Veritas NetBackup™ Appliance Troubleshooting Guide

Release 3.0

NetBackup 52xx and 5330

VERITAS™

Veritas NetBackup™ Appliance Troubleshooting Guide

Release 3.0

Legal Notice

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

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

.

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

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

APPL.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1

About using the Troubleshooting Guide

This chapter includes the following topics:

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

About this guide

This guide provides the information to troubleshoot the Veritas NetBackup Appliances with the appliance software version 3.0. 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 troubleshoot the 52xx and 5330 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 NetBackup Appliance Documentation web page 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 Technical Support

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

www.veritas.com/support

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

- Locate and note the serial number of your appliance, storage devices, and switches as applicable.
  See "Determining the NetBackup Appliance serial number" on page 13.
- 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 101.
  See "Error messages displayed on the NetBackup Appliance Web Console" on page 103.
  See "Error messages displayed on the NetBackup Appliance Shell Menu" on page 121.
  See "NetBackup status codes applicable for NetBackup Appliance" on page 130.
- Gather device logs using the `Datacollect` command.
  See "Gathering device logs with the DataCollect command" on page 40.
- 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 19.

See "About best practices" on page 11.

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 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 Appliance. 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**. See "Error messages displayed during initial configuration" on page 101. See "Error messages displayed on the NetBackup Appliance Web Console" on page 103. See "Error messages displayed on the NetBackup Appliance Shell Menu" on page 121. ■ 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 "About NetBackup Appliance log files" on page 34. ■ 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 *NetBackup Appliance Hardware Installation Guides*

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 “About NetBackup Appliance log files” on page 34.

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 Appliance issue, you can find additional troubleshooting information from the NetBackup Appliance page on the Technical Support website. 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 130. For more information, refer to the *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 "About NetBackup support utilities" on page 31. See the *NetBackup Troubleshooting Guide* for additional information specific to NetBackup.
Step 5	Complete a problem report for Technical Support	If you can identify the logs that can help resolve the issue, collect the appropriate logs. If you cannot identify the required logs for resolving the problem, contact Technical Support to get advice on which logs to collect. If your troubleshooting is unsuccessful, prepare to contact Technical Support by filling out a problem report. See "About contacting Technical Support" on page 7. See "About NetBackup Appliance log files" on page 34.
Step 6	Contact Technical Support	The Veritas Technical Support website has a wealth of information that can help you solve NetBackup Appliance problems. Access Technical Support at the following URL: www.veritas.com/support See "About contacting Technical Support" on page 7.

See "Enabling and disabling VxMS logging" on page 42.

Best practices

This chapter includes the following topics:

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 "Determining the NetBackup Appliance serial number" on page 13.

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

Section	Description	Link
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 18.
About Notification settings	This section provides the importance for enabling the Notification and re-directs you to the MyAppliance portal to register your appliance and edit registration details.	See “About Notification settings” on page 19.
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 IPMI configuration” on page 20.
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 22.
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 23.
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 24.
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 24.

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 45.

Determining the NetBackup Appliance serial number

You need to note and refer to the NetBackup Appliance serial number when you report an issue to Veritas Technical Support.

You can use either of the following options to determine the NetBackup Appliance serial number and storage shelf chassis numbers.

Table 2-2 Options for determining the NetBackup Appliance system serial numbers and chassis numbers

To use this option:	See:
NetBackup Appliance Web Console	Determining the serial number of the NetBackup Appliance using the Web Console
NetBackup Appliance Shell Menu	Determining the serial number for a NetBackup Appliance using the Shell Menu
	Determining the serial number and chassis number of a NetBackup 5330 Primary Storage Shelf using the Shell Menu
	Determining the serial number and chassis number for a NetBackup 5330 Expansion Storage Shelf using the Shell Menu

Determining the serial number of the NetBackup Appliance using the Web Console

Use the following procedure to determine the serial number of the NetBackup Appliance by using the NetBackup Appliance Web Console.

To use the NetBackup Appliance Web Console to determine the NetBackup Appliance serial number:

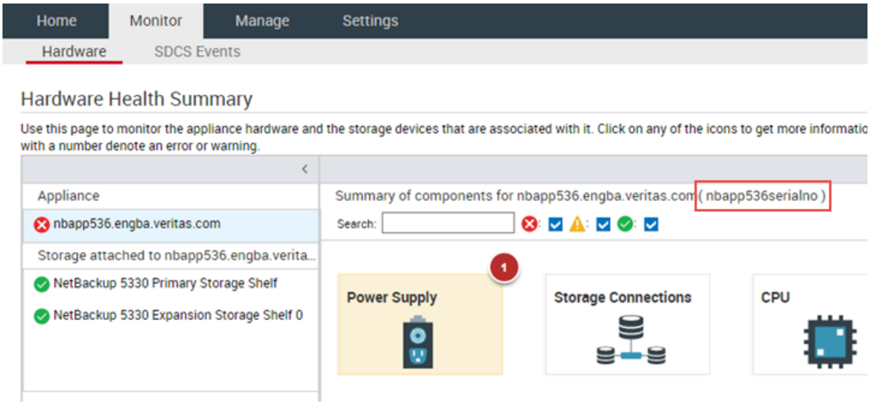
1 Log on to the NetBackup Appliance Web Console using your user credentials.

2 Select **Monitor > Hardware**.

The **Hardware Health Summary** page appears.

3 From the left-pane, click the appliance name.

The serial number is located in-line to the right of the name of the NetBackup 5330 server in the NetBackup Appliance Web Console.



Hardware Health Summary

Use this page to monitor the appliance hardware and the storage devices that are associated with it. Click on any of the icons to get more informatic
with a number denote an error or warning.

Appliance

nbapp536.engba.veritas.com

Storage attached to nbapp536.engba.verita...

NetBackup 5330 Primary Storage Shelf

NetBackup 5330 Expansion Storage Shelf 0

Summary of components for nbapp536.engba.veritas.com (nbapp536serialno)

Search:

Note: On the NetBackup 5330 Appliance, you can also determine the serial number of each attached storage shelf by clicking the name of the storage shelf in the left pane.

To determine the chassis number of a Primary Storage, use the NetBackup Appliance Shell Menu.

See Determining the serial number and chassis number of a NetBackup 5330 Primary Storage Shelf using the Shell Menu.

To determine the chassis number of an Expansion Storage Shelf, use the NetBackup Appliance Shell Menu.

See Determining the serial number and chassis number for a NetBackup 5330 Expansion Storage Shelf using the Shell Menu.

For more information, refer to the *NetBackup Appliance Administrator's Guide*.

Determining the serial number for a NetBackup Appliance using the Shell Menu

Use the following procedure to determine the serial number of a NetBackup Appliance or a NetBackup 5330 server using the NetBackup Appliance Shell Menu.

Determining the serial number and chassis number of a NetBackup 5330 Primary Storage Shelf using the Shell Menu

Use the following procedure to determine the serial number and chassis number of a NetBackup 5330 Primary Storage Shelf by using the NetBackup Appliance Shell Menu

To determine the serial number and the chassis number of a Primary Storage Shelf

1 Log on to the administrative NetBackup Appliance Shell Menu using your login credentials.

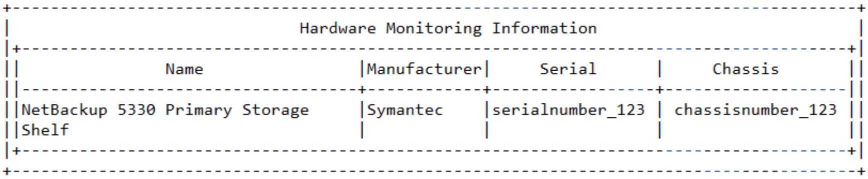
2 From the `Main_Menu>` command prompt, type `Monitor` and press **Enter**.

The command prompt changes to `Monitor>`.

3 Type the following command: `Hardware ShowHealth PrimaryShelf Product`, and then press **Enter**.

For example, `Monitor > Hardware ShowHeath PrimaryShelf Product`

The serial number and the chassis number for the Primary Storage Shelf appears, as seen in the following example:



```
+---------------------------------------------------------------------------------------+
|                              Hardware Monitoring Information                          |
|+-------------------------------------------------------------------------------------+|
||               Name               |Manufacturer|      Serial      |     Chassis      ||
||----------------------------------+------------+------------------+------------------||
||NetBackup 5330 Primary Storage    |Symantec    |serialnumber_123  | chassisnumber_123||
||Shelf                             |            |                  |                  ||
|+-------------------------------------------------------------------------------------+|
+---------------------------------------------------------------------------------------+
```

Determining the serial number and chassis number for a NetBackup 5330 Expansion Storage Shelf using the Shell Menu

Use the following procedure to locate the serial number and chassis number for a NetBackup 5330 Expansion Storage Shelf by using the NetBackup Appliance Shell Menu.

To determine the serial number and the chassis number for an Expansion Storage Shelf

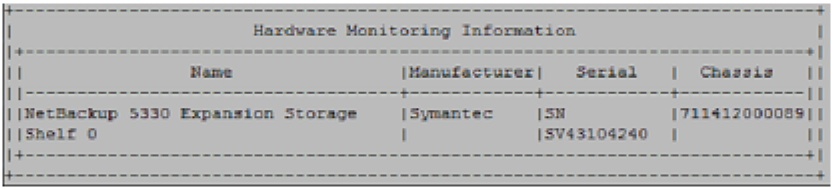
1. Log on to the administrative NetBackup Appliance Shell Menu using your logon credentials.
2. From the `Main_Menu>` prompt, type `Monitor` and press **Enter**.

   The command prompt changes to `Monitor>`.
3. Type the following command: `Hardware ShowHealth ExpansionShelf ExpansionShelfID Product`, and then press **Enter**.

   Note: *ExpansionShelfID* is the ID of the Expansion Storage Shelf. To check the *ExpansionShelfID*, use the `Main > Monitor > Hardware ShowComponents` command.

   For example, `Monitor > Hardware ShowHeath ExpansionShelf 0 Product`

   The serial number and the chassis number for the Expansion Storage Shelf appears, as seen in the following example:



```
+------------------------------------------------------------------------------+
|                        Hardware Monitoring Information                       |
|+----------------------------------------------------------------------------+|
||                 Name                 |Manufacturer|   Serial    |  Chassis  ||
||--------------------------------------+------------+-------------+-----------||
||NetBackup 5330 Expansion Storage      |Symantec    |SN           |711412000089||
||Shelf 0                               |            |SV43104240   |           ||
|+----------------------------------------------------------------------------+|
+------------------------------------------------------------------------------+
```

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

See “About best practices” on page 11.

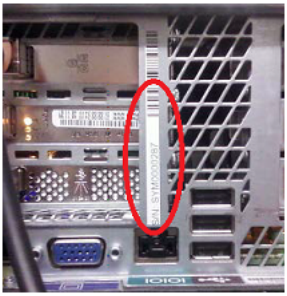
Locating hardware serial numbers

You can locate the serial numbers on the hardware to record the units that you need to install.

