruption

Catalog corruption may have occured if you lose the ability to perform backups and restores or you are not seeing images being backed up.

Use the following steps as a guide to recover a corrupt catalog on the appliance.

Table 10-9 Steps for recovering from catalog corruption on the appliance

Steps	Action	Description
Step 1	Perform a factory reset on the appliance while retaining the storage configuration and backup data.	An appliance factory reset returns your appliance to a clean, unconfigured, and default state. You can choose to retain the storage configuration and backup data during this process to avoid reconfiguring the appliance after a factory reset. See "Starting a factory reset from the appliance shell menu" on page 173. for a detailed procedure on performing a factory reset. See "Appliance factory reset" in the *Symantec NetBackup Appliance 2.6 Administrator's Guide* for more information on the topic of factory reset.

Table 10-9 Steps for recovering from catalog corruption on the appliance *(continued)*

Steps	Action	Description
Step 2	Verify that the factory reset is successful.	Verify that the rollback has reverted the following components: ■ Appliance operating system ■ Appliance software ■ NetBackup software ■ Tape media configuration on the master server ■ Networking configuration ■ Storage configuration and backup data (optionally retain) **Note:** If the factory reset does not fix the catalog corruption, proceed to Step 3.
Step 3	Reconfigure the appliance with the catalog recovery option.	If the factory reset is not successful, an appliance can be reconfigured to your original configuration. Symantec recommends that you record all of your initial configuration information so that you can reference that information during the reconfiguration process. See the section called "Appliance reconfiguration procedures" on page 141. for detailed procedures on reimaging and reconfiguring your appliance. See "Reconfiguring a NetBackup appliance" in the *Symantec NetBackup Appliance 2.6 Administrator's Guide* for more information about the reconfiguration process.

Factory reset procedures

Use the following procedures as a guide to walk through performing a factory reset on your appliance:

Starting a factory reset from the appliance shell menu

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

Note: Factory reset operations are not supported if a 52xx master server or media server has been upgraded to version 2.6. Factory reset is only supported after a clean installation of version 2.6 on a 52xx appliance, or if a 52xx appliance is reimaged to version 2.6

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

```
Appliance factory reset will reset the entire system
to the factory installed image. The appliance will have the following components
reset to the factory restored settings/image:
1) Appliance Operating System
2) Appliance Software
3) NetBackup Software
4) Tape media configuration on the master server
5) Networking configuration (optionally retain)
6) Storage configuration and backup data (optionally retain)

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

RESET NETWORK CONFIGURATION [Optional]
        -- Resets the IP and routing configuration.
        -- Resets the DNS configuration.
 >> Do you want to reset the network configuration? [yes/no] (yes) no

RESET STORAGE CONFIGURATION and BACKUP DATA [Optional]
        -- Removes all the images on the AdvancedDisk and MSDP storage pools.
        -- Resets the storage partitions.
        -- Resets storage expansion units, if any.
 >> Do you want to delete images and reset backup data? [yes/no] (yes)
 >> Resetting the storage configuration will remove all backup
    data on the storage partitions and any connected expansion
    units. This is not reversible. Are you sure you want to
    reset storage configuration? [yes/no] (yes)
 >> A reboot of the appliance is required to complete the factory reset.
    Reboot automatically after reset? [yes/no] (no) yes
 >> Automatically rebooting after the reset will not provide you with an
    opportunity to review the progress/final status of the reset. Are you sure
    you would like to automatically reboot? [yes/no] (no) yes
```

3 After you respond to these questions, the **Factory Reset Summary** is shown. The following is an example of the summary:

```
FACTORY RESET SUMMARY
---------------------
Reset Appliance OS, software configuration          : [YES]
Reset Appliance network configuration               : [NO]
Reset Appliance storage configuration (REMOVE DATA) : [YES]
Auto reboot after reset?                            : [YES]

Appliance will make the following version changes:

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

4 The following warning appears. If you want to begin the factory reset operation, enter **Yes**.

```
WARNING: An Appliance Factory reset cannot be reversed!
Continue with factory reset?? (yes/no) yes
```

The following summary messages appear as the factory reset continues:

```
- [Info] PERFORMING APPLIANCE RESET TO FACTORY STATE ON : app2.symantec.com
- [Info] Delete checkpoints (type: NON_FACT) succeeded
- [Info] Reset of the appliance to FACTORY STATE successful.
- [Info] Stopping NetBackup processes... (6 mins approx)
- [Info] Moving NetBackup Appliance Directory to ce-win21-urmi1...
- [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.

NetBackup appliance operating system corruption

Operating system corruption may have occurred if you are not able to log in or you are not able to perform any of the NetBackup or NetBackup appliance operations.

Use the following steps as a guide to recover a corrupt operating system on the appliance.

Table 10-10 Steps for recovering from operating system corruption on the appliance

Steps	Action	Description
Step 1	Perform a factory reset on the appliance while retaining the storage configuration and backup data.	An appliance factory reset returns your appliance to a clean, unconfigured, and default state. You can choose to retain the storage configuration and backup data during this process to avoid reconfiguring the appliance after a factory reset. See "Starting a factory reset from the appliance shell menu" on page 173. for a detailed procedure on performing a factory reset. See "Appliance factory reset" in the *Symantec NetBackup Appliance 2.6 Administrator's Guide* for more information on the topic of factory reset. **Note:** If a factory checkpoint is not available, proceed to Step 3 to reconfigure the appliance.
Step 2	Verify that the factory reset is successful.	Verify that the rollback has reverted the following components: ■ Appliance operating system ■ Appliance software ■ NetBackup software ■ Tape media configuration on the master server ■ Networking configuration ■ Storage configuration and backup data (optionally retain) **Note:** If the factory reset does not fix the operating system corruption, proceed to Step 3.

Table 10-10 Steps for recovering from operating system corruption on the appliance *(continued)*

Steps	Action	Description
Step 3	Reconfigure the appliance.	An appliance can be reconfigured to your original configuration. Symantec recommends that you record all of your initial configuration information so that you can reference that information during the reconfiguration process. See the section called "Appliance reconfiguration procedures" on page 141. for detailed procedures on reimaging and reconfiguring your appliance. See "Reconfiguring a NetBackup appliance" in the *Symantec NetBackup Appliance 2.6 Administrator's Guide* for more information about the reconfiguration process.

Chapter 11

NetBackup Appliance error messages

This chapter includes the following topics:

- About NetBackup Appliance error messages
- Error messages displayed during initial configuration
- Error messages displayed on the NetBackup Appliance Web Console
- Error messages displayed on the NetBackup Appliance Shell Menu
- NetBackup status codes applicable for NetBackup Appliance

About NetBackup Appliance error messages

For the 2.6.0.x release we have put together a repository of the most important error messages that you may come across when accessing the NetBackup Appliance using the NetBackup Appliance Web Console and theNetBackup Appliance Shell Menu. This section displays the Explanation and Recommended action for each error message. This section also lists the NetBackup status codes applicable to the NetBackup Appliance. This section includes the following types of error messages:

- See "Error messages displayed during initial configuration" on page 182.
- See "Error messages displayed on the NetBackup Appliance Web Console" on page 183.
- See "Error messages displayed on the NetBackup Appliance Shell Menu" on page 203.
- See "NetBackup status codes applicable for NetBackup Appliance" on page 210.