Serial number location for the NetBackup 5230 Appliance

The serial number of the appliance is located on a vertical bar on the rear panel.

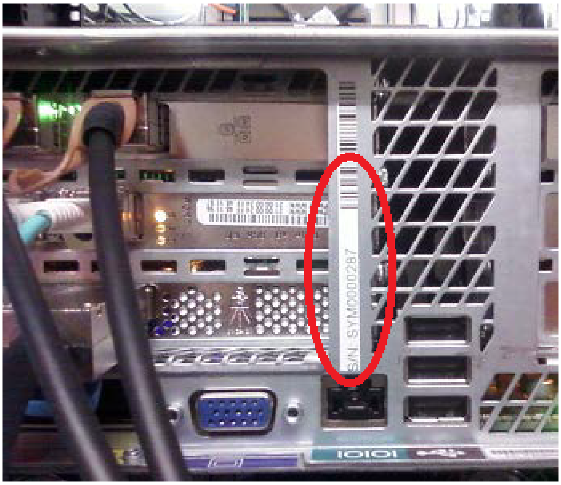
Figure 2-1 NetBackup 5230 Appliance serial number location



Serial number location for the NetBackup 5230, 5240, and 5330 appliances

On NetBackup 5230, 5240, and 5330 appliances, the serial number is located on a vertical bar on the rear panel.

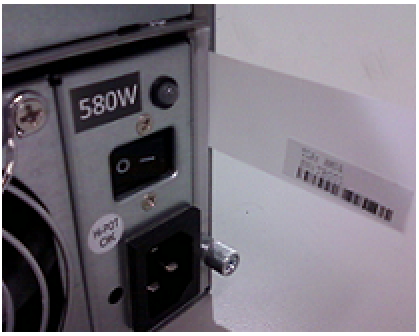
Figure 2-2 NetBackup 5230, 5240, and 5330 Appliance serial number locations



Serial number location for the 3U16 storage shelf

The serial number of the 3U16 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.

Figure 2-3 3U16 Storage Shelf serial number location



Note: Earlier models of the storage shelves 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.

About Fibre Channel HBA card configuration verification

The NetBackup Appliance server can be ordered with up to six Fibre Channel (FC) HBA cards already installed. Each card includes two standard Fibre Channel ports. You can configure a Fibre Channel HBA card on the appliance as Fibre Transport media server to use with SAN clients, or as a target host for optimized duplication and Auto Image Replication over FC.

Note: Veritas does not support reconfiguring the FC HBA cards in the appliance rear panel. Do not switch cards in different slots or install a used card from another appliance without contacting Veritas Technical Support.

After you configure the Fibre Channel HBA cards, you may want to verify that 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 VERITAS  10.182.0.209 FCPIPE  (NBU 50x0) 0x21000024ff232438
/dev/sg2 VERITAS  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 Veritas AutoSupport server periodically.

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 Veritas AutoSupport server for further analysis and support. These error logs are also stored on the appliance. You can access these logs from `/log/upload/<date>` folder. If there is a problem with a piece of hardware, you might want to contact Veritas 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 Veritas 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 3.0:

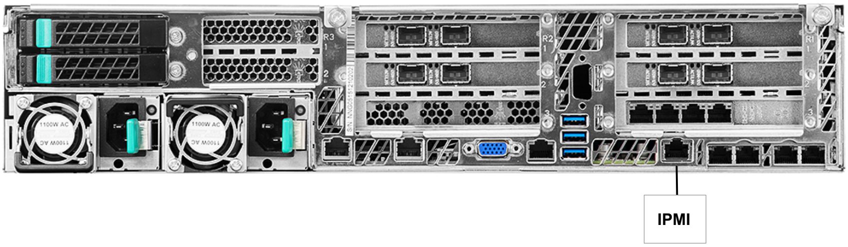
- ManageEngine™ SNMP server
- HP OpenView SNMP server

Also ensure that you register the appliance and your contact information on the MyAppliance portal. Registering your NetBackup Appliance helps to make sure that you are alerted to product updates and other important information about your appliance.

About IPMI configuration

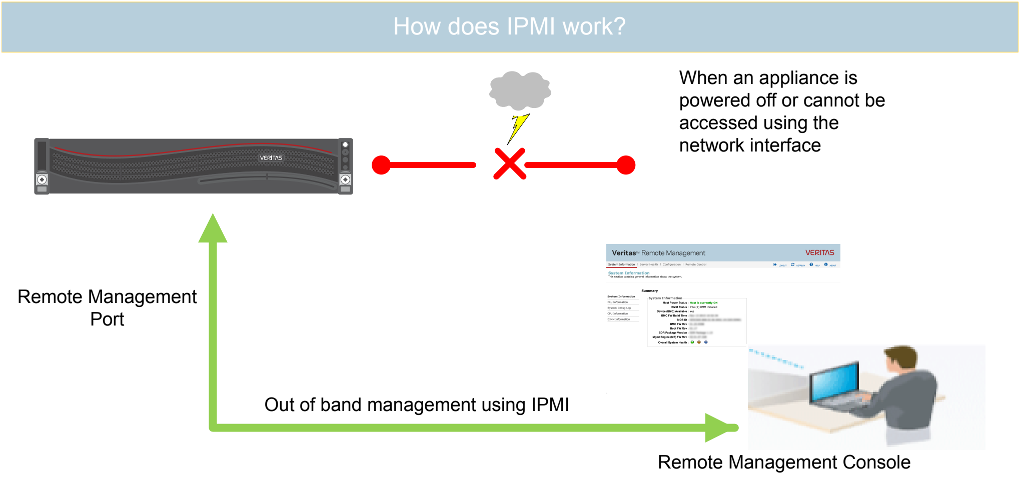
The Intelligent Platform Management Interface (or IPMI) provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system. You can configure the IPMI sub-system for your appliances. You can use the remote management port, located on the rear panel of the appliance, to connect to the IPMI sub-system.

The following figure shows the remote management port (or the IPMI port) on the rear panel of a NetBackup 5240 appliance:



The IPMI is beneficial after an unexpected power outage shuts down the connected system. In case the appliance is not accessible after the power is restored, you can use a laptop or desktop computer to access the appliance remotely by using a network connection to the hardware rather than to an operating system or login shell. This enables you to control and monitor the appliance even if it is powered down, unresponsive, or without any operating system.

The following diagram illustrates how IPMI works:


How does IPMI work?
When an appliance is powered off or cannot be accessed using the network interface
Remote Management Port
Out of band management using IPMI
Remote Management Console
Veritas Remote Management
VERITAS

Some of the main uses of IPMI are the following:

- Manage an appliance that is powered off or unresponsive. Using the IPMI, you can power on, power off, or restart the appliance from a remote location.
- Provides out-of-band management and help manage situations where local physical access to the appliance is not possible or preferred like branch offices and remote data center.
- In case the appliance is not accessible using regular network interfaces, you can access the NetBackup Appliance Shell Menu remotely using IPMI.

- Reimage the appliance from the IPMI interface by using ISO redirection.
- Monitor hardware health of the appliance from a remote location.
- Avoid messy cabling and hardware like keyboard, monitor, and mouse (KVM) solutions.

About password management and recovery

You may need to recover the admin password or a user password so that those users can regain appliance access. Password recovery can be done based on the following methods:

Table 2-3 Password recovery for local and LDAP users

User Type	Steps to change password	Password recovery situations and action
Local Users	Use the **Settings > Password Management** tab from the NetBackup Appliance Web Console.	Situations: An employee that maintains the password may leave the company, or you may lose or forget the password. Action: If any of these situations occur, contact Veritas Technical Support for assistance and ask the representative to reference tech note TECH189518/000016161.
LDAP, Active Directory, or Kerberos-NIS users	Use the following steps to reset or change the password: ▪ Update the user password in the Active Directory server, LDAP server, or Kerberos-NIS server. ▪ Change the appliance admin password from the **Settings > Password Management** tab in the NetBackup Appliance Web Console.	Situation: An LDAP user leaves the company, or may lose or forget the password. Use the following steps to reset or change the password for an LDAP user: ▪ Recover the password using the LDAP server. ▪ Contact Veritas Technical Support for changing the password.

See “About best practices” on page 11.

About IPv4-IPv6-based network support

The NetBackup Appliance is supported on a dual stack IPv4-IPv6 network and can communicate with IPv6 clients for backups and restores. You can assign an IPv6 address to an appliance, configure DNS, and configure routing to include IPv6 based systems.

Either the NetBackup Appliance Web Console or the NetBackup Appliance Shell Menu can be used to enter the IPv4 and IPv6 address information.

Review the following considerations for IPv6 addresses:

- NetBackup appliances do not support a pure IPv6 network. An IPv4 address must be configured for the appliance, otherwise the initial configuration (which requires the command `hostname set`) is not successful. For this command to work, at least one IPv4 address is required.
  For example, suppose that you want to set the `hostname` of a specific host to v46. To do that, first make sure that the specific host has at least one IPv4 address and then run the following command:

  ```
  Main_Menu > Network > Hostname set v46
  ```

- Only global addresses can be used, not addresses with link-local or node-local scope. Global-scope and unique-local addresses are both treated as global addresses by the host.
  Global-scope IP addresses refer to the addresses that are globally routable. Unique-local addresses are treated as global.
- You cannot use both an IPv4 and an IPv6 address in the same command. For example, you cannot use `Configure 9ffe::9 255.255.255.0 1.1.1.1`. You should use `Configure 9ffe::46 64 9ffe::49 eth1`.
- Embedding the IPv4 address within an IPv6 address is not supported. For example, you cannot use an address like 9ffe::10.23.1.5.
- You can add an appliance media server to the master server if the IPv6 address and the host name of the appliance media server are available.
  For example, to add an appliance media server to the master server, enter the IPv6 address of the appliance media server as follows:
  Example:

  ```
  Main > Network > Hosts add 9ffe::45 v45 v45
  ```

  ```
  Main > Appliance > Add v45 <password>
  ```

  You do not need to provide the IPv4 address of the appliance media server.
- A pure IPv6 client is supported in the same way as in NetBackup.
- You can enter only one IPv4 address for a network interface card (NIC) or bond. However, you can enter multiple IPv6 addresses for a NIC or bond.

- Network File System (NFS) or Common Internet File System (CIFS) protocols are supported over an IPv4 network on appliance. NFS or CIFS are not supported on IPv6 networks.
- The NetBackup client can now communicate with the media server appliance over IPv6.
- The `Main_Menu > Network > Hosts` command supports multiple IPv6 addresses to be assigned to the same host name having one network interface card (NIC). However, only one IPv4 address can be assigned to a specific host name having one NIC using this command.
- You can add an IPv6 address of a network interface without specifying a gateway address.