Error messages displayed during initial configuration

Table 11-1 lists some of the common error messages that you may come across during the initial configuration of your NetBackup Appliance:

Table 11-1 Errors in initial configuration

Error messages	Explanation	Recommended action
Failed to configure DNS settings or host name Resolution entries due to some unexpected error.	This error message is displayed when there is a problem in setting the DNS information. This error may occur because the script did not return valid input or some unexpected condition occurs.	Please gather the device logs using the `DataCollect` command and Contact support.
Failed to load Host Configuration settings due to some unexpected error.	This message appears when there is a problem in getting the DNS information for the appliance. This error may occur because the script did not return a valid input or some unexpected condition occurs.	Please gather the device logs using the `DataCollect` command and Contact support.
Failed to validate host name due to some unexpected error.	This message appears when there is some problem in host name lookup service. The script did not return a valid output or some unexpected condition occurred.	Please gather the device logs using the `DataCollect` command and Contact support.
Unable to connect to Master Server.	This message appears due to the following reasons: ■ If you select the role as media, and enter the host name of a master server. ■ If the master server is not reachable or if the NetBackup processes on the master server are down.	You can resolve this issue by performing the following checks: ■ Please check if master server is pingable. ■ Please ensure that all the NetBackup precesses are up and running.
Incorrect user input - The master server name cannot be same as the appliance host name.	This message appears if you select the role as media, and enter the host name of a master server.	Please enter the correct master server name.

See “NetBackup status codes applicable for NetBackup Appliance” on page 210.

See “Error messages displayed on the NetBackup Appliance Shell Menu” on page 203.

See "Error messages displayed on the NetBackup Appliance Web Console" on page 183.

Error messages displayed on the NetBackup Appliance Web Console

This section lists the common error messages that you may come across while working with the NetBackup Appliance using the NetBackup Appliance Web Console on the following tabs:

- Table 11-2 lists the error messages displayed on the Login screen and the NetBackup Appliance Web Console Dashboard.
- Table 11-3 lists the error messages displayed on the **Monitor > Hardware** tab.
- Table 11-4 lists the error messages displayed on the **Monitor > SCSP** tab.
- Table 11-5 lists the error messages displayed on the **Manage > Storage** tab.
- Table 11-6 lists the error messages displayed on the **Manage > Host** tab.
- Table 11-7 lists the error messages displayed on the **Manage > Appliance Restore** tab.
- Table 11-8 lists the error messages displayed on the **Manage > License** tab.
- Table 11-9 lists the error messages displayed on the **Manage > Migration Utility** tab.
- Table 11-10 lists the error messages displayed on the **Manage > Software Updates** tab.
- Table 11-11 lists the error messages displayed on the **Manage > Additional Server** tab.
- Table 11-12 lists the error messages displayed on the **Settings > Notification** tab.
- Table 11-13 lists the error messages displayed on the **Settings > Network** tab.
- Table 11-14 lists the error messages displayed on the **Settings > Date and Time** tab.
- Table 11-15 lists the error messages displayed on the **Settings > Authentication** tab.
- Table 11-16 lists the error messages displayed on the **Settings > Password** tab.
- Table 11-17 lists the error messages that are common across all the tabs on the NetBackup Appliance Web Console.

Table 11-2 lists all the error messages, displayed on the Login screen and NetBackup Appliance Web Console Dashboard.

Table 11-2 Login screen and NetBackup Appliance Web Console Dashboard

Error message	Explanation	Recommended action
The current session has expired. Redirecting to Login Page.	Your current session has expired because the appliance NetBackup Appliance Web Console has been idle for more than 10 minutes.	Kindly try to log on to your appliance again.
Login was unsuccessful, click ? for details.	This error is displayed: ■ 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.	■ 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`
User authentication failed. Please enter valid user name and password. If problem persists contact your System Administrator.	This error can be displayed due to the following reasons: ■ If the provided user name and password is incorrect. ■ If the authentication server is not responsive.	■ Verify that you have entered the correct user name and password. ■ Contact your System Administrator in case the error appears again.
The connection has timed out.	This error is displayed, if the web server is not responsive the login page is not displayed.	Contact your System Administrator for more assistance.
Unable to connect	This error is displayed, if the web server has been shut down.	Contact your System Administrator for more assistance.
Error occurred while connecting to the Symantec Product Authentication Service (AT). Please ensure that the AT service is running.	This error is displayed, if the authentication server is not responsive.	Contact your System Administrator in case the error appears again.

Table 11-2 Login screen and NetBackup Appliance Web Console Dashboard *(continued)*

Error message	Explanation	Recommended action
Error retrieving the deduplication ratio, due to an unexpected error.	This error is displayed, if the current deduplication ratio could not be displayed on the Deduplication tile.	Ensure that the deduplication solution is configured. If the problem persists contact Symantec Support.
Error retrieving the deduplication ratio, check again after 10 minutes.	This error is displayed, if the deduplication ratio could not be displayed due to an unexpected error.	Refresh the information from the Dashboard after 10 minutes. If the error persists, contact Symantec Support.
Login failure due to an unrecognized or invalid user	If the user is removed from the LDAP directory (and not removed from appliance allowed to log in list), though the user is listed as LDAP authorized user, the user will not be able to log in. So, these users poses no security threat.	In the case, an LDAP user that is configured to use the Appliance need to be deleted or removed from the LDAP directory, then the user needs to be first removed from the appliance. Otherwise, we will not be able to remove that user from the appliance user list.

Table 11-3 lists all the error messages that are displayed on the **Monitor > Hardware** tab.

Table 11-3 Monitor > Hardware

Error messages	Explanation	Recommended action
Unable to retrieve the hardware health information.	This message is displayed when the appliance is unable to reach the Call Home server and retrieve hardware health information.	The Call Home server might be unreachable. Try viewing the details later.
Unable to acknowledge/remove acknowledgment for the selected errors.	This message is displayed when there is an internal error in acknowledging or removing the acknowledgment for an error notification.	You may want to try acknowledging or removing the acknowledgment for an error notification through the NetBackup Appliance Shell Menu using the `Settings > Alerts > AcknowledgeErrors` command.
Cannot flash the disk drive light.	This message is displayed when the beacon is unable to flash lights for a disk drive.	There may be a technical issue with the beacon on the disk drive. Call Symantec Technical Engineer to fix the beacon.

Table 11-3 Monitor > Hardware *(continued)*

Error messages	Explanation	Recommended action
Invalid entry. Enter a whole number from 1 to 300.	This message is displayed when you enter an invalid value for the duration to flash the beacon. The value should be a whole number and it should range between 1 and 300 (in minutes).	Check the value that you have entered for flashing the beacon and ensure that it falls in the valid range.
No adapters were detected.	This message is displayed when the adapter information cannot be retrieved from the Call Home server.	You may want to call Symantec Technical Support for assistance in resolving this error.
No BBUs were detected.	This message is displayed when the Battery Backup Unit (BBU) information cannot be retrieved from the Call Home server.	You may want to call Symantec Technical Support for assistance in resolving this error.
No CPUs were detected.	This message is displayed when the CPU information cannot be retrieved from the Call Home server.	You may want to call Symantec Technical Support for assistance in resolving this error.
No disks were detected.	This message is displayed when the disks information cannot be retrieved from the Call Home server.	You may want to call Symantec Technical Support for assistance in resolving this error.
No fans were detected.	This message is displayed when the fan information cannot be retrieved from the Call Home server.	You may want to call Symantec Technical Support for assistance in resolving this error.
No firmware were detected.	This message is displayed when the firmware information cannot be retrieved from the Call Home server.	You may want to call Symantec Technical Support for assistance in resolving this error.
MSDP information is not available.	This message is displayed when the MSDP is not configured for the appliance or the appliance is unable to reach the Call Home server.	Verify if you have configured MSDP for your appliance. If you have configured MSDP and you encounter this error, call Symantec Technical Support for assistance in resolving this error.