  For more details, see the *NetBackup Appliance Command Reference Guide*.

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 11.

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 it results in an error condition.

Note: If the user is removed from the LDAP directory or Active Directory (and not removed from appliance), though the user is listed as LDAP or AD 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.
```

For more information refer to the *NetBackup™ Appliance Security Guide*.

See “About best practices” on page 11.

About troubleshooting tools

This chapter includes the following topics:

Tools for troubleshooting the NetBackup Appliance

This chapter describes the tools and commands that you can use to diagnose the issues faced by your NetBackup Appliance. It includes the following sections:

Table 3-1 Sections in the Troubleshooting Tools chapter

Section	Description	Link
About hardware monitoring	This section describes the hardware monitoring and alerting mechanisms that are available on the appliance.	See "About hardware monitoring" on page 27.

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

Section	Description	Link
Troubleshooting and tuning your appliance using the Appliance Diagnostics Center	This section describes the Appliance Diagnostics Center, which is used to troubleshoot 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 28.
About NetBackup support utilities	This section describes the NetBackup support utilities that the NetBackup Appliance supports.	See "About NetBackup support utilities" on page 31.

For more specific troubleshooting information about a particular issue, go to the NetBackup Appliance page on the Veritas Support website. This page contains articles and troubleshooting information relevant to NetBackup Appliance. Use the search function to look for helpful articles about specific issues.

See "About this guide" on page 6.

About hardware monitoring

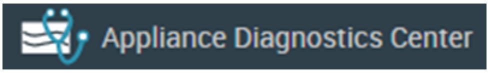
The appliance has the ability to monitor itself for hardware problems. If it detects a problem that needs attention, it uses the following notification mechanisms:

- Hardware monitoring and alerting from the NetBackup Appliance Web Console.
- Sending a notification to Veritas using Call Home.
- Sending an email to the local administrator.
- Sending an alert to the SNMP manager.
  See the *NetBackup Appliance SNMP Trap Reference Guide* for a full list of the appliance SNMP traps and recommended actions for when an error occurs.

For a full explanation of the hardware monitoring features, refer to the *NetBackup Appliance Administrator's Guide*.

Troubleshooting and tuning appliance from the Appliance Diagnostics Center

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



Appliance Diagnostics Center

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

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

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.

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

Click **Collect Log files**

Use this wizard 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 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 Veritas 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.

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` ■ `/msdp/data/dp1/pdvol/log`
NetBackup Appliance Web Console	All logs related to NetBackup Appliance Web Console logs are collected under the following directories: `/log/webgui`
NetBackup support utility (`nbsu`)	Diagnostic information about NetBackup and the operating system.
DataCollect	Hardware and storage device logs. The logs created by the `DataCollect` utility are collected.

About NetBackup support utilities

The NetBackup Appliance 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 Appliance to perform the following tasks:

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

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

```
 Running audit as Media Server.

 Collection Version: x.x
    Collection Time: Tuesday, October 7, 2010 at 19:17:11 PM
        NBU Release: NetBackup-RedHat2.6.18 7.7.1
        NBU Version: 7.7.1
  NBU Major Version: 7
  NBU Minor Version: 7
  NBU Release Update: 1
     NBU Patch Type: Release Update
    NBU GlobDB Host: "host name"
     Is GlobDB HOST? No
              UNAME:
           Hostname: sample.name.veritas.com
   Host's  Platform: Linux
  Perl Architecture: Linux

 Initialization completed in 14.040101 seconds.


 Brief Description of What It Does (for type 1):
----------------------------------------------------
 1) Perform basic self checks.
 2) Check connectivity to 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 2.867581 seconds.

 Initiating tests...
```

```
COMPLETED.  Thank you for your patience.


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

NetBackup Support Utility (nbsu)

You can use the `nbsu` utility to gather appropriate diagnostic information about NetBackup and the operating system.

The NetBackup Support Utility (NBSU) is a Veritas utility used to gather diagnostic information about the system on which the utility is run. By default, NBSU gathers appropriate diagnostic information based on the operating system and NetBackup environment.

You can use the `Support > NBSU` command to create or remove the NetBackup configuration support files that the NBSU utility uses.

For more information, see the *NetBackup Appliance Commands Reference Guide*.

See "Tools for troubleshooting the NetBackup Appliance" on page 26.

Chapter 4

Working with log files

This chapter includes the following topics:

About NetBackup Appliance log files

Log files help you to identify and resolve any issues that you may encounter with your appliance.

NetBackup Appliance has the ability to capture hardware-, software-, system-, and performance-related data. Log files capture information such as appliance operation, issues such as unconfigured volumes or arrays, temperature or battery issues, and other details.

Table 4-1 describes the methods you can use to access the appliance log files.

Table 4-1 Viewing log files

From...	Using...	Log details
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 the Collect Log files wizard" on page 36. See "Troubleshooting and tuning appliance from the Appliance Diagnostics Center" on page 28.	■ 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 > SDCS Audit View** screen from the NetBackup Appliance Web Console to retrieve the audit logs of an appliance.	Appliance 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 37.	■ Appliance configuration log ■ Appliance command log ■ Appliance debug log ■ NetBackup logs, Volume Manager logs, and the NetBackup logs that are contained in the `openv` directory ■ Appliance operating system (OS) installation log ■ NetBackup administrative web user interface log and the NetBackup web server log ■ NetBackup 52xx appliance device logs

Table 4-1 Viewing log files *(continued)*

From...	Using...	Log details
NetBackup Appliance Shell Menu	You can use the `Main > Support > Logs > VxLogView Module` *`ModuleName`* commands to access the 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. See "Viewing log files using the Support command" on page 37.	Appliance unified logs: ■ `All` ■ `CallHome` ■ `Checkpoint` ■ `Commands` ■ `Common` ■ `Config` ■ `CrossHost` ■ `Database` ■ `Hardware` ■ `HWMonitor` ■ `Network` ■ `RAID` ■ `Seeding` ■ `SelfTest` ■ `Storage` ■ `SWUpdate` ■ `Trace` ■ `FTMS` ■ `FTDedup` ■ `TaskService` ■ `AuthService`
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 40.	Appliance 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.	Logs relating to the NetBackup-Java applications

About 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 for NetBackup, the appliance, operating system, NBSU (NetBackup Support Utility), DataCollect, and others.

You can collect log files from any NetBackup appliance.

After you have generated the log files you can email them to recipients, download them to your computer, or upload them to Veritas Support.

Refer to the following for information about the Appliance Diagnostics Center:

See "Troubleshooting and tuning appliance from the Appliance Diagnostics Center" on page 28.

See "About NetBackup Appliance log files" on page 34.

Viewing log files using the Support command

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

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

1 Enter browse mode using the `Main_Menu` > `Support` > `Logs` followed by the `Browse` command in the NetBackup Appliance Shell Menu. The `LOGROOT/>` prompt appears.

2 To display the available log directories on your appliance, type `ls` at `LOGROOT/>` prompt.

3 To see the available log files in any of the log directories, use the `cd` command to change directories to the log directory of your choice. The prompt changes to show the directory that you are in. For example, if you changed directories to the `GUI` directory, the prompt appears as `LOGROOT/GUI/>`. From that prompt you can use the `ls` command to display the available log files in the `GUI` log directory.

4 To view the files, use the `less <FILE>` or `tail <FILE>` command. Files are marked with `<FILE>` and directories with `<DIR>`.

See "Where to find NetBackup Appliance log files using the Browse command" on page 38.

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.

2 If you want, you can copy the unified logs with the `Main > Support > Logs > Share Open` command. Use the desktop to map, share, and copy the logs.

Note: The NetBackup 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 28.

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

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

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 NetBackup Appliance log files" on page 34.

Where to find NetBackup Appliance log files using the Browse command

Table 4-2 provides the location of the logs and the log directories that are accessible with the `Support > Logs > Browse` command.

Table 4-2 NetBackup Appliance log file locations

Appliance log	Log file location

Configuration log	`<DIR> APPLIANCE`
	`config_nb_factory.log`

Selftest report	`<DIR> APPLIANCE`
	`selftest_report`

Host change log	`<DIR> APPLIANCE`
	`hostchange.log`

NetBackup logs, Volume Manager logs, and the NetBackup logs that are contained in the `openv` directory	`<DIR> NBU` ■ `<DIR> netbackup` ■ `<DIR> openv` ■ `<DIR> volmgr`

Operating system (OS) installation log	`<DIR> OS`
	`boot.log`
	`boot.msg`
	`boot.omsg`
	`messages`

NetBackup deduplication (PDDE) configuration script log	`<DIR> PD`
	`pdde-config.log`

NetBackup Administrative web user interface log and the NetBackup web server log	`<DIR> WEBGUI` ■ `<DIR> gui` ■ `<DIR> webserver`
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 NetBackup Appliance log files” on page 34.

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 Veritas Support team to resolve device-related issues.

The DataCollect command collects the following logs:

- Release information
- Disk performance logs
- Command output logs
- iSCSI logs

Note: The iSCSI logs can be found in /var/log/messages and /var/log/iscsiuio.log.

- CPU information
- Memory information
- Operating system logs
- Patch logs
- Storage logs
- File system logs
- Test hardware logs
- AutoSupport logs
- Hardware information
- Sysinfo logs

To gather device logs with the DataCollect command

1. Log on to the NetBackup Appliance Shell Menu.
2. From the `Main > Support` view, type the following command to gather storage device logs.

   ```
   DataCollect
   ```

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

3. Copy the `DataCollect.zip` to your local folders using the `Main > Support > Logs > Share Open` command.
4. You can send the `DataCollect.zip` file to the Veritas Support team to resolve your issues.

See "About NetBackup Appliance log files" on page 34.

About 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	If NetBackup is installed on the computer where the application was started, the script logs the data in a log file at *`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`. If NetBackup was not installed on this computer, the script logs the data in a log file at *`install_path`*`\Veritas\Java\logs`. **Note:** When NetBackup is installed where the application is started, and when install_path is not set in the `setconf.bat` file, the script logs the data here: *`install_path`*`\Veritas\Java\logs`.
`/usr/openv/java/get_trace`	UNIX/Linux only. 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.

UNIX/Linux:
`/usr/openv/netbackup/bin/support/nbsu`
Windows:
`install_path``\NetBackup\bin\support\nbsu.exe`
	Queries the host and gathers appropriate diagnostic information about NetBackup and the operating system.

The following example describes how you can gather troubleshooting data for Veritas 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.
UNIX/Linux only: 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. Otherwise, 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 the `nbsu` command that is listed in this topic. Run this command after you complete the NetBackup installation and every time you change the NetBackup configuration.
Contact Veritas Technical Support	Provide the log file and the output of the `nbsu` command for analysis.

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, Veritas recommends that you only enable VxMS logging when it is necessary to troubleshoot an issue. Disable VxMS logging again when the issue is resolved.