Table 11-3 Monitor > Hardware *(continued)*

Error messages	Explanation	Recommended action
Partition information is not available.	This message is displayed when the partition information cannot be retrieved from the Call Home server.	You may want to call Symantec Technical Support for assistance in resolving this error.
No RAID groups were detected.	This message is displayed when the information for the RAID groups cannot be retrieved from the Call Home server.	You may want to call Symantec Technical Support for assistance in resolving this error.
Temperature information is not available.	This message is displayed when the temperature information cannot be retrieved from the Call Home server.	You may want to call Symantec Technical Support for assistance in resolving this error.

Table 11-4 lists all the error messages, displayed on the **Monitor > SCSP** tab.

Table 11-4 Monitor > SCSP

Error messages or Error type	Explanation	Recommended action
Certificate download failed.	The provided SSL certificate for the SCSP server cannot be found and downloaded.	Please check your Internet connection, verify the used path to download the certificate, and try again.
Please enter a valid port	The provided SCSP server port details are incorrect.	Please verify that the port number, entered for the SCSP server is correct.
There are no audit logs to display.	The SCSP logs cannot be displayed on the NetBackup Appliance Web Console. This error is displayed when: ■ If you are connected to the SCSP server and the audit logs are currently being pushed to SCSP server. ■ If the logs are not available locally.	To view the SCSP logs, log onto the SCSP server and check the logs.

Table 11-4 Monitor > SCSP *(continued)*

Error messages or Error type	Explanation	Recommended action
There are no audit logs to display.	If you are not connected to the SCSP server and you cannot see the logs.	Please use any of the following methods to fix this error: ■ Refresh GUI couple of times, verify using the NetBackup Appliance Shell Menu. ■ Stop and restart the web server. Revisit the **Monitor > SCSP** tab.
The SCSP documentation link does not provide the required information.	This error can occur if your Internet connection is down.	Please use any of the following methods to fix this error: ■ Check your Internet connection. ■ Check SymHelp for additional information about SCSP
Logs are filling up the storage space on your appliance.	This error is displayed when the SCSP server is not connected and the retention settings are set to default.	Please use any of the following methods to fix this error: ■ Establish the connection to your SCSP server. ■ Set the retention period that is lesser than the default retention period of 30 days.
The connection to the SCSP server could not be established.	This error is displayed when: ■ The SCSP server should be in the same network as the appliance. ■ The SCSP server or host name or IP address are incorrect. ■ The authentication certificate for the SCSP server cannot be found. ■ The authentication certificate for the SCSP server is corrupted.	Please use any of the following methods to fix this error: ■ Ensure that the SCSP server is in the same network as the appliance. ■ Ensure that the SCSP server or host name or IP address are correct. ■ Download a local copy of the authentication certificate and use it to authenticate the SCSP server. ■ Replace the existing certificate with a valid authentication certificate for the SCSP server.
Retention button is disabled	This error is displayed if you are connected to SCSP server, then the audit logs are managed by SCSP server and retention settings are not applicable.	There is no action recommended for this situation.

Table 11-5 lists all the error messages, displayed on the **Manage > Storage** tab.

Table 11-5 Manage > Storage

Error messages	Explanation	Recommended action
Failed to fetch storage information.	This error can be displayed due to the following reasons: ■ This message appears if storage script is not able to fetch any partitions, disks, and distributions. ■ This message can also appear if the connection between the appliance core and the NetBackup Appliance Web Console is lost.	Please contact Symantec Support. **Warning:** This is non-recoverable error. You need to collect all the `Vxul` logs using the `DataCollect` command and share them with the Symantec Support team to debug the error.
Source and target disks are same.	This message can appear when you perform the **Move Partition** operation. It occurs if you select the same disk name in the **From** and **To** drop-down lists.	You cannot select the same disk name, select a different target disk than source.
The maximum length is 256 characters.	This message appears in case there is an error in the provided name for a storage unit or a disk pool.	Enter a name that is lesser than 256 characters.
The following characters are not allowed: in the storage unit and disk pool name	This message appears in case the provided name for a storage unit or a disk pool contains following characters: `~!@#$%^&*()=|\\\"\'\:;<,>,?/	Remove the following special characters from the storage unit or disk pool name: `~!@#$%^&*()=|\\\"\'\:;<,>,?/

Table 11-6 lists all the error messages, displayed on the **Manage > Host** tab.

Table 11-6 Manage > Host

Error messages	Explanation	Recommended action
Error resetting deduplication parameters.	The appliance cannot reset the current deduplication parameters to the default settings.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.

Table 11-6 Manage > Host *(continued)*

Error messages	Explanation	Recommended action
Error while retrieving deduplication parameters	The current deduplication parameters for the appliance cannot be displayed.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Error in updating deduplication Parameters	The current deduplication parameters for the appliance cannot be updated to the new parameters.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Error resetting data buffer parameters.	The appliance cannot reset the current data buffer parameters to the default settings.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Error in updating data buffer parameters.	The current data buffer parameters for the appliance cannot be updated to the new parameters.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Error while retrieving data buffer parameters.	The current data buffer parameters for the appliance cannot be displayed.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Error while retrieving storage lifecycle parameters.	The current storage lifecycle parameters for the appliance cannot be displayed.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Error in updating storage lifecycle parameters.	The current storage lifecycle parameters for the appliance cannot be updated to the new parameters.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Error while retrieving BMR status.	The current BMR status for the appliance cannot be displayed.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Error in updating BMR settings. Error updating BMR status on this appliance.	The BMR settings for the appliance cannot be enabled.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
The BMR option was not selected.	The BMR settings for the appliance cannot be enabled.	Select the **Enable BMR on this Appliance** option.

Table 11-7 lists all the error messages, displayed on the **Manage > Appliance Restore** tab.

Table 11-7 Manage > Appliance Restore

Error messages	Explanation	Recommended action
Failed to reset all or some of the appliance(s).	System resources could be busy.	Restart the appliance and then retry factory reset.
Failed to reset the storage. Check the logs for additional information.	Mount points could be busy.	Look at the logs and contact Symantec Technical Support for further assistance.
Factory reset is not supported because no factory checkpoints exist. Please see the *Symantec NetBackup Appliance Administrator's Guide* for more information on how to reset this appliance. Click ? for more information.	This error occurs when trying to reset the appliance after it has been upgraded.	Roll back the appliance to a post-upgrade checkpoint.
Appliance checkpoint creation failed. Click **Finish** to go back to the Appliance Restore page.	This error can occur due to insufficient disk space to store the checkpoint.	Look for additional information, listed above the error message. Retry the operation. Cleanup is done in case of such failures, which can free up disk space.
Checkpoint validation was unsuccessful. The rollback operation cannot be started. Click ? for more information.	Secured network communication has issues.	Look for additional information, listed above the error message. Try to correct the error and retry the operation.
Rollback of the appliance configuration was not successful. Click ? for more information.	Appliance configuration (NetBackup Appliance Directory) rollback failed.	Contact Symantec Technical Support for further assistance.

Table 11-8 lists all the error messages, displayed on the **Manage > License** tab.

Table 11-8 Manage > License

Error messages	Explanation	Recommended action
Selected licenses could not be deleted for media server {0}. Selected licenses could not be deleted for master server {0}.	This error may appear due to an internal system error.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.

Table 11-8 Manage > License *(continued)*

Error messages	Explanation	Recommended action
Error in adding License	This error can appear due to the following reasons: ■ The license key may be invalid. ■ Due to an internal system error.	Try the following actions to resolve this issue: ■ Check whether the license is valid, or contact Symantec Technical Support. ■ Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Error in deleting License	This error may appear due to an internal system error.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Error while retrieving License List.	This error may appear due to an internal system error.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Error occurred while loading the license keys.	This error may appear due to an internal system error.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
License key: {0} failed to install on media server {1}. License key: {0} failed to install on master server {1}.	This error can appear due to the following reasons: ■ The license key may be invalid. ■ Due to an internal system error.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.

Table 11-9 lists all the error messages, displayed on the **Manage > Migration Utility** tab.

Table 11-9 Manage > Migration Utility

Error messages	Explanation	Recommended action
Failed to send the selected criteria.	This message appears when there is an internal NetBackup problem or a communications error.	Please try again as it can be due to an intermittent communications error. If the problem persists, collect the GUI logs using the `DataCollect` command for additional details or contact Symantec Technical Support.

Table 11-9 Manage > Migration Utility *(continued)*

Error messages	Explanation	Recommended action
Failed to cancel the job.	This message appears when there is an internal NetBackup problem or a communications error.	Please try again as it can be due to an intermittent communications error. If the problem persists, collect the GUI logs using the `DataCollect` command for additional details or contact Symantec Technical Support.
Failed to view the job details.	This message appears when there is an internal NetBackup problem or a communications error.	Please try again as it can be due to an intermittent communications error. If the problem persists, collect the GUI logs using the `DataCollect` command for additional details or contact Symantec Technical Support.
Failed to send the selected policy.	This message appears when there is an internal NetBackup problem or a communications error.	Please try again as it can be due to an intermittent communications error. If the problem persists, collect the GUI logs using the `DataCollect` command for additional details or contact Symantec Technical Support.

Table 11-10 lists all the error messages, displayed on the **Manage > Software Updates** tab.

Table 11-10 Manage > Software Updates

Error messages	Explanation	Recommended action
Load online updates failed.	This error is displayed when the appliance fails to get the online updates.	Please check the network connection to Symantec's software update center, or check the script for internal errors.
Load available updates failed.	This error is displayed when you do not get the available update, that is you cannot get the status of the downloaded software update.	Please check the script for internal errors.
Error while retrieving online update list manage.	This error is displayed when there is an error retrieving the online updates.	Please check the network connection to Symantec's software update center, or check the script for internal errors.
Error while retrieving software update list.	This error is displayed if the software update list cannot be retrieved.	Please check the script for internal errors.

Table 11-10 Manage > Software Updates *(continued)*

Error messages	Explanation	Recommended action
Error while retrieving preinstallation check questions, please contact system admin to check if there is a problem with rpm file.	This error is displayed if preinstallation check questions cannot be retrieved.	Please contact system admin to check if there is a problem with `rpm` (SUSE installer package) file.

Table 11-11 lists all the error messages, displayed on the **Manage > Additional Server** tab.

Table 11-11 Manage > Additional Server

Error messages	Explanation	Recommended action
Unable to add additional server.	This error may appear due to an internal system error.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Unable to delete additional server.	This error may appear due to an internal system error.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Please provide a valid server name entries separated using a comma(,).	This error may appear if the server names are added without a comma or the list of servers end with a comma.	Please check the list of servers and ensure that the server names are separated using a comma and the list does not end with comma.

Table 11-12 lists all the error messages, displayed on the **Settings > Notification** tab.

Table 11-12 Settings > Notification

Error messages	Explanation	Recommended action
Please verify if this system has been provisioned to SYMAPPMON.	You might encounter this error when your appliance is not provisioned to SYMAPPMON and you try to save changes on the **Settings > Notifications** page.	Provision the appliance to SYMAPPMON server (or the Registration server). If the issue persists, call Symantec Technical Support.
Call Home test failed. Verify that this system has been correctly provisioned to SYMAPPMON.	This error message is displayed when the appliance is not provisioned and you click **Test Call Home** in the **Call Home Configuration Settings** pane of the **Settings > Notifications** page.	Provision the appliance to SYMAPPMON server. If the issue persists, call Symantec Technical Support.

Table 11-12 Settings > Notification *(continued)*

Error messages	Explanation	Recommended action
Failed to enable Call Home.	You might encounter this error when Call Home cannot be enabled and you try to save changes for the **Settings > Notifications** page.	You may want to call Symantec Technical Support for assistance in resolving this error.
Failed to disable Call Home.	You might encounter this error when Call Home cannot be disabled and you try to save changes for the **Settings > Notifications** page.	You may want to call Symantec Technical Support for assistance in resolving this error.
Unable to reach Call Home server.	You may encounter this error when the appliance is unable to reach the Call Home server.	You may want to call Symantec Technical Support for assistance in resolving this error.
Proxy authentication failed. One or more proxy entries could not be resolved or validated. Please review the proxy entries and make any necessary corrections.	This error message is displayed when you have entered invalid authentication details while enabling the proxy server and you try to save changes on the **Settings > Notifications** tab.	Verify that you have entered correct and valid authentication details for the proxy server, such as your proxy server credentials.
Error occurred while saving the registration details, update the details later.	This message is displayed when the appliance is unable to update the registration details to SYMAPPMON server. The failure to update the details may occur due to the following: ■ The appliance is not provisioned to SYMAPPMON. ■ Connectivity issues between the appliance and the SYMAPPMON server. ■ SYMAPPMON server might be unreachable.	You may want to verify the following: ■ Appliance is provisioned to SYMAPPMON server. ■ There are no connectivity issues between the appliance and the SYMAPPMON server.

Table 11-12 Settings > Notification *(continued)*

Error messages	Explanation	Recommended action
The appliance was unable to contact the Symantec support site to retrieve the location and the contact information that is currently on file for this appliance. Please re-enter the information in the fields below.	This message is displayed when the appliance is unable to retrieve the registration details from SYMAPPMON server. The failure to update the details may occur due to the following: ■ The appliance is not provisioned to SYMAPPMON. ■ Connectivity issues between the appliance and the SYMAPPMON server. ■ SYMAPPMON server might be unreachable.	You may want to verify the following: ■ Appliance is provisioned to SYMAPPMON server. ■ There are no connectivity issues between the appliance and the SYMAPPMON server.
Notification interval cannot be blank or 0 if SNMP or SMTP server with hardware administrator email is configured. Enter notification interval in multiples of 15.	You may encounter this message when you have left the **Notification Interval** field of the **Alert Configuration** tab blank or entered 0 (zero) after enabling SNMP details or entered SMTP details and now you try to save the changes on the **Settings > Notifications** tab.	Verify whether you have entered a value for the **Notification Interval** field of the **Alert Configuration** tab and that this value is in multiples of 15 (and not zero).
Proxy server and proxy port fields are required.	This message is displayed when you have selected the **Enable Proxy Server** check box, but left the required proxy server details blank.	Ensure that you have entered correct values, which are required to set up a proxy server.
Proxy port value should be an integer in the range of 1-65535	This message is displayed when an invalid value is entered for the port number for the proxy server.	Ensure that you have entered correct and valid value for the port number of the proxy server.
Invalid value entered for proxy server	This message is displayed when you have entered invalid values while configuring the proxy server, such as an invalid IPv4 or an IPv6 address.	Ensure that the values, which you have provided for configuring the proxy server, are correct and valid.
Please enter the user name for proxy server	This message is displayed when a password for the proxy server has been entered, but a user name for the proxy server has not been entered.	Enter valid user name and password for the proxy server.

Table 11-12 Settings > Notification *(continued)*

Error messages	Explanation	Recommended action
Failed to send a test email. Please verify that the SMTP server and the email configuration are correct for this appliance. Do you want to continue?	You may encounter this error when: A test email cannot be sent using the **SMTP Server Configuration** or the SMTP server is temporarily unreachable; although the configuration details that are entered for the SMTP server are correct.	Verify the configuration setting for the SMTP server and try sending a test email.

lists all the error messages, displayed on the **Settings > Network** tab.