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

To enable VxMS logging

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

```
SetLevel VxMS 1
```

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

```
VxMS log level is set to 1
```

To disable VxMS logging

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

```
SetLevel VxMS 0
```

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

```
VxMS log level is set to 0
```

See “About NetBackup Appliance log files” on page 34.

Chapter 5

Disaster recovery

This chapter includes the following topics:

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 Technical Support for assistance. The 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 Veritas 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 *NetBackup Appliance 52xx Initial Configuration Guide* or the *NetBackup Appliance 5330 Initial Configuration Guide* for more information.
- 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.

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 46.
- See "Appliance hardware failure" on page 48.
-

- See “Complete loss of appliance with recoverable operating system drives and attached storage disks” on page 55.
- See “Complete loss of appliance with recoverable attached storage disks” on page 57.
- See “Complete loss of appliance and attached storage disks” on page 86.

Software-related scenarios

- See “NetBackup appliance software corruption” on page 87.
- See “NetBackup appliance database corruption” on page 88.
- See “NetBackup appliance catalog corruption” on page 93.
- See “NetBackup appliance operating system corruption” on page 99.

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 5-1 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 47. For more information on the hardware initialization process, see "Verifying the operation of the appliance and storage hardware" in the *NetBackup 5230 Appliance Hardware Installation Guide*.

Table 5-1 Steps for restoring power to an appliance following a power interruption *(continued)*

Step	Action	Description
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 28. ■ Download the DataCollect log to check any logs associated with the hardware.
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:

Restoring operation to a NetBackup appliance following a power outage

This section describes how to restore operation to a NetBackup appliance after the source power is restored following a power outage.

To restore a standalone appliance following a power outage

1 Make sure that source power is available to the unit and that the unit is turned off.

> **Note:** On the control panel, the LEDs for the Ethernet ports (1, 2, and 3) that are connected are green. The system status LED is also green.

2 Press the power button on the control panel. The fans turn on as the unit starts initiation.

See "Restoring operation to a NetBackup appliance with external storage following a power outage" on page 48.

Restoring operation to a NetBackup appliance with external storage following a power outage

This section describes the sequence you must follow to restore operation to a NetBackup appliance with external storage after the source power is restored following a power outage

To restore operation to a NetBackup appliance with a storage system following a power outage

1 Make sure that the Veritas Storage Shelves are on and have initialized.

2 Make sure that source power is available to the appliance and that the appliance is turned off.

> **Note:** On the appliance control panel, the LEDs for the Ethernet ports (1, 2, and 3) that are connected are green. The system status LED is also green.

3 Press the power button on the control panel. The fans come on as the unit starts initiation.

See "Restoring operation to a NetBackup appliance following a power outage" on page 47.

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 5-2 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. ■ If the unit still does not turn on, contact Veritas 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. ■ 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 28.

Table 5-2 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 For more detailed procedures not covered in this Guide, navigate to the following link: http://www.veritas.com/docs/DOC7757 **Note:** If you find that non-user replaceable hardware is faulty, contact Veritas 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. ■ 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 28.
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.

Removing and replacing hardware components

If a hardware component fails, it may need to be replaced with a new part. 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 Veritas 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.

For the procedures on replacing individual components in the NetBackup appliances and the storage shelves, navigate to the NetBackup Appliance Hardware Service Procedures page.

Setting a NetBackup 5330 storage shelf component to the Service Allowed mode

Before service or replacement can be performed on a Primary Storage Shelf or an Expansion Storage Shelf, the specific component of the unit must be set to the Service Allowed mode.

Typically, a failure automatically sets the component of the affected unit to the Service Allowed mode. When a warning of an impending failure occurs, the component is not automatically set to the Service Allowed mode. For this situation, you must set the component to the Service Allowed mode manually, by using the NetBackup Appliance Shell Menu.

In the `Main_Menu > Support` view, two main commands are available:

- `ServiceAllowed Set PrimaryShelf`

  This command is used with options to set the appropriate Primary Storage Shelf component to the Service Allowed mode.
- `ServiceAllowed Set ExpansionShelf`

  This command is used with options to set the appropriate Expansion Storage Shelf component to the Service Allowed mode.

The following describes the available command options for setting a Primary Storage Shelf component or an Expansion Storage Shelf component to the Service Allowed mode.

Table 5-3 Service Allowed command options

Storage unit	Command options

Primary Storage Shelf	■ `Controller`
	Set the Service Allowed flag for a Primary Shelf Controller. When you enter this option, you must also identify the controller location (`A/B`). The following shows the complete command:
	`ServiceAllowed Set PrimaryShelf Controller A/B On/Off`
	■ `FanCanister`
	Set the Service Allowed flag for a Primary Shelf fan canister. When you enter this option, you must also identify the fan canister location (`Left/Right`).The following shows the complete command:
	`ServiceAllowed Set PrimaryShelf FanCanister Left/Right On/Off`
	■ `HDD`
	Set the Service Allowed flag for a Primary Shelf hard disk drive. When you enter this option, you must also identify the drawer location (`DrawerID`) and the disk drive location (`SlotNo`). The following shows the complete command:
	`ServiceAllowed Set PrimaryShelf HDD DrawerID SlotNo On/Off`
	Note: Before you run this command, first run the `Monitor > Hardware ShowHealth PrimaryShelf RAID` command. Refer to the "Precautions and guidelines" section for more information.
	■ `PowerCanister`
	Set the Service Allowed flag for a Primary Shelf power canister. When you enter this option, you must also identify the power canister location (`Top/Bottom`). The following shows the complete command:
	`ServiceAllowed Set PrimaryShelf PowerCanister Top/Bottom On/Off`

Table 5-3 Service Allowed command options *(continued)*

Storage unit	Command options
Expansion Storage Shelf	■ `ExpansionCanister` Set the Service Allowed flag for an Expansion Shelf canister. When you enter this option, you must also identify the canister location (`Top/Bottom`). The following shows the complete command: `ServiceAllowed Set ExpansionShelf ExpansionCanister` *`Top/Bottom On/Off`* ■ `FanCanister` Set the Service Allowed flag for a Primary Shelf fan canister. When you enter this option, you must also identify the fan canister location (`Left/Right`).The following shows the complete command: `ServiceAllowed Set ExpansionShelf FanCanister` *`Left/Right On/Off`* ■ `HDD` Set the Service Allowed flag for an Expansion Shelf hard disk drive. When you enter this option, you must also identify the exanpsion shelf ID (`ExpansionShelfID`), the drawer location (`DrawerID`), and the disk drive location (`SlotNo`). The following shows the complete command: `ServiceAllowed Set ExpansionShelf HDD` *`ExpansionShelfID DrawerID SlotNo On/Off`* **Note:** Before you run this command, first run the `Monitor > Hardware ShowHealth PrimaryShelf RAID` command. Refer to the "Precautions and guidelines" section for more information. ■ `PowerCanister` Set the Service Allowed flag for a Primary Shelf power canister. When you enter this option, you must also identify the power canister location (`Top/Bottom`). The following shows the complete command: `ServiceAllowed Set ExpansionShelf PowerCanister` *`Top/Bottom On/Off`*

Precautions and guidelines

Veritas requires that you perform this procedure only with assistance from Veritas Technical Support. It is important to understand that certain situations can adversely affect system operation. Care must be taken when you run the Service Allowed command options.

To keep your system at peak performance, fix each problem as it occurs and do not let problems accumulate. Multiple problems can degrade system performance and make servicing the system more difficult. Multiple problems can also increase the potential for a situation that may cause data loss.

The following describes how the Service Allowed mode may affect the system:

- Degraded performance

In some situations, setting a component to the Service Allowed mode can cause degraded performance. A message appears to alert you of this possibility before you proceed. For example, when you use the `Controller` option for the Primary Shelf, the following message appears:

```
Support> ServiceAllowed Set PrimaryShelf Controller A on
Service allowed flag is used for component replacement. Setting
this flag may cause performance degradation due to write cache
being turned off.
>> Do you want to continue? (yes, no):
```

- RAID volume status in Degraded state

  When you use the `HDD` option to set a hard disk drive to the Service Allowed mode, the following message appears:

  ```
  Support> ServiceAllowed Set PrimaryShelf HDD 1 2 on
  Service allowed flag is used for component replacement. Before
  you set this flag, run the
  'Monitor->Hardware ShowHealth PrimaryShelf RAID' command to
  make sure that this Hard Disk Drive (HDD) is in a RAID volume
  with a status of Optimal. If the RAID volume status is not Optimal,
  executing this command creates a RISK OF POTENTIAL DATA LOSS.
  >> Do you want to continue? (yes, no): no
  ```

  In this situation, the best practice is to enter `no`. Then you must resolve the current RAID volume issue to return it to Optimal status. Only then can you proceed with setting the affected hard disk drive to the Service Allowed mode.

  Veritas recommends that before you attempt to set any hard disk drive to the Service Allowed mode, first run the `Monitor > Hardware ShowHealth PrimaryShelf RAID` command. Check to make sure that the hard disk drive that you want to set to the Service Allowed mode is in a RAID volume with Optimal status.

  Warning: Make sure that you contact and work with Veritas Technical Support for guidance to avoid any situation that may cause the potential for data loss.

The following procedure describes how to set a Primary Storage Shelf or an Expansion Storage Shelf component to the Service Allowed mode.

To set a Primary Storage Shelf or an Expansion Storage Shelf component to the Service Allowed mode

1. Contact Veritas Technical Support and inform the representative that you need to set a storage shelf component to the Service Allowed mode.

   Allow the representative to assist you with the remaining steps that follow.

2. Log in to the NetBackup Appliance Shell Menu.

3. Enter `Main_Menu > Support`.

4. From the list of commands in Table 5-3, enter the appropriate command.

   Note: Before you attempt to set a hard disk drive to the Service Allowed mode, first run the `Monitor > Hardware ShowHealth PrimaryShelf RAID` command. Refer to the "Precautions and guidelines" section for more information.

   ---

5. Verify that the component is in the Service Allowed mode by checking that the blue Service Action Allowed LED on the affected storage shelf is on.

6. Perform the necessary work on the affected unit.

   After the work has been completed and the unit has been restored to normal operation, the Service Allowed mode is cleared automatically.

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 Veritas 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 5-4 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.	Veritas Technical Support dispatches service personnel to you who remove the drives from the appliance.
Step 2	Remove the damaged appliance and replace with a new appliance.	Veritas 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.	Veritas 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.

Table 5-4 Steps for replacing an appliance with recoverable operating system drives and attached disk storage *(continued)*

Steps	Action	Description
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 Veritas 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 5-5 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.	Veritas 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 5-5 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 5-5 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 60. ■ See "Reconfiguring a 52xx master server appliance using the NetBackup Appliance Shell Menu" on page 64. ■ See "Configuring a master server to communicate with an appliance media server" on page 72. ■ See "Reconfiguring a 52xx or 5330 media server appliance using the NetBackup Appliance Shell Menu" on page 74. **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 reimaging and reconfiguration procedures

Use the following procedures as a guide to walk through reimaging and 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. Existing backup data on the storage volumes are preserved automatically. In order to complete the data recovery the appliance must be reconfigured from the NetBackup Appliance Shell Menu. The NetBackup Appliance Web Console cannot be used if you want to preserve the previous storage configuration.

To re-image an appliance from the USB drive

1. 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.

   Note: If you cannot log into the appliance, insert the USB drive into the appliance, turn on the appliance, and then proceed to Step 4.

   Contact Veritas Technical Support if you cannot login to the appliance to export IPsec credentials. More in depth assistance is needed in this situation.

   - 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>
  ```

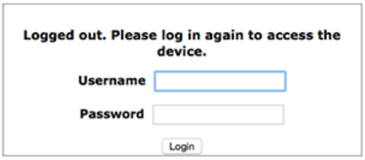
- Copy the .pfx file as follows:

  ```
  # 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 re-image.

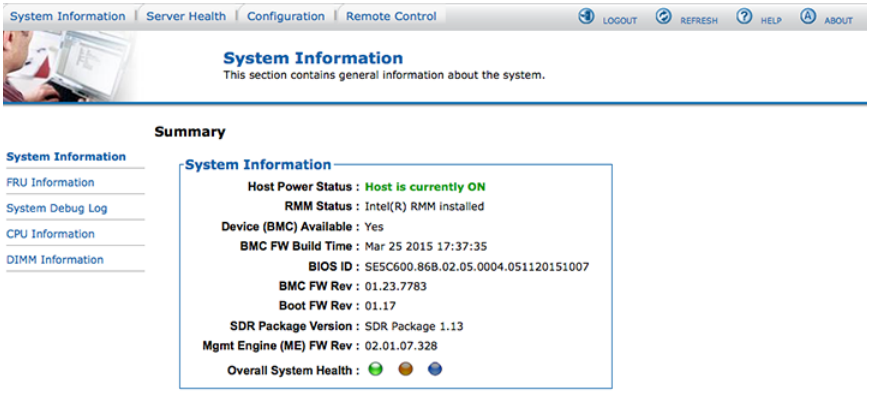
3 Connect the remote management (IPMI) port of the appliance that you are reconfiguring to the corporate network, then do the following:

- 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.



Logged out. Please log in again to access the device.

On the **System Information** page, click **Remote Control**.



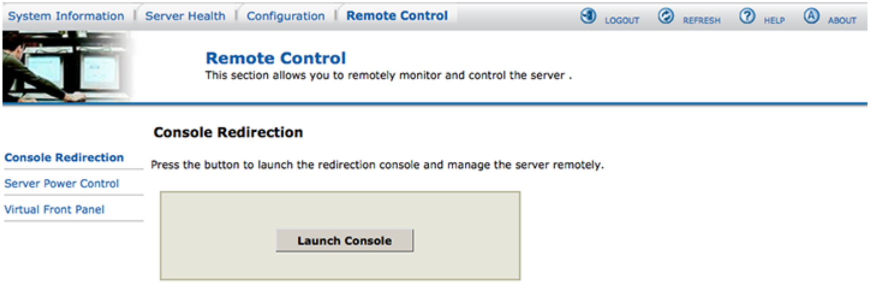
System Information
This section contains general information about the system.

Summary

System Information

Host Power Status : Host is currently ON
RMM Status : Intel(R) RMM installed
Device (BMC) Available : Yes
BMC FW Build Time : Mar 25 2015 17:37:35
BIOS ID : SE5C600.86B.02.05.0004.051120151007
BMC FW Rev : 01.23.7783
Boot FW Rev : 01.17
SDR Package Version : SDR Package 1.13
Mgmt Engine (ME) FW Rev : 02.01.07.328
Overall System Health : ● ● ●

On the **Remote Control** page, click **Launch Console**.



Remote Control
This section allows you to remotely monitor and control the server .

Console Redirection

Press the button to launch the redirection console and manage the server remotely.

4 Click **Launch Console**. This step opens a **JViewer** application that lets you remotely monitor and control the media server appliance.

5 From the **Veritas Remote Management** interface, select **Server Power Control**. On that Web page do the following:

- Select the **Reset Server** radial button.
- Click **Perform Action**.

6 In the JViewer application window, press F6 to enter the boot menu of the appliance.

7 After you select the USB drive, press the ESC key. A screen appears that lets 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. 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 re-image 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 Type `Return` twice to return to the main menu.

11 Verify that you are at the main menu.

The appliance is now ready for initial configuration.

Refer to the following topics to reconfigure your NetBackup appliance:

See "Reconfiguring a 52xx master server appliance using the NetBackup Appliance Shell Menu" on page 64.

See "Reconfiguring a 52xx or 5330 media server appliance using the NetBackup Appliance Shell Menu" on page 74.

Reconfiguring a 52xx master server appliance 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: The appliance comes configured with a known default password for the `Maintenance` user account. You should change this password either before or immediately after the initial configuration to prevent unauthorized access to the appliance maintenance mode. Note that you must provide the `Maintenance` user password to Veritas Technical Support in the event that the appliance requires troubleshooting services. Step 14 in the following procedure describes how to change the `Maintenance` user password.

To reconfigure a 52xx master server appliance using the NetBackup Appliance Shell Menu

1 Before performing the reconfiguration process, make sure you have followed the re-image procedure. See “Reimaging a NetBackup appliance from the USB drive” on page 60.

2 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 23.

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`.

3 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 6.

```
DNS Domain Name
```

Where *Name* is the new domain name for the appliance.

4 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 23.

To add multiple IP addresses, use a comma to separate each address and no space.

5 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.

6. 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 23.

7. From the **Main_Menu** > **Network** view, use the following command to set the host name for your appliance.

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

   ```
   Hostname Set Name
   ```

   Where *Name* is the short host name or the fully qualified domain name (FQDN) of this appliance.

   The host name is applied to the entire appliance configuration with a few exceptions. The short name always appears in the following places:

   - NetBackup Appliance Shell Menu prompts
   - Deduplication pool catalog backup policy
   - Default storage unit and disk pool names

   If this appliance has been factory reset and you want to import any of its previous backup images, the appliance host name must meet one of the following rules:

   - The host name must be exactly the same as the one used before the factory reset.
   - If you want to change the host name to an FQDN, it must include the short name that was used before the factory reset. For example, if “myhost” was used before the factory reset, use “myhost.domainname.com" as the new FQDN.
   - If you want to change the host name to a short host name, it must be derived from the FQDN that was used before the factory reset. For example, if “myhost.domainname.com” was used before the factory reset, use “myhost” as the new short host name.

Note: The host name can only be set during an initial configuration session. After the initial configuration has completed successfully, you can re-enter initial configuration by performing a factory reset on the appliance. See the *NetBackup Appliance Administrator's Guide* for more information.

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
```

8 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*.

9 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.

10 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.

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

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

```
Master
```

12 If an existing NetBackup catalog is detected choose `yes` to preserve it or choose `no` to create a new catalog. The following message is displayed:

```
A NetBackup catalog database has been found on the disk that belongs to this appliance.
You have an option to create an empty catalog or reuse the preexisting NetBackup catalog.

If you choose 'yes', the following occurs:
1. The preexisting NetBackup catalog will be used.
2. Any preexisting storage partitions and objects will be used.

If you choose 'no', the following occurs:
1. The preexisting NetBackup catalog will be backed up.
2. An empty NetBackup catalog will be created.
3. You will an have opportunity to customize storage pools.

If you want to remove the backup and catalog data,
run 'Support->Storage Reset' before you proceed.

>> Do you want to reuse the NetBackup catalog? [yes,no]: yes
```

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

Note: If you chose to reuse the NetBackup catalog in 12, the storage prompts are not presented. Skip to 15.

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 MSDP. 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 MSDP. 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 Change the `Maintenance` user password as follows:

- Enter the `Main_Menu > Support > Maintenance` command.
- At the password prompt, enter the default `Maintenance` user password (`P@ssw0rd`).
- At the `Maintenance` shell prompt, enter the `passwd` command to change the password.

- Type `Exit` to return to the NetBackup Appliance Shell Menu.

For complete information about using the `Support > Maintenance` command, see the *NetBackup Appliance Commands Reference Guide*.

15 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:

See "About NIC1 (eth0) port usage on NetBackup appliances" on page 85.

16 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 72.

See "Reconfiguring a 52xx or 5330 media server appliance using the NetBackup Appliance Shell Menu" on page 74.

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:
  443, 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 or 5330 media server appliance using the NetBackup Appliance Shell Menu" on page 74.

Reconfiguring a 52xx or 5330 media server appliance using the NetBackup Appliance Shell Menu

The following procedure describes how to reconfigure a 52xx media server appliance from the NetBackup Appliance Shell Menu.

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

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

Caution: The appliance comes configured with a known default password for the `Maintenance` user account. You should change this password either before or immediately after the initial configuration to prevent unauthorized access to the appliance maintenance mode. Note that you must provide the `Maintenance` user password to Veritas Technical Support in the event that the appliance requires troubleshooting services. Step 15 in the following procedure describes how to change the `Maintenance` user password.

To reconfigure a 52xx media server appliance using the NetBackup Appliance Shell Menu

1 Before performing the reconfiguration process, make sure you have followed the re-image procedure. See “Reimaging a NetBackup appliance from the USB drive” on page 60.

2 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 23.

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`.

3 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 6.

```
DNS Domain Name
```

Where *Name* is the new domain name for the appliance.

4 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 23.

To add multiple IP addresses, use a comma to separate each address and no space.

5 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.

6 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 23.

7 From the **Main_Menu** > **Network** view, use the following command to set the host name for your appliance.

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

```
Hostname Set Name
```

Where *Name* is the short host name or the fully qualified domain name (FQDN) of this appliance.

The host name is applied to the entire appliance configuration with a few exceptions. The short name always appears in the following places:

- NetBackup Appliance Shell Menu prompts
- Deduplication pool catalog backup policy
- Default storage unit and disk pool names

If this appliance has been factory reset and you want to import any of its previous backup images, the appliance host name must meet one of the following rules:

- The host name must be exactly the same as the one used before the factory reset.
- If you want to change the host name to an FQDN, it must include the short name that was used before the factory reset. For example, if “myhost” was used before the factory reset, use “myhost.domainname.com" as the new FQDN.
- If you want to change the host name to a short host name, it must be derived from the FQDN that was used before the factory reset. For example, if “myhost.domainname.com” was used before the factory reset, use “myhost” as the new short host name.

Note: The host name can only be set during an initial configuration session. After the initial configuration has completed successfully, you can re-enter initial configuration by performing a factory reset on the appliance. See the *NetBackup Appliance Administrator's Guide* for more information.

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
```

8 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*.