Table 11-13 Settings > Network

Error messages	Explanation	Recommended action
Failed to create VLAN. <vlan_id> already exists.	This message is displayed when you try to tag a VLAN with a *vlan_id* that already exists.	VLAN ID is a unique identifier. Therefore, provide a different *vlan_id* to tag the VLAN.
Cannot tag VLAN <vlan_id>. The specified IP address <ip> is already configured. Specify an IP address that is not in use.	This message is displayed when you try to tag VLAN with an IP address that is already configured for another interface.	Specify an IP address that is not used by other interfaces.
Invalid netmask <subnet_mask>.	This message is displayed if you enter an invalid subnet mask.	Enter an valid subnet mask.
Invalid IP address. IP address <ip> is in use. Use Main->Network->Show Status to verify.	This message is displayed when you attempt to create a bond with an IP address that is configured for another interface.	Specify an IP address that is not used by other interfaces.
Failed to update routing information. The network gateway is not reachable with the route information that you have provided. The gateway might not be reachable because it is not covered under a subnet mask that can be reached through your network interface settings.	This message is displayed if you enter gateway information that is in another domain.	Enter gateway information that corresponds to your domain.
Error while retrieving Fibre Transport Settings	The current Fibre Transport Settings for the appliance cannot be displayed.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.

Table 11-13 Settings > Network *(continued)*

Error messages	Explanation	Recommended action
Error in enabling/disabling FT flag configuration	The Fibre Transport settings cannot be enabled for your appliance.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Error in updating SAN client flag configuration	The SAN Client Fibre Transport cannot be enabled for your appliance.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Load failed.	The current Fibre Transport Settings for the appliance cannot be displayed.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Error updating network optimization status.	This message appears due to an internal system error.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Error while retrieving WAN optimization setting.	This message appears due to an internal system error.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.

Table 11-14 lists all the error messages, displayed on the **Settings > Date and Time** tab.

Table 11-14 Settings > Date and Time

Error messages	Explanation	Recommended action
Unable to save the date and time settings.	This error can appear due to the following reasons: ■ An internal system error has occurred. ■ The connection to the NTP server cannot be established. ■ The connection to the web server is not established.	Please ensure that the NTP server and the web server are connected. If the problem persists, collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Unable to save the NTP server settings. Check if the specified NTP server exists.	This error appears if the NTP server IP details are incorrect or the NTP server is non-existent.	Please ensure that the provided IP address for the NTP server is valid. Also ensure that the NTP server is connected to the appliance

Table 11-15 lists all the error messages, displayed on the **Settings > Authentication** tab.

Table 11-15 Settings > Authentication

Error messages	Explanation	Recommended action
Could not disable the current LDAP configuration. Could not enable the current LDAP configuration.	The configured LDAP server cannot be disabled. This error can occur in case the LDAP server is not responsive. The connection to the web server is not established.	Collect the web GUI and Perl logs all using the `DataCollect` command and then contact Symantec Technical Support.
Could not unconfigure the current LDAP configuration.	The configured LDAP server cannot be unconfigured.	Please use either of the following actions to resolve the error: ■ Verify that the LDAP server is responsive. ■ Verify that you have the correct authorization to unconfigure the LDAP server. ■ Verify the connectivity to the LDAP server using the NetBackup Appliance Shell Menu.
Error while configuring LDAP.	This error can be displayed due to the following reasons: ■ The provided details for the LDAP server are incorrect. ■ The LDAP server is not responsive.	Verify the configuration details of the LDAP server to be configured.
Error while setting server name.	The provided LDAP server name cannot be configured.	Verify that the provided server name for the LDAP server is correct.
Error while setting base DN.	The provided base directory name for the LDAP server could not be configured.	Verify that the provided base directory name is correct and do not contain any typos or spelling errors. Verify that the base directory name matches the Active Directory or LDAP server settings.
Error while setting bind DN.	The provided bind directory name for the LDAP server could not be configured.	Verify that the provided bind directory name is correct. Verify that the bind directory name matches the Active Directory or LDAP server settings.
Error while setting password.	The provided password to access the LDAP server is incorrect.	Enter a valid password to configure the LDAP server.

Table 11-15 Settings > Authentication *(continued)*

Error messages	Explanation	Recommended action
Error while setting common user name.	The user name of an existing LDAP user, provided to access the LDAP server, is incorrect.	Enter a valid user name to configure the LDAP server.
Error while setting common group name.	The group name of an existing LDAP group, provided to access the LDAP server, is incorrect.	Enter a valid group name to configure the LDAP server.
Error while setting SSL.	This error can be displayed due to the following reasons: ■ The SSL certificate has got corrupted. ■ The path to the SSL certificate is incorrect. ■ The SSL certificate is outdated.	Please use either of the following actions to resolve the error: ■ Please ensure that the SSL certificate is not corrupt. ■ Please ensure the path to the SSL certificate is correct. ■ Please ensure that the SSL certificate is up-to-date.
Error in exporting the LDAP configuration settings.	This error can be displayed due to the following reasons: ■ The path to save the generated XML file is incorrect. ■ The XML file could not be generated.	Please refresh the page and if the problem persists contact Symantec Technical Support.
Error in saving user.	The appliance cannot save the newly added user.	Please ensure that you have the appropriate permissions to perform the task. Please refresh the page and try again. If the problem persists contact Symantec Technical Support.
Error in saving group.	The appliance cannot save the newly added user group.	Please ensure that you have the appropriate permissions to perform the task. Please refresh the page and try again. If the problem persists contact Symantec Technical Support.
Error in authorizing.	The appliance cannot grant administrative permissions to the selected user.	Please ensure that you have the appropriate permissions to perform the task. Please refresh the page and try again. If the problem persists contact Symantec Technical Support.

Table 11-15 Settings > Authentication *(continued)*

Error messages	Explanation	Recommended action
Error in unauthorizing.	The appliance cannot revoke administrative permissions to the selected user.	Please ensure that you have the appropriate permissions to perform the task. Please refresh the page and try again. If the problem persists contact Symantec Technical Support.
Error in deleting user.	The appliance cannot delete the added user.	Please ensure that you have the appropriate permissions to perform the task. Please refresh the page and try again. If the problem persists contact Symantec Technical Support.
Error in deleting user group.	The appliance cannot delete the added user group.	Please ensure that you have the appropriate permissions to perform the task. Please refresh the page and try again. If the problem persists contact Symantec Technical Support.
Login failure due to an unrecognized or invalid user	If the user is removed from the LDAP directory (and not removed from appliance allowed to log in list), though the user is listed as LDAP authorized user, the user will not be able to log in. So, these users poses no security threat.	In the case, an LDAP user that is configured to use the Appliance need to be deleted or removed from the LDAP directory, then the user needs to be first removed from the appliance. Otherwise, we will not be able to remove that user from the appliance user list.
The server configuration is unsuccessful. View error messages for more information.	This error can appear due to multiple reasons. Please view the complete error message to obtain the resolution.	Please refresh the page and if the problem persists contact Symantec Technical Support.

Table 11-16 lists all the error messages, displayed on the **Settings > Password** tab.

Table 11-16 Settings > Password

Error messages	Explanation	Recommended action
Supplied password does not meet the required pattern!	The new password does not contain all the required parameters.	Enter a new password. Passwords with seven characters must include all of the following requirements while longer passwords must include at least three: ■ One uppercase letter. ■ One lowercase letter. ■ One number (0-9) ■ One special character (@#$%%^&*(){}[].) 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.
Failed to reset the password, please try again. Click ? for more details. If the error persists, contact Symantec Technical Support.	The password cannot be reset due to a technical error.	Please contact Symantec Support.