9 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.

10 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.

11 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. Veritas 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. Veritas 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, Veritas recommends that you provide all of the associated master server names.

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

12 The configuration process determines whether NetBackup storage objects have been detected. You must decide if you want to preserve any preexisting storage objects and data.

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
```

13 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 partition size in GB/TB [1GB..4.51TB]: (1 GB) [1.6395 GB..51.8 TB]:`
- `AdvancedDisk diskpool name: (dp_adv_5230)`
- `AdvancedDisk storage unit name: (stu_adv_5230)`

To configure an MSDP storage pool provide the following information:

- `MSDP partition size in GB/TB [118GB..4.49TB]: (4.23 TB)`
- `MSDP diskpool name: (dp_disk_5230)`
- `MSDP storage unit name: (stu_disk_5230)`
- `MSDP Catalog partition size in GB/TB [19GB..294GB]: (19 GB)`

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.

---

14 Choose whether or not you want to make changes to the storage configuration from above.

Note: The estimated time to configure storage can range depending on the system load. There may also be several minutes to restart the NetBackup services. The greater the system load the longer it takes to complete the operation.

```
Do you want to make changes to the storage configuration shown
above? [yes,no]: no
```

15 Change the default `Maintenance` user password as follows:

- Enter the `Main_Menu > Support > Maintenance` command.
- At the password prompt, enter the default `Maintenance` user password (`P@ssw0rd`).
- At the `Maintenance` shell prompt, enter the `passwd` command to change the password.
- Type `Exit` to return to the NetBackup Appliance Shell Menu.

For complete information about using the `Support > Maintenance` command, see the *NetBackup Appliance Commands Reference Guide*.

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

Note: If you are performing the reconfiguration from the network, skip to the next step.

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

See “About NIC1 (eth0) port usage on NetBackup appliances” on page 85.

About NIC1 (eth0) port usage on NetBackup appliances

By default, NIC1 (eth0) is factory set to IP address 192.168.229.233. This private network address is reserved to provide a direct connection from a laptop to perform the initial configuration. NIC1 (eth0) is typically not connected to your network environment.

Once the initial configuration has been completed, you can connect NIC1 (eth0) to an administrative network that does not provide any backup data transfer. However, you may need to change the default IP address if your primary network uses the same IP address range. NetBackup appliances do not support the use of any network configuration in the same range as the default IP address for the administrator interface on NIC1 (eth0).

For example, if NIC2 (eth1) is set to the 192.168.x.x IP address range, you must change the default IP address of NIC1 (eth0) to a different IP address range.

To change the IP address for NIC1 (eth0) after the initial configuration has been completed, do one of the following:

- From the NetBackup Appliance Web Console
  After logging into the appliance, click **Settings > Network > Network Settings**. In the **Network Configuration** section, edit the IPv4 address setting for NIC1 (eth0).
  For more information, see the *NetBackup Appliance Administrator's Guide*.
- From the NetBackup Appliance Shell Menu
  After logging into the appliance, use the `Network > IPv4` command to change the IP address for NIC1 (eth0).
  For more information, see the *NetBackup Appliance Command Reference Guide*.

Note: If NIC1 (eth0) is not configured on your appliance, checkpoint operations do not work from the NetBackup Appliance Web Console. This issue occurs only if you have removed the IP address configuration for the port. If you encounter this issue, configure the port or use the NetBackup Appliance Shell Menu to create a checkpoint or to roll back to one. As a best practice, even if NIC1 (eth0) is not used, make sure that it is configured with an IP address.

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 Veritas 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 5-6 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.	Veritas 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. Veritas Technical Support will assist you in replacing the storage systems.
Step 3	Power on the new components.	Power on the components in the following order: ■ Storage systems ■ Master server ■ Media server

Table 5-6 Steps for replacing an appliance and attached storage disk units after they have been rendered non-operational *(continued)*

Steps	Action	Description
Step 4	Configure the appliance and storage systems.	Configure the appliance as you would a new configuration. For a 52xx appliance, see the "Initial Configuration" chapter of the *NetBackup 52xx Initial Configuration Guide* for more information on setting up your 52xx appliance and attached storage systems. For a 5330 appliance, see the "Initial Configuration" chapter of the *NetBackup 5330 Initial Configuration Guide* for more information on setting up your 5330 appliance and attached storage systems.
Step 5	Recover the data from a secondary backup site.	If you have a secondary backup site, Veritas 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 5-7 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 Veritas 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 88. for database corruption disaster recovery. See See "NetBackup appliance catalog corruption" on page 93. for catalog corruption disaster recovery. See See "NetBackup appliance operating system corruption" on page 99. for operating system corruption disaster recovery.

NetBackup appliance database corruption

Appliance configuration 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 5-8 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 configuration 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 89.
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 93.

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.

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

Rolling back to an Appliance Checkpoint will revert the following
components:
        1) Appliance Operating System
        2) Appliance Software
        3) NetBackup Software
        4) Networking Configuration
        5) Any previously applied patches
        6) Backup data is not reverted

The existing Appliance Checkpoints in the system are:
------------------------------------------------------------
(1) Checkpoint Name: User directed checkpoint
Date Created: Fri Oct  5 09:27:32 2016
Description: User checkpoint after configuring network
------------------------------------------------------------
Please enter the checkpoint to rollback to (Available
options: 1 only):
```

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

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

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

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

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

```
----------------------------
ROLLBACK OPTIONS AND SUMMARY
----------------------------
Rollback to checkpoint name : [User directed checkpoint]
Auto reboot after rollback? : [YES]

The rollback reverts the entire system to the following versions:

+------------------------------------------------------+
|    Appliance    | Current Version | Reverted Version |
|-----------------+-----------------+------------------|
|app1.Veritas.com |NetBackup 8.0    |NetBackup 8.0     |
|                 |Appliance 3.0    |Appliance 3.0     |
|-----------------+-----------------+------------------|
|app2.Veritas.com |NetBackup 8.0    |NetBackup 8.0     |
|                 |Appliance 3.0    |Appliance 3.0     |
+------------------------------------------------------+
```

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

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

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

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

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

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

About 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 NetBackup catalog on the master server appliance is not included.
  - The backup data is not included.

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

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

NetBackup appliance catalog corruption

Appliance configuration catalog corruption may have occurred 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 configuration catalog on the appliance.

Table 5-9 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 95. for a detailed procedure on performing a factory reset. See "Appliance factory reset" in the *NetBackup Appliance Administrator's Guide* for more information on the topic of factory reset.
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.

Table 5-9 Steps for recovering from catalog corruption on the appliance *(continued)*

Steps	Action	Description
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. Veritas 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 reimaging and reconfiguration procedures” on page 60. for detailed procedures on reimaging and reconfiguring your appliance. See "Reconfiguring a NetBackup appliance" in the *NetBackup Appliance Decommissioning and Reconfiguration 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: A factory reset operation returns the password to the original, default value.

Note: Before performing a storage reset during a factory reset, remove ownership of any attached tape libraries. A factory reset operation may fail if tape libraries are still associated with an appliance.

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

To begin a factory reset from the appliance shell menu

1 Log on to the appliance as an administrator 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)
7) Fibre Transport Deduplication target port configuration

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

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

RESET STORAGE CONFIGURATION and BACKUP DATA [Optional]
 -- Removes all the images on the AdvancedDisk, MSDP, and Share partitions.
 -- Resets the storage partitions.
 -- Resets storage expansion units, if any.
- [Warning] Performing a factory reset interrupts all share activity and
  removes and resets all share data.
  Unmount all the shares on clients before continuing with this operation.
- [Info] Performing a factory reset removes the current Fibre Transport
  Deduplication target port configuration.
 >> Do you want to delete images and reset backup data? [yes/no] (yes) yes
 >> Resetting the storage configuration will remove all backup data on the
    storage partitions and any connected expansion units. This is not reversible.
    Are you sure you want to reset storage configuration? [yes/no] (yes) yes
 >> A reboot of the appliance is required to complete the factory reset.
    Reboot automatically after reset? [yes/no] (no) yes
 >> Automatically rebooting after the reset will not provide you with an opportunity
    to review the progress/final status of the reset. Are you sure you would like to
    automatically reboot? [yes/no] (no) yes
```

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

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

Appliance will make the following version changes:

+------------------------------------------------------------------------------+
|             Appliance             |  Current Version   |  Reverted Version   |
|-----------------------------------+--------------------+---------------------|
|appl1                              |NetBackup 7.7.3     |NetBackup 7.7.3      |
|                                   |Appliance 2.7.3     |Appliance 2.7.3      |
+------------------------------------------------------------------------------+
```

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

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

The factory reset continues and info messages are shown.

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 5-10 Steps for recovering from operating system corruption on the appliance

Steps	Action	Description
Step 1	Perform a re-image of the appliance using the USB drive.	Re-imaging an appliance from the USB drive returns your appliance to a clean and unconfigured state. See “Reimaging a NetBackup appliance from the USB drive” on page 60.
Step 2	Perform an initial configuration of the appliance.	Configure the appliance as you would a new configuration. Veritas recommends that you record all of your initial configuration information so that you can reference that information during the configuration process. For a 52xx appliance, see the "Initial Configuration" chapter of the *NetBackup 52xx Initial Configuration Guide* for more information on setting up your 52xx appliance and attached storage systems.
Step 3	Recover the data from a secondary backup site.	If you have a secondary backup site, Veritas Technical Support will help you work through recovering your data from a secondary backup site.

Chapter 6

NetBackup Appliance error messages

This chapter includes the following topics:

About NetBackup Appliance error messages

This chapter is 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 the NetBackup 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 101.
- See "Error messages displayed on the NetBackup Appliance Web Console" on page 103.
- See "Error messages displayed on the NetBackup Appliance Shell Menu" on page 121.
- See "NetBackup status codes applicable for NetBackup Appliance" on page 130.

The appliance also has the ability to send email alerts when certain failures are detected. Appliance email alerts contain error messages with Unique Message Identifier (UMI) codes. The UMI codes are associated with specific error conditions.

Each alert email includes a link to a related tech note. Click on the link to find more error details and suggested user actions for the specific error you encountered.

For more information about a particular UMI code, go to the Veritas Support website and search for the code that you need assistance with.

Error messages displayed during initial configuration

Table 6-1 lists some of the common error messages that you may come across during the initial configuration of your NetBackup Appliance:

Table 6-1 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.

Table 6-1 Errors in initial configuration *(continued)*

Error messages	Explanation	Recommended action
Cannot set the hostname "Name". An internal error occurred in Appliance. Check the logs to see the detailed reason.	This error can occur for the following reasons: ■ The appliance IP address is not configured when setting the host name. ■ If you try to use “nb-appliance” either as a short name or as the host name in a fully qualified domain name (FQDN). ■ Other internal errors	Try the following actions to resolve this issue: ■ Configure the appliance IP address before the host name is configured. ■ Use a host name other than the short name “nb-appliance” and the FQDNs “nb-appliance.domain.com”. ■ If the above actions do not resolve the problem, collect all the `Vxul` logs by using the `DataCollect` command and contact Technical 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 130.