Table 11-17 lists the error messages that are common to all the tabs on the NetBackup Appliance Web Console.

Table 11-17 Common error messages that can appear on the NetBackup Appliance Web Console

Error	Explanation	Recommended action
An unknown error has occurred. Please contact Symantec Support to resolve the issue. To continue with the operations, click any tab.	This is generic error and may appear if the web server is not responsive.	Please restart your web server and try again.
	This icon is displayed next to the field that does not display the updated information. This happens when the entered value has not got updated in the NetBackup Appliance Directory. That is the new value does not match the data store.	Please enter the appropriate value and save again. Please ensure that the connection to the NetBackup Appliance Directory is not down.

See "NetBackup status codes applicable for NetBackup Appliance" on page 210.

See "Error messages displayed on the NetBackup Appliance Shell Menu" on page 203.

See "Error messages displayed during initial configuration" on page 182.

Error messages displayed on the NetBackup Appliance Shell Menu

Table 11-18 lists some of the common error messages that you may come across while working from the NetBackup Appliance Shell Menu:

Table 11-18 Common error messages in NetBackup Appliance Shell Menu

Error messages	Explanation / Recommended action
The disk pool name is missing for the AdvancedDisk storage partition. Please add the disk pool name and try again. If the problem persists, refer to the troubleshooting guide.	If disk pool for a storage partition during role configuration /post configuration is missing, it fails to configure storage and also fails role configuration. Add the disk pool name and try again, if the problem persists, contact Symantec Support.
The storage unit name is missing for the AdvancedDisk storage partition. Please add the storage unit name and try again. If the problem persists, refer to the troubleshooting guide.	If storage unit name for a storage partition during role configuration /post configuration is missing, it fails to configure storage and also fails role configuration. Add the storage unit name and try again, if the problem persists, contact Symantec Support.
Failed to save the disk pool information for the AdvancedDisk storage partition in the NetBackup Appliance Directory, please try again. If the problem persists, refer to the troubleshooting guide.	If NetBackup Appliance Directory is not responsive, the disk pool cannot be saved in Appliance Directory. As a result the storage configuration and role configuration fails. Ensure that the NetBackup Appliance Directory is responsive and retry to save the storage unit in the Appliance Directory.
Failed to save the storage unit information for the AdvancedDisk storage partition in the NetBackup Appliance Directory, please try again. If the problem persists, refer to the troubleshooting guide.	If NetBackup Appliance Directory is not responsive, the storage unit cannot be saved in Appliance Directory. As a result the storage configuration and role configuration fails. Ensure that the NetBackup Appliance Directory is responsive and retry to save the storage unit in the Appliance Directory.
Unable to ping master server	'Make sure that you configured your appliance media server network properly. You should ensure that the appliance has a proper IP address, network gateway, and Netmask. Ensure that the DNS server and DNS search domains are defined or there are appropriate entries in the /etc/hosts file.

Table 11-18 Common error messages in NetBackup Appliance Shell Menu *(continued)*

Error messages	Explanation / Recommended action
Master server denied access to this appliance	Verify that you added the appliance host name to the master server's known server list. You can use the NetBackup Administration Console to add the appliance to the master server"s known server list. See the *NetBackup Administrator's Guide* for instructions.
Unable to connect to master server	Make sure that the NetBackup services are up and running on the master server. Also verify that there are no firewalls blocking accesses to the master server services. See the *NetBackup Administrator's Guide* for more information on how to allow access through firewalls.
Failed to get NetBackup version	Make sure that the NetBackup services are up and running on the appliance. If you encounter this issue, restart the NetBackup services.
Master server version is lower than the media server version	If the master server is a standard non-appliance master server, upgrade the NetBackup software on the master server to a version that is equal to or higher than the current media server version. Upgrade the master server if it is an appliance with the appliance version that contains NetBackup release equal to or higher than the NetBackup release on the media server.
Failed to access disk storage	This problem can arise due to multiple issues. For example, if the disks are offline or the disk volume is disabled. In these scenarios: ■ Collect `DataCollect` log and the output of `vxprint-hqt` command. ■ Check `/log/app_vxul/409-9-*.log` for the actual disk group and volume-related errors.
Failed to resize volumes	First, attempt to change value of the required partition size or the percentage. Second, enter a value that is in a different format than what was originally used. For example, enter an absolute size if a percentage was used first. Finally, restart the appliance host. Check `/var/log/sf.log` for volume (VxVM) error messages.
Resize hangs for a long period of time	Then log out, and then log back into the appliance user interface and attempt a resize operation again.
Failed license check for AdvancedDisk storage	Make sure that a valid license for the NetBackup **Flexible Disk Option** is installed on the media server.

Table 11-18 Common error messages in NetBackup Appliance Shell Menu *(continued)*

Error messages	Explanation / Recommended action
Failed license check for Deduplication storage	Make sure that a valid license for NetBackup **Deduplication Option** is installed on the media server
Failed to create Deduplication storage unit	Check if the storage unit or the corresponding disk volume already exists on the media server. If they do exist, verify if the storage unit or the corresponding disk volume is currently used. If the storage is redundant only then use the NetBackup Administration Console or the `nbdecommission` utility to delete them. These tools are available on the NetBackup master server. Check the NetBackup Appliance VxUL (unified) logs with the `Support > Logs > VxLogView Module ALL` command for more precise error information.

Table 11-19 lists error messages that are specific to `Manage > Software view` commands.

Table 11-19 Manage > Software view

Error message	Explanation	Recommended action
Failed to read the update configuration for *<RPM name>*.	There are some errors in rpm patch.	Please contact Symantec support for help.
The NetBackup appliance version is already at *<version number>*.	The current appliance version is the same as the version in the patch. The appliance has stopped installing the patch.	Please check if this patch has been installed, if yes then identify the correct patch to install on the appliance.
Cannot install the software update. The software update version is *<version number>* and the appliance version is *<version number>*.	The current version installed on the appliance is higher than the version of the patch you are trying to install.	Please identify and try to install the correct patch on the appliance.
The installation failed because the patch does not exist or you did not run the `List downloaded` command to check for the downloaded patch.	The installation has failed as the patch you are trying to download does not exist or is not up-to-date.	Please identify and try to install the correct patch on the appliance. Run the `List downloaded` command to check for the downloaded patch and install the correct patch.
An upgrade process is already running on this appliance.	Unable to get the upgrade lock, which means another upgrade is running on the appliance.	Please check if there is another instance of the upgrade process running on the appliance.

Table 11-19 Manage > Software view *(continued)*

Error message	Explanation	Recommended action
Unknown error. Please contact Symantec Technical Support!	The source of the error cannot be found.	Please contact Symantec Technical Support.
Software update, *<rpm>* is already installed on compute node, *<node name>*.	The `rpm` (SUSE installer package) is already installed on the appliance.	Please check if the `rpm` you are trying to install has already been installed on the appliance.
Unable to verify that software update, *<rpm>*, is installed	Unable to check weather the `rpm` (SUSE installer package) you are trying to install is already present on the appliance.	Please check if there are some system errors.
Failed to get NetBackup version on Master *<master server name>*.	Failed to get the version info on the master server.	Please check if there are some network problems, or the master server was turn off un-expectedly.
Version of NetBackup on Master *<master server name>* is *<version number>*, should be *<version number>*	The version number on the master does not match the requirements from the patch.	Please ensure that the NBU version is installed on the master server, or it's not the proper patch to install.
Invalid Appliance mode.	The appliance mode in `bp.conf` file is not correct.	Please check the appliance mode in bp.conf and contact Symantec Support.
Please provide a valid EEB name.	This error message is only for the rollback of EEB. The EEB name is not valid.	Please check that the EEB name you have used.
Patch *<rpm name>* signature check failed.	Signature error found in the `rpm` (SUSE installer package) .	Please check if the `md5` number of the `rpm` (SUSE installer package) is correct. It's commended to re-download the `rpm`.
NetBackup jobs are currently in progress. Stop all NetBackup jobs and then try the upgrade again.	The upgrade requires stopping all NetBackup jobs.	Please stop the NetBackup jobs, before upgrading the appliance software.
Unable to gather backup job summary information. This may indicate that some processes are not running and that you should restart your appliance.	The upgrade process checks to see if there are any active NetBackup jobs. The upgrade process only proceeds if it is determined no active jobs are detected. If the backup job summary cannot be complied it means that some of the process are not running.	Please check if the NetBackup services are running correctly.

Table 11-19 Manage > Software view *(continued)*

Error message	Explanation	Recommended action
The software upgrade process failed. The appliance is rolling back to a pre-upgrade state using the Pre-upgrade checkpoint!	The software upgrade process has failed and the appliance will automatically roll back to pre-upgrade state.	Please wait till the rollback is complete.
Automatic rollback failed. Please contact Symantec Technical Support!	When the software upgrade process fails, the appliance will automatically roll back to pre-upgrade state. However, due to an unexpected reason the automatic rollback has failed.	Please contact Symantec support to take a look at the checkpoint log.
Failed to create the pre-upgrade checkpoint, please resolve this issue first!	The pre-upgrade checkpoint cannot be created due to an unexpected error.	Please contact Symantec support to take a look at the checkpoint log.
Self-Test failed, please resolve this issue first!	The self-test has failed due to an unexpected error.	Please run the `Support > Test software` command to see the detailed error message.

Table 11-20 lists error messages that are specific to `Manage > Appliance Restore` commands.

Table 11-20 Manage > Appliance Restore view

Error message	Explanation	Recommended action
Appliance Checkpoint creation failed. Retry again once errors are resolved.	This can be caused by insufficient disk space.	Look for additional information listed above the error message. Retry the operation. Cleanup is done in case of such a failure, which could free up the space.
Rollback validation failed. Unable to continue with rollback to Appliance Checkpoint. Please correct the errors above and try again.	Secured network communication has issues.	Look for additional information listed above the error message. Try to correct the error and retry the operation.
Rollback to Appliance Checkpoint <checkpoint_name> failed. Please proceed with the suggested system reboot. Some rollback to Appliance Checkpoint errors can be resolved by rebooting the appliance(s).	System resources could be busy.	Restart the appliance and retry the rollback operation.

Table 11-20 Manage > Appliance Restore view *(continued)*

Error message	Explanation	Recommended action
Factory reset validation failed. Unable to continue. Please fix the errors above and try again.	Secured network communication has issues.	Look for additional information listed above the error message. Try to correct and retry the operation.
Reset of the appliance to a Factory State failed. Please proceed with the suggested system reboot. Some reset failures can be resolved by rebooting the appliance(s).	System resources could be busy.	Restart the appliance and retry factory reset.

Table 11-21 lists error messages that are specific to `Main_Menu > Network` commands.

Table 11-21 Main_Menu > Network view

Error message	Explanation	Recommended action
Failed to create VLAN <vlan_id>. Ether device {interface} does not exist.	This error occurs when you enter an enter invalid interface.	Provide a valid numeric identifier for the <vlan_id>.
Failed to create VLAN <vlan12>. Interface <eth4> is configured with IP address 10.10.10.10. Cannot create a VLAN device over a configured interface. Unconfigure the IP before adding a VLAN device.	This error occurs when you try to tag a VLAN over an interface that is configured with an IP address .	Enter an IP address that is not configured to another interface. Alternatively, you may also unconfigure the existing IP address for the given interface and then tag VLAN.
Failed to create VLAN <vlan12>. Interface <eth2> is not cabled.	This error occurs when you try to tag a VLAN over an unplugged interface.	Ensure that the interface that is selected for tagging VLAN is plugged.
Failed to create VLAN <vlan12>. Interface <eth4> is slave to bond <bond0> .Cannot create a VLAN over a bonded interface.	This error is displayed if you try to tag a VLAN over a bonded interface.	Ensure that the interfaces that is selected for VLAN tagging is not already a part of a bond.
Interface {interface} does not exist.	This error occurs if you enter an invalid interface name for creating bond using the `LinkAggregation` command.	Enter a valid interface name for creating a bond.
None of the given interfaces <interface(s)> are cabled. Make sure at least one interface is cabled.	This error is displayed if any of the interfaces that participate in creating bond are unplugged.	Ensure that at least one of the interfaces that participates in bond creation is plugged.

Table 11-21 Main_Menu > Network view *(continued)*

Error message	Explanation	Recommended action
Cannot enable bonding for a single interface. To enable bonding, provide details for more than one interface.	This error is displayed if you provide a information for a single interface for creating a bond.	To create a bond, provide interface details for more than one interface.
Interfaces <interface(s)> are not of same type and speed.	This error occurs when you try to create a bond with interfaces that have different port speeds.	Ensure that the interface that are selected for creating a bond have same port speed.
Interface <interface> is part of a bond.	This error occurs when you provide details of an interface that is already a part of another bond.	Ensure that the interfaces that is selected for the operation is not already a part of a bond.
Cannot enable bonding for duplicate interface(s), <eth4> To enable bonding, provide details for different interface(s)	This error is displayed if you enter duplicate interface names while creating a bond. For example, <eth3>, <eth4>, <eth4>	Do not enter duplicate interfaces names while creating a bond.
Interface <bond0> is a bonded interface. Cannot use bonded interfaces in bond.	This error is displayed if you try to create a bond over using an interface that is already a part of another bond.	Ensure that the interfaces that is selected for creating a bond is not a part of an existing bond.
Cannot use interface <eth4> in a bond. Interface is in use by VLAN <vlan12>.	This error occurs when you try to create a bond using an interface over which a VLAN is tagged.	Enter details for an interface that does not have any VLAN(s) tagged over it.
More than one interfaces (eth4:10.10.10.10 eth5:10.10.10.11) are configured. Use Main->Network->Unconfigure to remove one.	This error occurs when you try to create a bond with interfaces for which have IP addresses are configured.	To create a bond between interfaces, IP address should not be configured for more than one interface.

See “NetBackup status codes applicable for NetBackup Appliance” on page 210.

See “Error messages displayed on the NetBackup Appliance Shell Menu” on page 203.

See “Error messages displayed during initial configuration” on page 182.

NetBackup status codes applicable for NetBackup Appliance

This section lists the NetBackup error that can occur while, working with a NetBackup Appliance. It helps you to resolve the issues based on the corresponding error messages:

Table 11-22 NetBackup status codes

NetBackup status code	Message	Explanation
13	file read failed	A read of a file or socket failed.
48	client host name cannot be found	The system function `gethostbyname()` failed to find the client's host name.
83	media open error	The tape manager (`bptm`) or disk manager (`bpdm`) did not open the device or file that the backup or restore must use.
84	media write error	The system's device driver returned an I/O error while NetBackup wrote to removable media or a disk file.
89	problems encountered during setup of shared memory	The NetBackup processes use shared memory for some operations. This status is returned when an error is encountered in the initialization of the shared memory by the operating system's APIs.
213	no storage units available for use	The NetBackup resource broker (`nbrb`) did not find any storage units available for use. Either all storage units are unavailable or all storage units are configured for On demand only. In addition, the policy and schedule does not require a specific storage unit.
242	operation would cause an illegal duplication	If the request is processed, it causes a duplicate entry (for example, in the catalog or the configuration database). A duplicate catalog entry is usually due to a mistake in the specification of media IDs for NetBackup catalog backups.
1500	Invalid storage unit	The storage unit or storage unit group specified for one or more destinations in storage lifecycle policy is not valid.