See “Error messages displayed on the NetBackup Appliance Shell Menu” on page 121.

See “Error messages displayed on the NetBackup Appliance Web Console” on page 103.

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

Table 6-2 lists all the error messages, displayed on the Login screen and NetBackup Appliance Web Console Dashboard.

Table 6-2 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 web console logs to view the exceptions stack and trace all programmatic statements. You can use the Collect Logs Wizard to view the logs. See "About the Collect Log files wizard" on page 36.
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.
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 Veritas Support.

Table 6-2 Login screen and NetBackup Appliance Web Console Dashboard *(continued)*

Error message	Explanation	Recommended action
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 Veritas 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 needs 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 6-3 lists all the error messages that are displayed on the **Monitor > Hardware** tab.

Table 6-3 Monitor > Hardware

Error messages	Explanation	Recommended action
Unable to retrieve the hardware health information.	This message is displayed when the appliance is unable to retrieve hardware health information.	Wait at least ten minutes and then try to view the health information again. If the issue persists, contact Veritas Technical Support.
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 Veritas Technical Engineer to fix the beacon.
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.	You may want to call Veritas Technical Support for assistance in resolving this error.

Table 6-3 Monitor > Hardware *(continued)*

Error messages	Explanation	Recommended action
No BBUs were detected.	This message is displayed when the Battery Backup Unit (BBU) information cannot be retrieved.	You may want to call Veritas Technical Support for assistance in resolving this error.
No CPUs were detected.	This message is displayed when the CPU information cannot be retrieved.	You may want to call Veritas Technical Support for assistance in resolving this error.
No disks were detected.	This message is displayed when the disks information cannot be retrieved.	You may want to call Veritas Technical Support for assistance in resolving this error.
No fans were detected.	This message is displayed when the fan information cannot be retrieved.	You may want to call Veritas Technical Support for assistance in resolving this error.
No firmware were detected.	This message is displayed when the firmware information cannot be retrieved.	You may want to call Veritas 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 retrieve the status information.	Verify if you have configured MSDP for your appliance. If you have configured MSDP and you encounter this error, call Veritas Technical Support for assistance in resolving this error.
Partition information is not available.	This message is displayed when the partition information cannot be retrieved.	You may want to call Veritas 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.	You may want to call Veritas Technical Support for assistance in resolving this error.
Temperature information is not available.	This message is displayed when the temperature information cannot be retrieved.	You may want to call Veritas Technical Support for assistance in resolving this error.
Not able to fetch information for connections	This message is displayed when the connection information for the 5330 appliance cannot be retrieved.	You may want to call Veritas Technical Support for assistance in resolving this error.

Table 6-3 Monitor > Hardware *(continued)*

Error messages	Explanation	Recommended action
No controllers detected	This message is displayed when the controller information for the 5330 appliance cannot be retrieved.	You may want to call Veritas Technical Support for assistance in resolving this error.
No volumes detected	This message is displayed when the volume information for the 5330 appliance cannot be retrieved.	You may want to call Veritas Technical Support for assistance in resolving this error.

Table 6-4 lists all the error messages, displayed on the **Monitor > SDCS** tab.

Table 6-4 Monitor > SDCS

Error messages or Error type	Explanation	Recommended action
Certificate download failed.	The provided SSL certificate for the SDCS 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 SDCS server port details are incorrect.	Please verify that the port number, entered for the SDCS server is correct.
There are no audit logs to display.	The SDCS logs cannot be displayed on the NetBackup Appliance Web Console. This error is displayed when: ■ If you are connected to the SDCS server and the audit logs are currently being pushed to SDCS server. ■ If the logs are not available locally.	To view the SDCS logs, log onto the SDCS server and check the logs.
There are no audit logs to display.	If you are not connected to the SDCS 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 > SDCS** tab.

Table 6-5 lists all the error messages, displayed on the **Manage > Storage** tab.

Table 6-5 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 appliance storage component 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 Veritas Support. **Warning:** This is non-recoverable error. You need to collect all the `Vxul` logs using the `DataCollect` command and share them with the Veritas 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 6-6 lists all the error messages, displayed on the **Manage > Host** tab.

Table 6-6 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 logs using the `DataCollect` command and then contact Veritas Technical Support.

Table 6-6 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 logs using the `DataCollect` command and then contact Veritas Technical Support.
Error in updating deduplication Parameters	The current deduplication parameters for the appliance cannot be updated to the new parameters.	Collect the logs using the `DataCollect` command and then contact Veritas Technical Support.
Error resetting data buffer parameters.	The appliance cannot reset the current data buffer parameters to the default settings.	Collect the logs using the `DataCollect` command and then contact Veritas 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 logs using the `DataCollect` command and then contact Veritas Technical Support.
Error while retrieving data buffer parameters.	The current data buffer parameters for the appliance cannot be displayed.	Collect the logs using the `DataCollect` command and then contact Veritas Technical Support.
Error while retrieving storage lifecycle parameters.	The current storage lifecycle parameters for the appliance cannot be displayed.	Collect the logs using the `DataCollect` command and then contact Veritas 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 logs using the `DataCollect` command and then contact Veritas Technical Support.
Error while retrieving BMR status.	The current BMR status for the appliance cannot be displayed.	Collect the logs using the `DataCollect` command and then contact Veritas 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 logs using the `DataCollect` command and then contact Veritas 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 6-7 lists all the error messages, displayed on the **Manage > Appliance Restore** tab.

Table 6-7 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 Veritas Technical Support for further assistance.
Factory reset is not supported because no factory checkpoints exist. Please see the *Veritas 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 Veritas Technical Support for further assistance.

Table 6-8 lists all the error messages, displayed on the **Manage > License** tab.

Table 6-8 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 logs using the `DataCollect` command and then contact Veritas Technical Support.

Table 6-8 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 Veritas Technical Support. ▪ Collect the logs using the `DataCollect` command and then contact Veritas Technical Support.
Error in deleting License	This error may appear due to an internal system error.	Collect the logs all using the `DataCollect` command and then contact Veritas Technical Support.
Error while retrieving License List.	This error may appear due to an internal system error.	Collect the logs using the `DataCollect` command and then contact Veritas Technical Support.
Error occurred while loading the license keys.	This error may appear due to an internal system error.	Collect the logs using the `DataCollect` command and then contact Veritas Technical Support.
License key: {0} failed to install on media 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 logs using the `DataCollect` command and then contact Veritas Technical Support.

Table 6-9 lists all the error messages, displayed on the **Manage > Migration Utility** tab.

Table 6-9 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 Veritas Technical Support.

Table 6-9 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 Veritas 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 Veritas 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 Veritas Technical Support.

Table 6-10 lists all the error messages, displayed on the **Manage > Software Updates** tab.

Table 6-10 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 Veritas'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 Veritas'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 6-11 lists all the error messages, displayed on the **Manage > Additional Server** tab.

Table 6-11 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 logs using the `DataCollect` command and then contact Veritas Technical Support.
Unable to delete additional server.	This error may appear due to an internal system error.	Collect the logs using the `DataCollect` command and then contact Veritas 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 6-12 lists all the error messages, displayed on the **Settings > Notification** tab.

Table 6-12 Settings > Notification

Error messages	Explanation	Recommended action
Please verify if this system has been provisioned to Veritas.	You might encounter this error when your appliance is not provisioned to AutoSupport and you try to save changes on the **Settings > Notifications** page.	Provision the appliance to the AutoSupport server (or the Registration server). If the issue persists, call Veritas Technical Support.
Call Home test failed. Verify that this system has been correctly provisioned to Veritas.	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 the AutoSupport server. If the issue persists, call Veritas Technical Support.
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 Veritas 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 Veritas Technical Support for assistance in resolving this error.

Table 6-12 Settings > Notification *(continued)*

Error messages	Explanation	Recommended action
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 Veritas 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.
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 6-12 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.

Table 6-13 lists all the error messages, displayed on the **Settings > Network** tab.

Table 6-13 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 WAN optimization setting.	This message appears due to an internal system error.	Collect the logs using the `DataCollect` command and then contact Veritas Technical Support.

Table 6-13 Settings > Network *(continued)*

Error messages	Explanation	Recommended action
Error while retrieving Fibre Transport Settings	The current Fibre Transport Settings for the appliance cannot be displayed.	Collect the logs using the `DataCollect` command and then contact Veritas Technical Support.
Error in enabling/disabling FT flag configuration	The Fibre Transport settings cannot be enabled for your appliance.	Collect the logs using the `DataCollect` command and then contact Veritas Technical Support.
Error in updating SAN client flag configuration	The SAN Client Fibre Transport cannot be enabled for your appliance.	Collect the logs using the `DataCollect` command and then contact Veritas Technical Support.
Load failed.	The current Fibre Transport Settings for the appliance cannot be displayed.	Collect the logs using the `DataCollect` command and then contact Veritas Technical Support.
This appliance contains no detectable FC HBA card. Click the help(?) icon to see if your appliance configuration contains an HBA card(s).	This information shows in the following scenarios: ■ The appliance contains no HBA card in its hardware configuration. For example, a NetBackup 5220 Appliance, configuration A. ■ The appliance contains one or more HBA card(s), but all the HBA cards have failed.	■ See the *NetBackup Appliance Product Description Guide* to see if your appliance configuration contains one or more HBA card(s) ■ If the appliance configuration contains one or more HBA card(s), collect the logs using the `DataCollect` command and then contact Veritas Technical Support.
The appliance contains no HBA card for use as a target host for optimized duplication and replication over FC. Click the help(?) icon to see if your appliance HBA configuration supports this feature.	This information shows in the following scenarios: ■ The appliance contains one or more HBA card(s), but it does not support this feature. For example, a NetBackup 5330 Appliance, configuration C. ■ All the HBA cards that can be used for use as a target host for optimized duplication and replication have failed.	■ Check the product description guides to see if your appliance configuration supports this feature. ■ If the appliance configuration contains one or more HBA card(s) that supports this feature, collect the logs using the `DataCollect` command and then contact Veritas Technical Support.

Table 6-13 Settings > Network *(continued)*

Error messages	Explanation	Recommended action
The current HBA card configuration does not support the use of this appliance as a target host for optimized duplication and replication over FC. Click the help(?) icon to see the supported HBA configurations.	The current HBA card configuration cannot be used as a target host for optimized duplication or replication. The configuration is not any standard HBA configuration that the feature requires. The HBA card configuration can become non-standard for the following reasons: - Adding an HBA card(s) - Removing an HBA cards(s) - HBA cards failures	Collect the logs using the `DataCollect` command and then contact Veritas Technical Support.

Table 6-14 lists all the error messages, displayed on the **Settings > Date and Time** tab.

Table 6-14 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 logs using the `DataCollect` command and then contact Veritas 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 6-15 lists all the error messages, displayed on the **Settings > Authentication** tab.

Table 6-15 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 logs using the `DataCollect` command and then contact Veritas 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 password.	The provided password to access the LDAP server is incorrect.	Enter a valid password to configure the LDAP server.
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.

Table 6-15 Settings > Authentication *(continued)*

Error messages	Explanation	Recommended action
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 Veritas 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 Veritas 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 Veritas 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 Veritas 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 Veritas 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 Veritas Technical Support.

Table 6-15 Settings > Authentication *(continued)*

Error messages	Explanation	Recommended action
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 Veritas Technical Support.

Table 6-16 lists all the error messages, displayed on the **Settings > Password** tab.

Table 6-16 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.

Table 6-17 lists the error messages that are common to all the tabs on the NetBackup Appliance Web Console.

Table 6-17 Common error messages that can appear on the NetBackup Appliance Web Console

Error	**Explanation**	**Recommended action**
An unknown error has occurred. Please contact Veritas 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 130.

See “Error messages displayed on the NetBackup Appliance Shell Menu” on page 121.

See “Error messages displayed during initial configuration” on page 101.

Error messages displayed on the NetBackup Appliance Shell Menu

Table 6-18 lists some of the common error messages that you may come across while working from the NetBackup Appliance Shell Menu:

Table 6-18 Common error messages in the NetBackup Appliance Shell Menu

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.

Table 6-18 Common error messages in the NetBackup Appliance Shell Menu *(continued)*

Error messages	Explanation / Recommended action
Failed to get NetBackup version	Make sure that the NetBackup services are up and running on the appliance. If you encounter this issue, restart the NetBackup services.
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 ■ 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 and restart the appliance host. Check `/var/log/sf.log` for volume (VxVM) error messages.
Failed license check for AdvancedDisk storage	Make sure that a valid license for the NetBackup **Flexible Disk Option** is installed on the media server.
Failed license check for Deduplication storage	Make sure that a valid license for NetBackup **Deduplication Option** is installed on the media server
Failed to create Deduplication storage unit	Check if the storage unit or the corresponding disk volume already exists on the media server. If they do exist, verify if the storage unit or the corresponding disk volume is currently used. If the storage is redundant only then use the NetBackup Administration Console or the `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 6-19 lists error messages that are specific to the `Manage > Software` view commands.

Table 6-19 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 Veritas 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.
Unknown error. Please contact Veritas Technical Support!	The source of the error cannot be found.	Please contact Veritas Technical Support.
Software update, <*rpm*> is already installed on compute node, <*node name*>.	The `rpm` (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` (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 Veritas Support.

Table 6-19 Manage > Software view *(continued)*

Error message	Explanation	Recommended action
Please provide a valid EEB name.	This error message is only for the rollback of EEB. The EEB name is not valid.	Please check that the EEB name you have used.
Patch <*rpm name*> signature check failed.	Signature error found in the `rpm` (installer package) .	Please check if the `md5` number of the `rpm` (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.
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.
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 Veritas 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 6-20 lists error messages that are specific to the `Manage > Appliance Restore` view commands.

Table 6-20 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.
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 6-21 lists error messages that are specific to the `Main_Menu > Network` view commands.

Table 6-21 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 <*vlan_id*>. Interface <*eth*> 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.

Table 6-21 Main_Menu > Network view *(continued)*

Error message	Explanation	Recommended action
Failed to create VLAN <*vlan_id*>. Interface <*eth*> 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 <*vlan_id*>. Interface <*eth*> is slave to bond <*bond*>. 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.
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), <*eth*> 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 <*bond*> 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 <eth> in a bond. Interface is in use by VLAN <*vlan_id*>.	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.

Table 6-22 lists error message that are specific to the `Main_menu > Network > WANOptimization` view commands.

Table 6-22 Main_ Menu > Network > WANOptimization view

Error code and error message	Explanation	Recommended action
<V-409-925-11> Invalid result returned.	Cannot get the WAN optimization status because of an unexpected error or because a service may be down.	Restart the web service by starting the NetBackup Appliance Shell Menu. Then run the following command: `Support > InfraServices > Start WebServer` If the issue continues, contact technical support.
< V-409-925-12> Network interface optimization cannot be enabled for network port {{port}}.	The individual network interfaces are part of a network interface port bond. The individual network interfaces that comprise a bond cannot be enabled.	To enable WAN optimization for an individual network interface that is part of a bond, you must first delete the bond. After deleting the bond, you can then enable WAN optimization for the selected network interface. **Note:** Deleting the bond automatically disables WAN optimization for all network interfaces that comprise the bond.
< V-409-925-13> Network interface optimization cannot be disabled for network port {{port}}.	The individual network interfaces are part of a network interface port bond. Individual network interfaces that comprise a bond cannot be disabled	To delete WAN optimization for an individual network interface that is part of a bond, you must delete the bond. Deleting the bond automatically disables WAN optimization for all network interfaces that comprised the bond.
< V-409-925-14> Cannot disable WAN Optimization for network port {{port}}.	The specified network interface does not exist.	Remove the name of the network port that you want to disable from the parameters that you are entering on the command line.
< V-409-925-15> Cannot enable WAN Optimization for network port {{port}}.	The specified network interface does not exist.	Remove the name of the network port that you want to enable from the parameters that you are entering on the command line.

Table 6-23 lists error messages that are specific to the `Main_menu > Settings` view commands.

Table 6-23 Main_menu > Settings view

Error code and error message	Explanation	Recommended action
V-409-810-0001: Unable to detect the Deduplication service because the appliance role is not set. You must configure the appliance role using the Main_Menu > Appliance commands before you can enable this feature.	The appliance cannot be configured as a target host for Optimized Duplication and Auto Image Replication over Fibre Channel (FC) before the appliance role is set.	Set the appliance role.
V-409-810-0013: Failed to enable the Deduplication service because of an internal error. Contact Veritas Technical Support.	The appliance cannot be configured as a target host for Optimized Duplication and Auto Image Replication over FC because of an internal error.	Contact Veritas Technical Support.
V-409-810-0014: Failed to perform the operation because of an internal error. Contact Veritas Technical Support.	The appliance cannot perform the operation because of an internal error.	Contact Veritas Technical Support.
V-409-810-0015: Failed to enable the Deduplication service because of an internal error. Contact Veritas Technical Support.	The appliance cannot load the target port configuration because of an internal error.	Contact Veritas Technical Support.
V-409-810-0017: Failed to perform the operation because of an internal error. Contact Veritas Technical Support.	The appliance cannot disable Fibre Transport Deduplication because of an internal error.	Contact Veritas Technical Support.
V-409-810-0018: The current appliance model is not standard. Check your HBA card configuration and then contact Veritas Technical Support.	The appliance cannot enable Fibre Transport Deduplication because the HBA card configuration in the real panel is not a NetBackup Appliance standard hardware configuration. The factory HBA card configuration may have changed for the following reasons: ■ One or more HBA cards have failed. ■ One or more HBA cards have been installed or uninstalled.	To troubleshoot the problem, do the following: ■ Check the hardware health or hardware alerts ■ Check the HBA card in the real panel ■ Contact Veritas Technical Support.
V-409-810-0019: Failed to perform the operation because of an internal error. Contact Veritas Technical Support.	The appliance cannot perform the operation because of an internal error.	Contact Veritas Technical Support.

Table 6-24 lists error messages that are specific to the `Main_menu > Support > FibreTransport` view commands.

Table 6-24 Main_menu > Support > FibreTransport view

Error code and error message	Explanation	Recommended action
V-409-810-0006: Failed to configure the chunk size for optimized duplication and replication because the appliance role is not set. Before you can configure the chunk size for optimized duplication, you must first set the appliance role.	The Fibre Transport (FT) chunk size cannot be configured and used before the appliance role is set.	Set the appliance role.
V-409-810-0007: Failed to set the chunk size for optimized duplication and replication because of an internal error. Contact Veritas Technical Support.	The FT chunk size cannot be configured and used because of an internal error.	Contact Veritas Technical Support.
V-409-810-0016: Failed to perform the operation because of an internal error. Contact Veritas Technical Support.	The appliance cannot perform the operation because of an internal error.	Contact Veritas Technical Support.

Table 6-25 lists error message that are specific to the `Main_menu > Manage > FibreChannel` view commands.

Table 6-25 Main_menu > Manage > FibreChannel view

Error code and error message	Explanation	Recommended action
V-409-810-0002: Failed to restart the Deduplication service because of an internal error. Contact Technical Support.	The appliance cannot be configured as a target host for Optimized Duplication and Auto Image Replication over FC because of an internal error.	Contact Veritas Technical Support.
V-409-810-0011: Unable to configure the port *`Slot:Port`* as an FC Initiator port. The port is reserved for %s and cannot be changed. For more information about reserved HBA ports, refer to the NetBackup Appliance Fibre Channel Guide.	The port is reserved for use as target mode ports for SAN Client FTMS, and cannot be used as a initiator port for Optimized Duplication and Auto Image Replication over FC.	Use another port that can be used as a initiator port for Optimized Duplication and Auto Image Replication over FC. Refer to the *NetBackup Appliance Fibre Channel Guide* for the available ports.

Table 6-25 Main_menu > Manage > FibreChannel view *(continued)*

Error code and error message	Explanation	Recommended action
V-409-810-0012: Cannot find the port `Slot:Port`. Invalid HBA port identifier. Check the HBA ports on the appliance and make sure to enter a valid slot number (1-6) and a valid port number (1-2).	The appliance cannot find the port specified by the user. The user must have entered an invalid slot number, port number, or both.	Refer to the *NetBackup Appliance Fibre Channel Guide* for the available ports.
V-409-810-0014: Failed to perform the operation because of an internal error. Contact Veritas Technical Support.	The appliance cannot perform the operation because of an internal error.	Contact Veritas Technical Support.
V-409-810-0020: Failed to perform the operation because of an internal error. Contact Technical Support.	The appliance cannot perform the operation because of an internal error.	Contact Veritas Technical Support.

See “NetBackup status codes applicable for NetBackup Appliance” on page 130.

See “Error messages displayed during initial configuration” on page 101.

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 6-26 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.

Table 6-26 NetBackup status codes *(continued)*

NetBackup status code	Message	Explanation
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 *NetBackup™ Status Codes Reference Guide*.

See "NetBackup status codes applicable for NetBackup Appliance" on page 130.

See "Error messages displayed on the NetBackup Appliance Shell Menu" on page 121.

See "Error messages displayed on the NetBackup Appliance Web Console" on page 103.

See "Error messages displayed during initial configuration" on page 101.