For more information on NetBackup status codes, refer to *Symantec NetBackup™ Status Codes Reference Guide*.

See “NetBackup status codes applicable for NetBackup Appliance” on page 210.

See “Error messages displayed on the NetBackup Appliance Shell Menu” on page 203.

See “Error messages displayed on the NetBackup Appliance Web Console” on page 183.

See “Error messages displayed during initial configuration” on page 182.

Index

Symbols

52xx master server appliance
- initial configuration from NetBackup Appliance Shell Menu 149
- reconfigure from USB and NetBackup Appliance Shell Menu 149

52xx media server appliance
- reconfigure from USB and NetBackup Appliance Shell Menu 157

A

appliance
- disk drive status LED
  - troubleshooting 113
- power supply
  - troubleshooting 115
- troubleshooting
  - does not turn on 111

Appliance Diagnostics Center 35

appliance media server
- configure master server to communicate with 155

appliance serial number 19

available configurations
- NetBackup 5230 appliance 48

B

best practice
- notification settings 27

best practices
- BMR 30
- delete user 32
- HBA card verification 25
- IPMI 27
- password 28
- serial number 19
- troubleshooting 17

bezel 121
- NetBackup 5030 appliance 62
- NetBackup 5230 appliance 45

boot order change
- resolve 82

C

cables 63

Check Disk Configuration wizard 35

Collect Log files wizard 35

collect logs
- commands 70
- datacollect 72
- log file location 70
- NetBackup-Java applications 75
- types of logs 70

configure master server
- to communicate with appliance media server 155

CPU
- alert 118

current
- alert 118

D

datacollect
- device logs 72

disable security warnings
- on Mozilla 24

disk drive
- LEDs
  - NetBackup 5220 appliance 127

disk drive status LED
- appliance
  - troubleshooting 113

disk drive, storage
- NetBackup 5220 appliance
  - removing and replacing 127

E

environmental
- specifications
  - NetBackup 5220 appliance 54

environmental specifications
NetBackup 5230 appliance 44

F

factory reset
discard RAID preserved cache 101
troubleshooting 100
failure to boot
embedded RAID controller 106
fan
specifications
NetBackup 5220 appliance 54
NetBackup 5230 appliance 45
fibre channel
HBA card verification 25
Fibre Channel card
NetBackup 5230 appliance 48
front panel
hot spare drive
NetBackup 5220 appliance 55
local control panel
NetBackup 5220 appliance 55
NetBackup 5220 appliance 55
system drive
NetBackup 5220 appliance 55
fsck test failure 107

H

hot spare drive
front panel
NetBackup 5220 appliance 55
hot swap
about 120
humidity
specifications
NetBackup 5220 appliance 54
NetBackup 5230 appliance 44

I

initial configuration of 52xx master server appliance
from NetBackup Appliance Shell Menu 149
intial configuration failure
NetBackup Appliance Directory 87
IPv4 and IPv6 support 29
IPv6 networks
troubleshooting 102

L

LED
drive slots
appliance 61
system status
troubleshooting 118
LEDs
NetBackup 5030 appliance
control panel 61
NetBackup 5220 appliance
local control panel 56
local control panel
front panel
NetBackup 5220 appliance 55
NetBackup 5220 appliance 56
log files
enabling and disabling VxMS logging 76
introduction 64

M

manage
appliance restore 170–171, 173
matched pairs
NetBackup appliance and Symantec Storage Shelf 79
media server
configuration failure 91, 96
factory reset failure 105
memory
alert 118
specifications
NetBackup 5220 appliance 54
NetBackup 5230 appliance 45
Microsoft Internet Explorer 22
Mozilla Firefox 22

N

NetBackup 5030 appliance
bezel 62
front panel
LEDs 61
NetBackup 5220 appliance
disk drive
LEDs 127
disk drive, storage
removing and replacing 127
front panel 55
I/O expansion module 59

NetBackup 5220 appliance *(continued)*
local control panel 56
power supply
removing and replacing 128
power supply module 59
rear panel 59
remote management port 59
NetBackup 5230 appliance
available configurations 48
bezel 45
Fibre Channel card 48
PCIe slot numbers 48
power supply 48
rear panel 48
SAS_IN port 48
specifications
environmental 44
NetBackup appliance
about troubleshooting 13
appliance factory reset 173
appliance rollback validation 171
rollback appliance 170
NetBackup appliance and Symantec Storage Shelf
matched pairs 79
NetBackup Appliance Directory down
intial configuration failure 87
NetBackup support utilities
NBDNA 40
nbsu 40
NIC port
NetBackup 5220 appliance
private network 59
service network 59

O

operating temperature
NetBackup 5230 appliance 44
specifications
NetBackup 5220 appliance 54
over temperature 118
troubleshooting 116

P

PCIe slot numbers
NetBackup 5230 appliance 48
Perform a hardware health check wizard 35
physical dimensions
specifications
NetBackup 5220 appliance 53
power supply
alert 118
appliance
troubleshooting 115
NetBackup 5220 appliance
removing and replacing 128
NetBackup 5230 appliance 48
protection mode 116
specifications
NetBackup 5220 appliance 54
NetBackup 5230 appliance 45
power supply module
NetBackup 5220 appliance 59
protection mode
explained 116

R

rack mounting 63
rear panel
NetBackup 5220 appliance 59
NetBackup 5230 appliance 48
reconfiguration of 52xx master server appliance
from USB and NetBackup Appliance Shell Menu 149
reconfiguration of 52xx media server appliance
from USB and NetBackup Appliance Shell Menu 157
recording information 15
reinstallation
on 5220 104
remote management port
NetBackup 5220 appliance 59
resolve
boot order change problem 82

S

SAS_IN port
NetBackup 5230 appliance 48
self-repair wizards 35
shock
specifications
NetBackup 5220 appliance 54
NetBackup 5230 appliance 44

shutdown
    system-induced
        troubleshooting 116
specifications
    environmental
        NetBackup 5220 appliance 54
    fan
        NetBackup 5220 appliance 54
        NetBackup 5230 appliance 45
    memory
        NetBackup 5220 appliance 54
        NetBackup 5230 appliance 45
    operating temperature
        NetBackup 5220 appliance 54
        NetBackup 5230 appliance 44
    physical dimensions
        NetBackup 5220 appliance 53
        NetBackup 5230 appliance 44
    power supply
        NetBackup 5220 appliance 54
        NetBackup 5230 appliance 45
Symantec Product Authentication Service (AT) Server
  parameters 42
system drive
    front panel
        NetBackup 5220 appliance 55
system status
    LED
        state 118
        troubleshooting 118

T

TECH182738 31
TECH187722 106
Test and diagnose network issues wizard 35
Test Call Home functionality wizard 35
troubleshooting
    about factory reset 100
    and configuration 78
    configuration 81
    kernel coredump issues 101
    NetBackup appliance 13
    setup 78
    target mode port 92
Troubleshooting guide
    about the guide 11
    contacting support 12
    intended audience 12

V

VxAT properties 42
VxMS logging
    enabling and disabling 76
vxprint
    column description 31

W

web browser
    support 22
weight
    NetBackup 5230 appliance 44